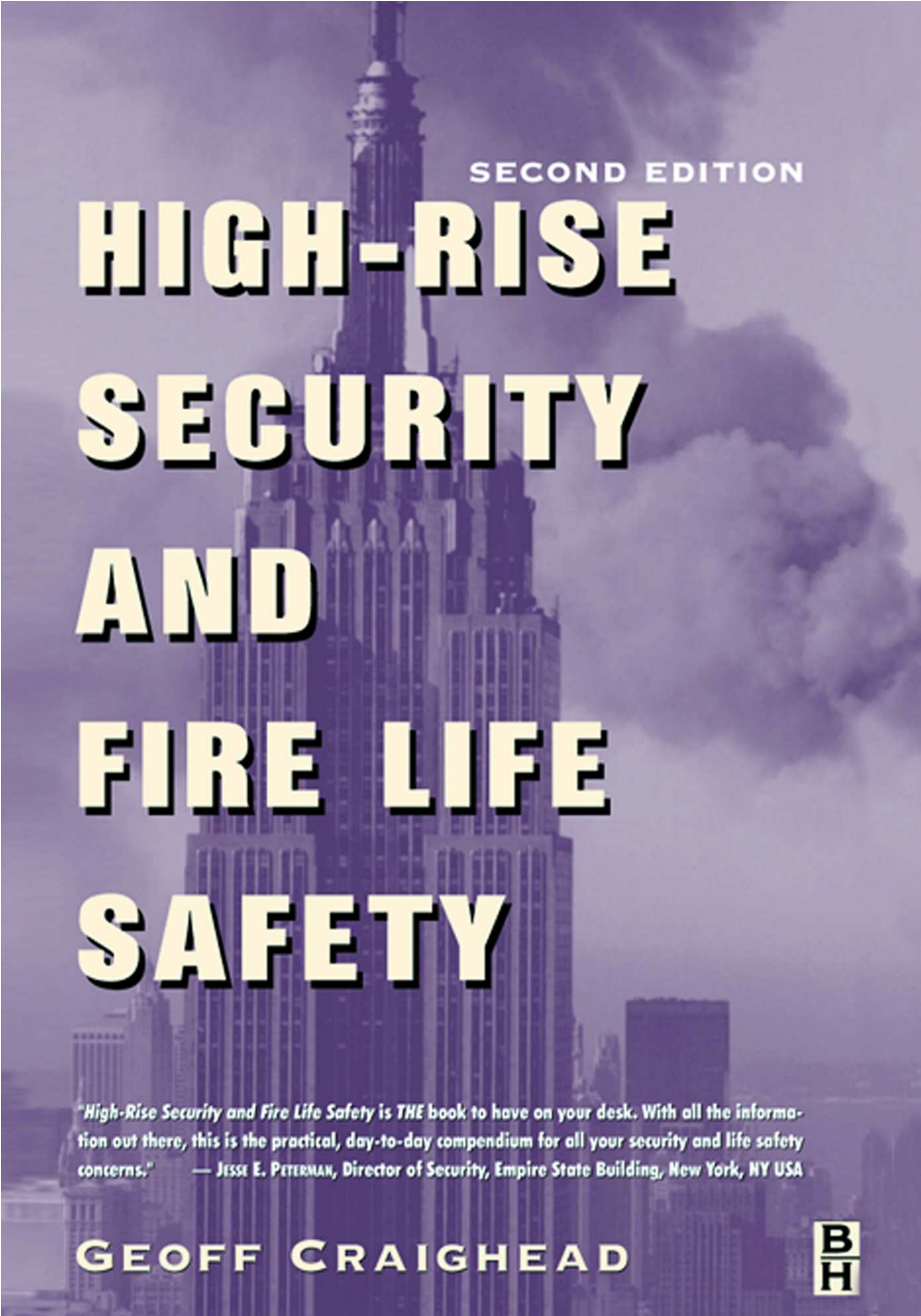


SECOND EDITION

HIGH-RISE SECURITY AND FIRE LIFE SAFETY

"*High-Rise Security and Fire Life Safety* is *THE* book to have on your desk. With all the information out there, this is the practical, day-to-day compendium for all your security and life safety concerns." — JESSE E. PETERMAN, Director of Security, Empire State Building, New York, NY USA

GEOFF CRAIGHEAD

BH

High-Rise Security and Fire Life Safety

This Page Intentionally Left Blank

High-Rise Security and Fire Life Safety

Second Edition

Geoff Craighead, CPP
Board Certified in Security Management by ASIS International
Certified in High-Rise Fire Life Safety Services by Los Angeles Fire Department

BUTTERWORTH HEINEMANN
An imprint of Elsevier Science

Butterworth-Heinemann is an imprint of Elsevier Science.

∞ Recognizing the importance of preserving what has been written, Elsevier-Science prints its books on acid-free paper whenever possible.

Library of Congress Cataloging-in-Publication Data

Craighead, Geoff.
High-rise security and fire life safety / Geoff Craighead.–2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 0-7506-7455-5 (alk. paper)
1. Skyscrapers–Security measures. 2. Skyscrapers–Fires and fire prevention. I. Title.

TH9745.S59 .C73 2003
658.4′73–dc21

2002038263

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

The publisher offers special discounts on bulk orders of this book.
For information, please contact:

Manager of Special Sales
Elsevier Science
225 Wildwood Avenue
Woburn, MA 01801-2041
Tel: 781-904-2500
Fax: 781-904-2620

For information on all Butterworth-Heinemann publications available, contact our World Wide Web home page at: http://www.bh.com

10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

Dedication

To those who gave their lives during the September 11, 2001, New York World Trade Center terrorist attack:

To Douglas G. Karpiloff, CPP, Port Authority of New York and New Jersey, security and life safety director for the New York World Trade Center, who at the time was transitioning his responsibilities to John P. O'Neill, Silverstein Properties, who was in his second day as head of the New York World Trade Center's security operation; James Corrigan, security and life safety director for 7 World Trade Center, Silverstein Properties; Robert H. Lynch, Jr., manager 5 World Trade Center, Port Authority of New York and New Jersey; Charles Magee, chief engineer, Silverstein Properties; John M. Griffin, director of operations, Silverstein Properties; Howard B. Kirschbaum, security manager for Marsh U.S.A. Inc.; Ronald G. Hoerner, resident manager of Summit Security Services, Inc.'s, World Trade Center contract security operation; Richard Rescorla, CPP, first vice president of security for Morgan Stanley Dean Witter; Larry Bowman, Denny Conley, Francisco Cruz, Samuel Fields, Daniel Lugo, Robert Martinez, Jorge Morron, Esmerlin Salcedo, and Ervin Gaillard, security officers from Summit Security Services; Andrew Bailey, Mannie Clark, Lamar Hulse, and Stanley McCaskill, security officers from Advantage Security; and Francisco E. Bourdier, security officer from Allied Security, who was killed at a nearby building when one of the towers collapsed.

and the 343 New York City Firefighters, 37 Port Authority Police Officers (including Robert D. Cirri, Police Lieutenant, Anthony P. Infante, Jr., Police Inspector, Robert M. Kaulfers, Police Sergeant, Kathy Mazza, Police Captain, Ferdinand V. Morrone, Director of Public Safety/Superintendent of Police, and James A. Romiot, Police Chief), an additional 35 Port Authority of New York and New Jersey civilians, and 23 New York City Police Officers who perished during the September 11, 2001, World Trade Center Terrorist Attack

And to Pinkerton, A Securitas Company, for giving me the opportunity to work in high-rise services

my wife, Sarah, my beloved helpmate and sweetheart,
and Pip and Searcy, our treasured children

and, the Lord, who sustains me everyday

The names of those persons, except for Francisco E. Bourdier, who perished on September 11, 2001, at the New York World Trade Center, were obtained from ASIS*Dynamics* (ASIS International, Alexandria, VA, November/December 2001) and *BOMA.org Staff* (The Building Owners and Managers International, Washington, D.C., May 2002).

This Page Intentionally Left Blank

Contents

Foreword to the Second Edition

In the world of high-rise building design and construction, a variety of security and life safety questions are posed to the engineers and architects who must provide a functional building. The solutions should balance the design with the risks associated with any building—regardless of size and occupancy.

These are among the issues discussed throughout the second edition of *High-Rise Security and Fire Life Safety*. Most of these subjects apply to the entire range of high-rise building stock in the world—both new and existing. While we have always known that the life safety protection of the occupants of buildings is of paramount importance, today's building tenants demand more: How secure is their space from a variety of threats, including theft of both real and intellectual property? Are tenant companies and their employees protected against personal harm by intruders, accidental fire and, now, terrorist attacks?

Achieving the proper level of protection is not possible with just one system or one procedure. It is the synergistic effect of all building systems and features working together that keeps facilities safe. Throughout the history of high-rise buildings, the norms for building safety have been derived from, and applied to, a great number of designs. World Trade Center 1 and 2 in New York; Petronas Tower 1 and 2 in Kuala Lumpur; Jin-Mao Building in Shanghai; Sears Tower in Chicago; and Emirates Tower in Dubai: all of these magnificent buildings have incorporated numerous systems and features that work, and have worked, to keep them safe during a wide range of events.

As building systems become more intricate and sophisticated, the overlap between systems is more pronounced now than ever before. The delineation between building security systems and fire alarm systems is just one example. Understanding the role, limitations and interface between systems is fundamental to system selection. Complementing the systems side of building design is the operating feature, or human interface, that supplements these sophisticated systems. The best written plans and the highest quality building systems and components are meaningless if they are not exercised, tested, reviewed, checked and updated on a periodic basis.

Geoff Craighead has provided us with a thorough description and review of all of these subjects as they relate to high-rise buildings. The public is now acutely aware of the importance of its own safety in high-rise buildings, and wants to know how building management teams are protecting them. As in the first edition of this book, we are given the road map of how to implement the best plan for a particular building.

The latest peril affecting design, namely the new level of hostile acts, is introduced in this edition of the text. Terrorist acts present unique threats that require new countermeasures.

High-rise buildings are not inherently dangerous structures, but they do require additional systems and features that other buildings do not. Keeping them safe and functional is what this text is all about.

Robert E. Solomon, PE
Assistant Vice President for Building and Life Safety Codes
NFPA
Quincy, Massachusetts

Foreword to the First Edition

Vertical cities—or high-rise buildings, as they are called—pose unique problems for security and safety professionals charged with the responsibility of protecting life and property. High-rise buildings, such as the Sears Tower in Chicago, the World Trade Center in New York, and thousands of others across the United States, are virtually cities within themselves. Just as the architecture within each varies, so do the regulations governing security and fire life safety programs for each building.

Every year, we see, hear, and read about the terrible tragedies caused by fires, earthquakes, tornadoes, bombings, disgruntled employees, terrorists, and the like. Every possible scenario must be accounted for. There is no substitute for an effective security and fire life safety program. Thousands of lives are dependent on it. Awareness and training are essential. Security and safety personnel must be trained for any and all eventualities.

The author includes here the terminology, the functions, the procedures, the equipment, and the standards for an effective program. *High-Rise Security and Fire Life Safety* is a comprehensive resource for everyone who manages, works in, or visits high-rise commercial office buildings.

Robert G. Lee, CPP, CFE, CDRP
Vice President and Corporate Security Director
Great Western Financial Corporation
Chairman of the National Standing Committee on Disaster Management
American Society for Industrial Security

This Page Intentionally Left Blank

Preface

Due to their design and construction, high-rise buildings are unique facilities with specialized needs. To protect the lives and property of the thousands of people who daily use these facilities, it is essential that high-rise security and fire life safety programs be well planned and executed. Useful reference materials for building owners and managers, architects, security and fire safety directors, security consultants, and contract security firms include the following:

1. High-rise development and utilization
2. High-rise assets and threats to those assets
3. The security and fire safety of modern high-rise buildings
4. How to conduct security and fire life safety surveys
5. Types of security and fire life safety systems and equipment found in high-rise buildings
6. Security policies and procedures for high-rise office buildings
7. How to effectively manage the security function, including investigations
8. The types of emergencies likely to occur and how to establish, implement, and maintain a Building Emergency Plan to effectively handle them
9. The laws, codes, and standards that are the framework of security and fire life safety
10. How to interact effectively with law enforcement and fire authorities

The second edition of *High-Rise Security and Fire Life Safety* addresses these areas. Wherever appropriate, updated information, including code changes, has been included.

In the seven years since this book was first published, there has been considerable change in the threats and vulnerabilities associated with high-rise buildings. The climactic events of September 11, 2001, when the twin towers of the New York World Trade Center were destroyed in a terrorist attack, are a watershed in the world of high-rise security and fire life safety. For obvious reasons this event is given special treatment. Also, a new chapter, Chapter 14, *Apartment and Residential Buildings, Hotels and Motels, and Hospitals and Health Care Facilities*, has been included.

This book supplies material which can be adapted, modified, rejected, or used for the reader's own purposes. I have endeavored to avoid errors, both of omission and commission. I will be glad to correct in future editions any inaccuracies that are brought to my attention.

In conclusion, I commend this book to the kind consideration of building owners and managers in general, and security and fire life safety professionals in particular, with the hope that it will continue to benefit the high-rise community. Only when knowledge is applied specifically to the needs of a particular facility will it become of real value. Therein lies the reader's part.

Geoff Craighead, CPP

Acknowledgments

There are many people who have contributed to the field of security and fire life safety during the time that high-rise buildings have existed. I am particularly indebted to those who took the time to document their thoughts so that others, such as myself, could learn and benefit.

The following have contributed to my experience, learning, and understanding of the world of high-rise security and fire life safety: Initially, Hong Kong, with its myriad of high-rise structures, followed by the United States of America, with its thousands of well-designed and well-operated buildings; the International Professional Security Association, incorporating the Institute of Industrial Security; ASIS International, the preeminent global organization for security professionals, its Professional Certification Board that oversees its certification programs, and the O.P. Norton Information Resources Center; the National Fire Protection Association (NFPA), with its sound standards and training materials for fire life safety professionals; the Institute of Real Estate Management (IREM); BOMA International; and the Council on Tall Buildings and Urban Habitat.

I am particularly grateful to those firms that have employed me during my professional career and afforded me the privilege of experiencing the world of security. In addition, there are many building owners and managers, security and life safety professionals, law enforcement and fire department personnel, and friends from whom I have learned. It is not possible to name them all without overlooking someone; however, particular recognition is due to those individuals who helped to make this second edition possible.

DAVID G. AGGLETON, CPP
President
Aggleton & Associates

ROBERT E. SOLOMON, PE
Assistant Vice President for Building and Life Safety Codes
NFPA

JIM DEWOLF
Vice President of Technical Publishing
Butterworth–Heinemann

JENNIFER RHUDA
Assistant Editor
Butterworth–Heinemann

GLEN W. KITTERINGHAM, CPP
Senior Manager Security and Life Safety
Brookfield Properties

SARAH CRAIGHEAD
Proofreader

MARK LISTEWNIK
Acquisitions Editor, Butterworth–Heinemann

GEORGE MORRISON
Project Manager, Butterworth–Heinemann

KELLY MABIE
Associate Production Editor
Graphic World Publishing Services

This Page Intentionally Left Blank

Come, let us build for ourselves a city, and a tower whose top will reach into heaven.

—GENESIS 11:4

This Page Intentionally Left Blank

1 *High-Rise Building Definition, Development, and Utilization*

Before entering the world of high-rise security and fire life safety, it is important to define what constitutes a *high-rise building* and to review the development and utilization of these unique structures.

What is a High-Rise Building?

A *high-rise building*[*] is defined by the National Fire Protection Association (NFPA) 101, *Life Safety Code*, as ''a building greater than 75 feet (23 meters) in height where the building height is measured from the lowest level of fire department vehicle access to the floor of the highest occupiable story'' (Section 3.3.25.6, 2000).

''Generally, a *high-rise structure* is considered to be one that extends higher than the maximum reach of available fire-fighting equipment. In absolute numbers, this has been set variously between 75 and 100 feet'' (POA, 2000, p. 19-100), or about seven to ten stories. The exact height above which a particular building is deemed a high-rise is specified by the fire and building codes in the area in which the building is located. When the building exceeds the specified height, then fire, an ever-present danger in such facilities, must be fought by fire personnel from inside the building rather than from outside using fire hoses and ladders.

Development of High-Rise Buildings

The origin of high-rise buildings is deeply rooted in world history. According to the Old Testament, after the Flood, people wanted to make a name for themselves by building a city with a tower that reached into heaven. The tower was constructed using brick for stone, and tar for mortar. God scattered these people over the face of the earth, and they stopped building. In the Roman Empire, during the reigns of Julius and Augustus Caesar, there were a large number of hurriedly constructed apartment buildings in the city of

[*]A *building* is an enclosed structure that has walls, floors, a roof, and usually windows.

Rome itself—many of which were built to considerable heights. Collapse of these buildings due to structural failure was common and led to laws limiting building heights—initially to 70 feet (21.3 meters) and then 60 feet (18.2 meters) (Cote, 1997, p. 1-42). Throughout subsequent history there have been other tall structures—pyramids and towers, castles and cathedrals—but it was not until the middle of the nineteenth century that the *skyscraper*[*] was born.

More than 150 years ago, cities looked very different from the way they look today. The buildings that housed people and their businesses were rarely taller than the height of a flagpole. Urban landscapes tended to be flat and uniform in pattern, apart from church steeples, temples, town halls, and monuments. Two major developments led to the skyscrapers that dominate major city skylines throughout the modern world:

1. In 1853 an American, Elisha Graves Otis, invented the world's first safety lift or elevator.[†] This new form of transportation enabled people to travel safely upward at a much greater speed and with considerably less effort than by walking.
2. In the 1870s, steel frames became available, gradually replacing the weaker combination of cast iron and wood previously used in construction. Until then, the walls had to be very thick to carry the weight of each floor.

> It usually was agreed that a 12-inch wall was needed to support the first story, and four inches had to be added to the thickness of the base to support each additional story. The depth-to-height ratio precluded building structures above 10 stories. (An exception was the 16-story Monadnock Building in Chicago, built in 1889 to 1891. Still standing, it is the last great monument to the age of load-bearing walls. At their base, the Monadnock Building's walls are six feet thick.) (Institute of Real Estate Management [IREM], 1985, p. 3) (Figure 1.1)

Steel frames were able to carry the weight of more floors, so walls became simply cladding for the purpose of insulating and adorning the building. This development, which included applying hollow clay tiles to the steel supports, resulted in a fireproof[‡] steel skeleton and ''also permitted movable interior partitioning, which allowed office suites to be reconstructed to meet the demands of new tenants'' (IREM, 1985, p. 3). ''This new method of

---

[*]The meaning of the term *skyscraper* has changed drastically since the first appearance of tall buildings. Obviously, the term itself implies something that ''scrapes the sky.'' Originally, a building of ten stories was considered a skyscraper, but today the word is seldom used to describe a building of less than fifty stories (Sonder, 1999, p. II).

[†]''Otis hadn't invented the first hoist. But he had invented the first 'safe' hoist. . . . People had been building hoists of various kinds for hundreds of years. And they all had the same serious defect: they plunged to the bottom every time the lifting cable snapped,'' (Otis Elevator Company, 1974, pp. 8, 10). ''In front of a crowd of spectators and journalists at the Crystal Palace of New York Exhibition [in 1854], he [Elisha Graves Otis] cut the cable of his elevator, which locked in place and did not fall. This rack and pinion safety lock which operates between the guiding rails and the elevator if it moves too fast, is still in use today'' (Mierop, 1995, pp. 70–71). Otis elevators were first constructed for freight purposes. The world's first passenger elevator was installed in 1857 by Otis in the five-story store of E.V. Haughwout & Company in New York City (Otis Elevator Company, 1974, p. 11).

[‡]''A fireproof building will minimize the destruction of fire, whenever it strikes. In order to be termed *fireproof*, a building must offer 100% fire protection. Fireproof does not mean the absence of fire. It simply refers to proper building design and detail that effectively checks the spread of fire, while allowing access for occupants to escape'' (Kruse, 1993, p. 12).

Figure 1.1 Monadnock building. This 16-story building is the tallest load-bearing brick structure in the world. At their base, the building walls are 6 feet thick. Courtesy of the Chicago Historical Society.

construction reduced the thickness of walls, increased valuable floor space, and because it weighed much less than masonry, allowed immense increases in height. Freed from the constraints of traditional construction, the facade could now be opened with windows to maximize the amount of daylight reaching the interior of the building'' (Dupre, 1996, p. 15).

Another factor that helped to make high-rises possible was the very foundation upon which they stood. ''The Egyptian method of spread footings didn't work for skyscrapers since too much weight would bear down on too small an area. Modern builders had to switch to another ancient method, the Roman use of piles, which were driven into the ground all the way to the bedrock'' (Sonder, 1999, p. 15) to provide a strong supporting base.

According to the Institute of Real Estate Management (1985, pp. 2, 15), ''The modern office building was created in response to rapid population increases and industrialization that occurred during the late nineteenth century. Between 1870 and 1920, the nation's population doubled, and demand for office space increased fivefold. The first commercial structures were in the East, but with railroads and a dynamic economy spurring national expansion, office buildings soon appeared in the Midwest, particularly in Chicago. In 1871, a fire destroyed this city. The disaster, combined with increased urban land values, the invention of the elevator, and the development of structural steel, gave rise to the skyscraper.''

Other developments, such as incandescent lamps, central heating, and forced-air ventilation, followed in the twentieth century by fluorescent lights and air-conditioning,[*] addressed the issue of providing adequate lighting, heating, ventilation, and air-conditioning in large buildings. Such advancements in technology have not significantly affected the design of high-rise buildings but have contributed to their use being more convenient and comfortable (Mierop, 1995, p. 60).

High-Rises Arise

The 10-story Home Insurance Building, built in Chicago in 1885, is generally considered to be the world's first skyscraper.[†] Engineer William Le Baron Jenney designed this 180-feet (55 meters) tall building using a steel frame to support the weight of the structure. Jenney stated in 1883, ''we are building to a height to rival the Tower of Babel'' (Dupre, 1996, p. 14) (Figure 1.2).

At the turn of the century, tall buildings began to spring up in New York City—in 1903, the triangular-shaped 22-story Flatiron (Fuller) Building, 285 feet (87 meters) high; in 1909, the 50-story Metropolitan Life Insurance Building, 700 feet (213 meters) high; and in 1913, the 57-story Woolworth Building, 792 feet (241 meters) high.

[*] Central ''air-conditioning became widespread in office buildings in the 1950s'' (Gillespie, 1999, p. 207).

[†] ''The Equitable Building was New York's only challenge to Chicago's claim to the first skyscraper. Built in 1870, it was . . . . only six stories tall'' (Bennett, 1995, p. 41).

Figure 1.2 Home Insurance Building. This 10-story building, designed by engineer William Le Baron Jenney, is generally considered the world's first skyscraper. Built in Chicago in 1885 using a steel frame, it was demolished in 1931. Courtesy of the Chicago Historical Society.

The first modern residential skyscraper, the 41-story Ritz Tower (540 feet, 165 meters), was constructed in New York in 1926. This tower ''rapidly became the prototype for a new lifestyle. Half hotel, half apartment block, it was particularly suited to the nomadic world of business and to people who were already deciding to move to the country and to maintain only a pied-a-terre in town. . . . By the early thirties New York had about 150 buildings of this type'' (Mierop, 1995, pp. 85–86).

In 1930 and 1931, two of the tallest buildings in the world were constructed in New York City: the 77-story Chrysler Building (1046 feet, 319 meters) and the 102-story Empire State Building (1250 feet, 381 meters). The latter, considered the ''Eighth Wonder of the World,'' was built in the record time of 1 year and 45 days (Wright, January 2002, p. 18). Both the Chrysler Building and the Empire State Building eclipsed the Woolworth Building as the world's tallest skyscrapers. After these buildings were erected, 40-, 50-, and 60-story structures were built all over the United States.

In 1969, the 100-story John Hancock Center (1127 feet, 344 meters) was built in Chicago. This mixed-use skyscraper has over 700 apartments on the highest floors, office space on floors below, and amenities such as shops, a restaurant, a swimming pool, a skating rink, and an underground plaza (Mierop, 1995, p. 78).

From 1970 to 1990, there were a combined total of 2273 new construction starts of buildings eight stories or higher in the major metropolitan areas of New York, Chicago, and Los Angeles (Dodge, 1991, p. 1). Two of these buildings were the 110-story Twin Towers of the New York World Trade Center (WTC): the north tower, One World Trade Center (WTC 1), 1368 feet (417 meters), was completed in 1972; and the south tower, Two World Trade Center (WTC 2), 1362 feet (415 meters), was completed in 1973. At that time, the WTC towers were the tallest buildings in the world (taking the title from the Empire State Building, which for over 40 years was the world's tallest building). In 1974, the world's tallest building became the Sears Tower. Located in Chicago, it has 110 floors, beginning at street level and ending 1450 feet (442 meters) in the air.

The ''World's Tallest'' Race

In 1972, the Council on Tall Buildings and Urban Habitat first compiled a list of ''The One Hundred Tallest Buildings in the World'' (LeHigh University, Bethlehem, Pennsylvania, United States). The following information was obtained from the current list (see Appendix 1-1).

Currently, Petronas Towers in Kuala Lumpur, Malaysia, built in 1998, with each 88-story tower 1483 feet (452 meters) high, connected at the 41st and 42nd floors by a glass-enclosed pedestrian ''skybridge,'' are the tallest buildings in the world.* The next tallest is the 110-story Sears Tower at 1450 feet

*''Petronas Tower holds the title of the world's tallest building measured in terms of architectural height, rising 1483 feet (452 meters) to its structural top. . . . The Sears Tower retains the title of the world's tallest building in three of four categories. It has the highest occupied floor: 1431 feet

(442 meters), followed by the 88-story, 1381 feet (421 meters), Jin Mao Building located in Shanghai, China.

This list indicates that 48 of the structures, almost one-half, are located outside of the United States. Cities such as Kuala Lumpur, Shanghai, Guangzhou, Shenzhen, Hong Kong, Dubai, Kaohsiung, Bangkok, Pyongyang, Frankfurt, Yokohama, Riyadh, Toronto, Singapore, Osaka, Jakarta, Seoul, Melbourne, Nagoya, Taipei, Tokyo, Makati, Moscow, Caracas, and London all have structures that qualify for the elite 100.

Other skyscrapers in Asia will soon surpass Petronas Towers as holder of the world's tallest building title. Presently under construction are the 88-story, 1516 feet (462 meters), Suyong Bay Tower in Pusan, South Korea; the 90-story, 1518 feet (463 meters), Shanghai World Financial Center in Shanghai, China; and Jakarta Tower in Jakarta, Indonesia. When Jakarta Tower is completed it will stand 1806 feet (558 meters) tall.

On the drawing board, the tallest building in the world is Illinois Tower, a 528-story, 5280-foot (1610 meters) office building. In 1956, architect Frank Lloyd Wright conceived this ''mile-high'' office building with the intention of it being constructed on Chicago's lakefront (Fortune, 1992, p. 87).

Three Generations of High-Rise Buildings

Since the first appearance of high-rise buildings, there has been a transformation in their design and construction. This has culminated in glass, steel, and concrete structures in the International and Postmodernist styles of architecture prevalent today.

The following information, adapted largely from *High Rise/Fire and Life Safety* by the late John T. O'Hagan, former fire commissioner and chief of the New York City Fire Department (O'Hagan, 1977, pp. 145, 146), describes three generations of high-rise buildings in the United States since their inception.

First Generation

The exterior walls of these buildings consisted of stone or brick, although sometimes cast iron was added for decorative purposes. The columns were constructed of cast iron, often unprotected; steel and wrought iron were used for the beams; and the floors were made of wood. ''In a fire, the floors tend to collapse, and the iron frame loses strength and implodes'' (Seabrook, 2001, p. 66). Elevator shafts were often unenclosed. The only means of escape from a floor was through a single stairway usually protected at each level by a metal-plated wooden door. There were no standards for the protection of steel used in the construction of these high-rises.

(436 meters). It has the highest roof in the world, at 1450 feet (442 meters). And it is the tallest building when measured to the uppermost reaches of its antenna or spire system: 1730 feet (527 meters)'' (Fickes, 2000).

Second Generation

''The second generation of tall buildings, which includes the Metropolitan Life Building (1909), the Woolworth Building (1913), and the Empire State Building (1931), are frame structures, in which a skeleton of welded- or riveted-steel columns and beams, often encased in concrete, runs through the entire building. This type of construction makes for an extremely strong structure, but not such attractive floor space. The interiors are full of heavy, load-bearing columns and walls'' (Seabrook, 2001, p. 66).

As Brannigan (1992, pp. 458, 459) describes them, these

> Pre-World-War II buildings were universally of steel-framed construction. Floor construction and fireproofing of steel were often of concrete or tile, both good heat sinks and slow to transmit heat to the floor above. The construction was heavy but no feasible alternative existed.
>
> Relatively small floor areas were dictated by the need for natural light and air. Advertisements for the RCA Building in New York proclaimed, ''no desk any farther than 35 feet from a window.'' This limited both the fire load and the number of occupants. . . . The typical office was quite spartan, though executive suites and eating clubs often were paneled with huge quantities of wood. Nevertheless, most fire loads[*] were low.
>
> Windows could be opened in buildings of this era. This provided local ventilation and relief from smoke migrating from the fire. The windows leaked, often like sieves, therefore there was no substantial stack effect.[†]

In this generation of buildings, developments such as the following occurred:

- The use of noncombustible construction materials that reduced the possibility of the collapse of structural members during a fire.
- The inclusion of assemblies rated for a particular fire resistance. (*Assemblies* are barriers that separate areas and provide a degree of fire resistance determined by the specific fire resistance rating of the assembly itself. An assembly may consist of a floor, ceiling, wall, or door.)
- The enclosure of vertical shafts with protected openings.
- The use of compartmentation. (*Compartmentation* involves the use of walls, floors, and ceilings to create barriers against the spread of smoke and fire.)

Third Generation

Buildings constructed after World War II until today comprise the most recent generation of high-rise buildings. Within this generation are two types of high-rises—those of *core construction* and those of *tube construction*.

[*] *Fire load* or *fuel load* is defined by the Fire Safety Institute as, ''the amount of material that is contained in a building, including both contents and combustible parts of the structure'' (Abbott, 1994, p. 3-59). Included in the contents are office furniture and furnishings such as draperies, curtains, carpets, and mats.

[†] ''*Stack effect* results from the temperature differential between two areas, which creates a pressure differential that results in natural air movements within a building. In high-rise buildings, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke uncontrolled through the building'' (Caldwell, 1997, p. 9-18).

Core Construction

These structures are built of lightweight steel or reinforced concrete frames, with exterior all-glass curtain walls, as Salvadori (1980) states: ''The so-called *curtain walls* of our high-rise buildings consist of thin, vertical metal struts or *mullions*, which encase the large glass panels constituting most of the wall surface. The curtain wall, built for lighting and temperature-conditioning purposes, does not have the strength to stand by itself and is supported by a frame of steel or concrete, which constitutes the structure of the building'' (p. 22). The majority of high-rise buildings are steel-framed rather than of reinforced concrete construction.

In the center of these buildings, or infrequently to the side, is an inner load-bearing core constructed of steel or reinforced concrete. Most building utilities and services—stairway shafts (stairwells); passenger and service elevator shafts; air-conditioning supply and return shafts; telecommunication systems; water, electrical power, and gas utilities; and rest rooms—are enclosed in this central core. The core braces the building against wind.

Tube Construction

Tube structures represented a change in the design of steel-frame buildings to enable them to be built very tall and yet remain strong enough to resist the lateral forces of winds and the possible effects of an earthquake. Tube construction used load-bearing exterior or perimeter walls to support the weight of the building.

''The key to stability is a resistance to lateral wind or earthquake forces, which grow dramatically in magnitude with the building's height'' (Salvadori, 1980, p. 116). ''If not counteracted by proper design, these forces would cause a tall building to slide on its base, twist on its axis, oscillate uncontrollably, bend excessively or break in two'' (Tucker, 1985, p. 70). As explained by Mierop (1995, pp. 60, 63)

> The height of a skyscraper has always been determined by the capacity of its structure to resist the lateral forces of wind and earthquake; 15 to 20 stories for a steel framework system made rigid by masonry walls; up to 60 stories, 200 meters (650 feet) high for a steel framework system made rigid by a load-bearing core, 30 meters (100 feet) wide; higher still with a bigger core, but this would be to the detriment of the economic viability of the building [since the amount of leaseable floor space would be reduced].
>
> When the structural role is shifted from the core to the outside walls of the building, resistance is increased together, proportionally, with possible height. . . . This system of load bearing exterior walls or ''tube structure''* was developed in the early sixties in the academic context of the Illinois Institute of Technology (IIT) by engineers Myron Goldsmith and Fazlur Khan, both of the Skidmore, Owings & Merrill Chicago Office. No spectacular advance has subsequently revolutionized the skyscraper from a structural point of view.

*''When the exterior walls are made rigid the building behaves like a huge hollow tube. As the interior columns no longer have to resist lateral pressure their position becomes optional and the floor layout more flexible'' (Mierop, 1995, p. 74).

> The best-known example of tube structure is the World Trade Center. . . . The walls of the towers are made up of a rigid lattice of closely spaced columns and beams, defining narrow windows.*

"Because the core and perimeter columns carry so much of the load, the designers could eliminate interior columns, with the result that there is more open floor space for tenants" (Seabrook, 2001, p. 66). Floor areas tend to be larger, with little compartmentation using floor-to-ceiling walls and barriers.

Utilization of High-Rise Buildings

The use or function of a building has considerable influence on fire life safety. As long as high-rise buildings have existed, the risk of fire occurring in them has been of special concern to building architects, structural engineers, fire protection engineers, code officials, owners, managers, fire safety directors, fire service personnel, and, of course, tenants.

Types of High-Rise Buildings

With reference to high-rise buildings, "in terms of reported fires, there are actually four property classes that dominate the statistics. Office buildings and hotels and motels are among them, but so are apartment buildings and hospitals (and other facilities that care for the sick)" (Hall, 2001, p. 3). Primarily, this book addresses high-rise office buildings; however, in the final chapter, the fire life safety of these other occupancies is discussed.

Types of Tenancy and Pattern of Use

"The types of building tenancy and the pattern of use are [also] important factors to consider when we plan and carry out a security program. A building can be (1) single-tenant/single-use, (2) single-tenant/multiple-use, (3) multiple-tenant/single-use, or (4) multiple-tenant/multiple-use" ("Introduction," *Commerical Building Security*, 1980, p. 3).

A *single-tenant/single-use* building is occupied by one particular tenant† and is used solely for one type of business—for example, a bank building where the business of that bank alone is conducted. A *single-tenant/multiple-use* building, however, is occupied by one particular tenant who uses the building not only for one type of business but also for other purposes. An example would be a

*"The World Trade Center used an innovative construction technique. The exterior walls carry the weight of the structure as well as providing bracing against the stress and strain of lateral winds. The entire building perimeter acts as a strong tube. The outer wall consists of closely spaced vertical columns" (Gillespie, 1999, p. 167).

†A *tenant* can be a person, a group of persons, or a company that rents and occupies space within a building. Throughout this book, the term generally refers to a business leasing space in a high-rise building.

bank building that has parking facilities, restaurants, or retail outlets open to the public.

A *multiple-tenant/single-use* building is occupied by more than one tenant, each of whom uses the building to conduct a similar type of business—for example, a medical office building where tenants conduct medical-related business. A *multiple-tenant/multiple-use* building is occupied by more than one tenant, each of whom conducts business not necessarily related to the other businesses. An example would be a commercial office building that includes law firms, public utilities or agencies, management consultants, and financial institutions.

Most of the high-rise buildings used as examples in this book are multiple-tenant/multiple-use structures used for commercial office purposes. The hypothetical high-rise Pacific Tower Plaza, later described in this book, is a 36-story building with a triple-level under-building parking garage, located in a major downtown financial district.

There are two types of structures commonly associated with buildings that technically are classified as high-rises, but usually are not required to conform to high-rise building laws, codes, and standards (particularly the laws requiring the installation of approved automatic sprinkler systems). These structures are (1) buildings used solely as open parking structures, and (2) buildings where all floors above the high-rise height limit are used for open parking.

Summary

Since their first appearance in the latter part of the nineteenth century, high-rise buildings have changed considerably in their design and construction. When designing a security and fire life safety program for any high-rise building, its use and type of tenancy are essential factors to consider. Primarily, this book addresses high-rise office buildings; however, other high-rise occupancies are also discussed.

References

Abbott, Richard J., ''Lesson 3,'' *Fire Science Institute Office Buildings Fire Safety Directors Course* (212/237-8650, New York, 1994).

Bennett, David, ''Soaring ambitions,'' *Skyscrapers: Form and Function* (Simon & Schuster, New York, copyright by Marshall Editions Developments Limited, 1995).

Brannigan, Francis L., *Building Construction for the Fire Service*, 3rd ed. (National Fire Protection Association, Quincy, MA, 1992).

Caldwell, Carol, ''Occupancies in special structures and high-rise buildings,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Cote, Arthur E., and Casey C. Grant, ''Building and fire codes and standards,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Council on Tall Buildings and Urban Habitat, *The One Hundred Tallest Buildings in the World* (LeHigh University, Bethlehem, PA, 2002).

Dupre, Judith, *Skyscrapers* (Black Dog & Leventhal Publishers, Inc., New York, First Black Dog & Leventhal Paperbacks edition, 2001).
Dodge, F. W., and National Information Services, as reported in the *Fire Protection Planning Report*, ''Fundamentals of firesafety in high-rise buildings'' (Concrete and Masonry Industry Firesafety Committee, Skokie, IL, November 1991).
Fickes, Michael, ''New security heights'' (*Access Control & Security Systems Magazine,* Atlanta, March 1, 2002).
Fortune, James W., ''Wright to the top.'' Adapted from a paper presented at the International Association of Elevator Engineers' Elevcon '92 conference; first published in *Elevator Technology* (*The Construction Specifier,* September 1992).
Gillespie, Angus Kress, ''Architecture,'' *Twin Towers: The Life of New York's World Trade Center* (Rutgers University Press, Piscataway, NJ, 1999).
Gillespie, Angus Kress, ''A city within a city,'' *Twin Towers: The Life of New York's World Trade Center* (Rutgers University Press, Piscataway, NJ, 1999).
Hall, John R., Jr., ''High-rise building fires,'' (National Fire Protection Association, Quincy, MA, September 2001).
Institute of Real Estate Management of the National Association of Realtors, ''Office building industry: past, present, and future,'' *Managing the Office Building*, revised ed. Revisions author, Ronald A. Harris (IREM, Chicago, 1985).
''Introduction,'' *Commercial Building Security: The Notebook Lesson Series for Security Officers* (American Protective Services, Inc., Oakland, CA, 1980).
Kruse, Tom, ''Designing fireproof buildings'' (*Skylines Magazine,* BOMA International, Baltimore, March 1993).
Mierop, Caroline, *Skyscraper Higher and Higher*, (Institut Francais D'Architecture, Paris, France, 1995).
NFPA 101, ''Chapter 3 Definitions,'' *Life Safety Code*, Section 3-3.25.6 (National Fire Protection Association, Quincy, MA, 2000).
O'Hagan, John T., *High Rise/Fire and Life Safety*, 2nd printing (Fire Engineering, A PennWell Publication, Saddle Brook, NJ, 1977).
Otis Elevator Company, *Tell Me About Elevators* (Otis Elevator Company, Farmington, CT, 1974).
POA, ''High-rise structures, Section A, Life safety considerations,'' *Protection of Assets Manual*, vol. III. Editor, Timothy L. Williams (Used with permission of POA Publishing, LLC, Los Angeles, CA, 2000, 323/663-4887.
Salvadori, Mario, *Why Buildings Stand Up: The Strength of Architecture* (W. W. Norton, New York, 1980).
Seabrook, John, ''The Tower Builder: why did the World Trade Center buildings fall down when they did?'' (*The New Yorker,* New York, November 19, 2001).
Sonder, Ben, *Skyscrapers* (MetroBooks, by Michael Friedman Publishing Group, Inc., New York, 1999).
Tucker, Jonathan B., ''Superskyscrapers,'' *High Technology*, vol. 5, No. 1, January 1985, as quoted in *Skyscraper Higher and Higher*, by Caroline Mierop (Institut Francais D'Architecture, Paris, France, 1995, p. 60).
Wright, Leigh Martinez, ''Spiders in the sky,'' *Smithsonian* (Palm Coast, FL, January 2002).

Additional Reading

Brannigan, Francis L., *Building Construction for the Fire Service*, 3rd ed. (National Fire Protection Association, Quincy, MA, 1992).

Klaene, Bernard J., ''Ben,'' and Russell E. Sanders, *Structural Fire Fighting* (National Fire Protection Association, Quincy, MA, 2000).

O'Hagan, John T., former Fire Commissioner and Chief of the New York City Fire Department, *High Rise/Fire and Life Safety*, 2nd printing (Fire Engineering, A PennWell Publication, Saddle Brook, NJ, 1977).

Appendix 1-1 The One Hundred Tallest Buildings in the World*

Rank	Building	City	Year	Stories	Height† (m)	Height† (ft)	Material	Use
1	Petronas Tower 1	Kuala Lumpur	1998	88	452	1483	Mixed	Multiple
2	Petronas Tower 2	Kuala Lumpur	1998	88	452	1483	Mixed	Multiple
3	Sears Tower	Chicago	1974	110	442	1450	Steel	Office
4	Jim Mao Building	Shanghai	1999	88	421	1381	Mixed	Multiple
5	Citic Plaza	Guangzhou	1996	80	391	1283	Concrete	Multiple
6	Shun Hing Square	Shenzhen	1996	69	384	1260	Mixed	Office
7	Empire State Building	New York	1931	102	381	1250	Steel	Office
8	Central Plaza	Hong Kong	1992	78	374	1227	Concrete	Office
9	Bank of China	Hong Kong	1989	70	369	1209	Mixed	Office
10	Emirates Tower One	Dubai	1999	55	355	1165	Mixed	Multiple
11	The Center	Hong Kong	1998	79	350	1148	Steel	Office
12	T & C Tower	Kaohsiung	1997	85	348	1140	Steel	Multiple
13	Aon Centre	Chicago	1973	80	346	1136	Steel	Office
14	John Hancock Center	Chicago	1969	100	344	1127	Steel	Multiple
15	Burj al Arab Hotel	Dubai	1999	60	321	1053	Mixed	Hotel

16	Baiyoke Tower II	Bangkok	1997	90	320	1050	Concrete	Hotel
17	Chrysler Building	New York	1930	77	319	1046	Steel	Office
18	Bank of America Plaza	Atlanta	1993	55	312	1023	Mixed	Multiple
19	Library Tower	Los Angeles	1990	75	310	1018	Mixed	Office
20	Telekom Malaysia Headquarters	Kuala Lumpur	1999	55	310	1017	N/A	Office
21	Emirates Tower Two	Dubai	2000	56	309	1014	Concrete	Hotel
22	AT&T Corporate Center	Chicago	1989	60	307	1007	Mixed	Office
23	Chase Tower	Houston	1982	75	305	1000	Mixed	Office
24	Two Prudential Plaza	Chicago	1990	64	303	995	Concrete	Office
25	Pyongyang Hotel	Pyongyang	1995	105	300	984	Concrete	Hotel
26	Commerzbank Tower	Frankfurt	1997	63	299	981	Mixed	Office
27	Wells Fargo Plaza	Houston	1983	71	296	972	Steel	Office
28	Landmark Tower	Yokohama	1993	70	296	971	Steel	Multiple
29	311 South Wacker Drive	Chicago	1990	65	293	961	Concrete	Office
30	Kingdom Centre	Riyadh	2001	72	292	958	Concrete	Office
31	SEG Plaza	Shenzhen	2000	72	292	957	N/A	Multiple
32	Bank of America Center	Seattle	1984	76	291	954	Mixed	Office

continued

Appendix 1-1 *continued*

Rank	Building	City	Year	Stories	Height† (m)	Height† (ft)	Material	Use
33	American International Building	New York	1932	67	290	952	Steel	Office
34	Cheung Kong Center	Hong Kong	1999	70	290	951	Steel	Office
35	First Canadian Place	Toronto	1975	72	290	951	Steel	Office
36	Key Tower	Cleveland	1991	57	290	950	Mixed	Office
37	One Liberty Place	Philadelphia	1987	61	288	945	Steel	Office
38	Plaza 66	Shanghai	2001	66	288	945	Concrete	Multiple
39	Sunjoy Tomorrow Square	Shanghai	1999	59	285	934	N/A	N/A
40	The Trump Building	New York	1930	72	283	927	Steel	Office
41	Bank of America Plaza	Dallas	1985	72	281	921	Mixed	Office
42	Overseas Union Bank Centre	Singapore	1986	66	280	919	Steel	Office
43	United Overseas Bank Plaza	Singapore	1992	66	280	919	Steel	Office
44	Republic Plaza	Singapore	1995	66	280	919	Mixed	Office
45	Citicorp Center	New York	1977	59	279	915	Steel	Multiple
46	Scotia Plaza	Toronto	1989	68	275	902	Mixed	Office

47	Williams Tower	Houston	1983	64	275	901	Steel	Office
48	Al Faisaliah Centre	Riyadh	2000	30	274	899	Mixed	Multiple
49	Renaissance Tower	Dallas	1975	56	270	886	Steel	Office
50	Trump World Tower	New York	2001	72	267	881	Concrete	Residential
51	900 North Michigan Avenue	Chicago	1989	66	265	871	Mixed	Multiple
52	NationsBank Corporate Center	Charlotte	1992	60	265	871	Concrete	Office
53	SunTrust Plaza	Atlanta	1992	60	265	871	Concrete	Office
54	Hong Kong New World Building	Shanghai	2001	58	265	871	Steel	Multiple
55	BCE Place-Canada Trust Tower	Toronto	1990	51	263	863	Mixed	Office
56	Water Tower Place	Chicago	1976	74	262	859	Concrete	Multiple
57	First Interstate Tower	Los Angeles	1974	62	262	858	Steel	Office
58	Transamerica Pyramid	San Francisco	1972	48	260	853	Mixed	Office
59	GE Building, Rockefeller Center	New York	1933	70	259	850	Steel	Office
60	First National Plaza	Chicago	1969	60	259	850	Steel	Office
61	Two Liberty Place	Philadelphia	1990	58	258	848	Steel	Office
62	Park Tower	Chicago	2000	67	257	844	Concrete	Multiple

continued

Appendix 1-1 *continued*

Rank	Building	City	Year	Stories	Height† (m)	Height† (ft)	Material	Use
63	Messeturm	Frankfurt	1990	70	257	843	Concrete	Office
64	USX Tower	Pittsburgh	1970	64	256	841	Steel	Office
65	Rinku Gate Tower	Osaka	1996	56	256	840	N/A	Multiple
66	Osaka World Trade Center	Osaka	1995	55	252	827	Steel	Office
67	One Atlantic Center	Atlanta	1987	50	250	820	Mixed	Office
68	BNI City Tower	Jakarta	1995	46	250	820	Concrete	Office
69	Korea Life Insurance Company	Seoul	1985	60	249	817	Steel	Office
70	City Spire	New York	1989	75	248	814	Concrete	Multiple
71	Rialto Tower	Melbourne	1985	63	248	814	Concrete	Office
72	One Chase Manhattan Bank	New York	1961	60	248	813	Steel	Office
73	Bank One Tower	Indianapolis	1989	48	247	811	Steel	Office
74	Conde Nast Building	New York	1999	48	247	809	N/A	Office
75	MetLife	New York	1963	59	246	808	Steel	Office
76	JR Central Towers	Nagoya	2000	51	245	804	N/A	Multiple
77	Shin Kong Life Tower	Taipei	1993	51	244	801	Mixed	Office

78	Malayan Bank	Kuala Lumpur	1988	50	244	799	Concrete	Office
79	Tokyo Metropolitan Government	Tokyo	1991	48	243	797	Mixed	Office
80	Woolworth Building	New York	1913	57	241	792	Steel	Office
81	Mellon Bank Center	Philadelphia	1991	54	241	792	Mixed	Office
82	Philippine Bank of Communications	Makati	2000	52	241	791	Concrete	Office
83	John Hancock Tower	Boston	1976	60	240	788	Steel	Office
84	Bank One Center	Dallas	1987	60	240	787	Mixed	Office
85	Canadian Imperial Bank of Commerce	Toronto	1973	57	239	784	Mixed	Office
86	Moscow State University	Moscow	1953	26	239	784	Steel	Multiple
87	Empire Tower	Kuala Lumpur	1994	62	238	781	Mixed	Office
88	NationsBank Center	Houston	1984	56	238	780	Steel	Office
89	Bank of America Center	San Francisco	1969	52	237	779	Steel	Office
90	Office Towers	Caracas	1985	60	237	778	Mixed	Office
91	Worldwide Plaza	New York	1989	47	237	778	Steel	Office
92	First Bank Place	Minneapolis	1992	58	236	775	Mixed	Office
93	IDS Center	Minneapolis	1973	57	236	775	Mixed	Multiple

continued

Appendix 1-1 *continued*

Rank	Building	City	Year	Stories	Height† (m)	Height† (ft)	Material	Use
94	One Canada Square	London	1991	50	235	774	Steel	Office
95	Norwest Center	Minneapolis	1988	57	235	773	Steel	Office
96	Temasek Tower	Singapore	1986	52	235	771	Mixed	Multiple
97	191 Peachtree Tower	Atlanta	1992	50	235	770	Mixed	Multiple
98	Opera City Tower	Tokyo	1997	54	234	768	N/A	Multiple
99	Shinjuku Park Tower	Tokyo	1994	52	233	764	Steel	Multiple
100	Heritage Plaza	Houston	1987	52	232	762	Steel	Office

*The World Trade Center Twin Towers of New York City were on this list until their destruction on September 11, 2001.

†Height is measured from the sidewalk level of the main entrance to the structural top of the building.

2 *High-Rise Assets and Security and Fire Life Safety Threats*

High-Rise Assets

Assets in the high-rise setting may be tangible or intangible. Tangible assets include the people using the facility, the building itself, its fittings, and its equipment. This equipment consists of the electrical, gas, mechanical, heating, ventilating, air conditioning, lighting, elevator, escalator, communication, security, and life safety systems. In addition, within offices there is equipment such as telephones, computers, word processors, printers, typewriters, fax machines, photocopiers, audio-visual equipment, general-use items—coffee machines, vending machines, refrigerators, microwaves, ovens, and furniture—and sometimes antiques and works of art, cash, and negotiable instruments. Also, vehicles parked in the building's parking garage are tangible assets. Intangible assets include the livelihood of building users; intellectual property and information stored in paper files, reference books, photographs, microfilm, x-rays, and within computer systems and peripherals; and the reputation and status of the facility, including the ability of tenants to conduct business.

Security and Fire Life Safety Threats

For the purposes of discussion, and to address issues in a systematic way, this book treats security and fire life safety in high-rise structures as two different disciplines. However, at times these subjects are so closely interwoven that they appear to be the same. Before identifying security and fire life safety threats to high-rise buildings, it is important to understand what these terms mean.

What Is Security?

Security is a noun derived from the Latin word *securus*, which means ''free from danger'' or ''safe.'' The *New Webster Dictionary* defines *security* as ''the

Note: The definitions of security and fire life safety threats were largely derived from *Black's Law Dictionary*, 6th ed., by the Publisher's Editorial Staff. Co-authors Joseph R. Nolan and Jacqueline M. Nolan-Haley. (Used with permission of West Publishing, St. Paul, 1990.)

state of being secure; confidence of safety; freedom from danger or risk; that which secures or makes safe; something that secures against pecuniary loss.'' Fischer and Green (1998, p. 3) write, ''Security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury.''

Public security involves the protection of the lives, property, and general welfare of people living in the public community. This protection is largely achieved by the enforcement of laws by police funded by public monies.

Private security, on the other hand, involves the protection of the lives and property of people living and working within the private sector. The primary responsibility for achieving this rests on an individual, the proprietor of a business employing an individual, the owner or agent of the facility where a business is conducted, or an agent of the aforementioned who specializes in providing protective services. As Post and Kingsbury state, ''In providing security for specific applications, the purpose of private security may be described as providing protection for materials, equipment, information, personnel, physical facilities, and preventing influences that are undesirable, unauthorized, or detrimental to the goals of the particular organization being secured'' (1991, p. 1).

What Is Fire Life Safety?

Safety is a noun derived from the Latin word *salvus*, which means safe (salvation is also from this root). The *New Webster Dictionary* defines *safety* as ''the state or quality of being safe; freedom from danger.'' Obviously, there is very little distinction between the terms security and safety. Fire life safety, fire and life safety, fire safety, and life safety are four synonymous terms commonly in use in relation to high-rise structures.

What Is a Threat?

A threat is any event that, if it occurs, may cause harm to or destruction of assets.

Security Threats

In the high-rise setting, security threats come in many forms. Threats to people include:

- *Murder*—the unlawful killing of a human by another with malice aforethought, either express or implied.
- *Manslaughter*—the unjustifiable, inexcusable, and intentional killing of a human without deliberation, premeditation, and malice.
- *Robbery*—felonious taking of money, personal property, or any other article of value in the possession of another, from his or her person or immediate presence, and against his or her will, accomplished by means of force or fear.

- *Assault*—any willful attempt or threat to inflict injury on the person of another. An assault may be committed without actually touching, striking, or doing bodily harm to another.
- *Assault and Battery*—any unlawful touching of another that is without justification or excuse.
- *Mayhem*—*Webster's College Dictionary* defines *mayhem* as, "the crime of willfully inflicting an injury on another so as to cripple or mutilate. Random or deliberate violence or damage." In many states, the crime of mayhem is treated as aggravated assault.
- *Sex Offenses* (including rape, sexual harassment, and lewd behavior)—rape is unlawful sexual intercourse with a female without her consent. Under some statutes, this crime may now include intercourse between two males. Sexual harassment is a type of employment discrimination that includes sexual advances, request for sexual favors, and other verbal or physical conduct of a sexual nature prohibited by federal law, and commonly by state statutes. Lewd behavior relates to morally impure or wanton conduct; indecent exposure is included.

Threats to property include:

- *Vandalism*—willful or malicious acts intended to damage or destroy property. Included among these acts is the use of graffiti. Often a sharp instrument, such as a key or pocket knife, is used to scratch initials, logos, or drawings, or graffiti is written using color markers, crayons, pencils, lipstick, or spray paint. In buildings, graffiti is commonly found in restrooms, on lockers, and on walls of elevator lobbies (particularly those of service or freight elevators), elevator cars, rest areas, and walls immediately adjacent to public pay phones.
- *Trespass*—any unauthorized intrusion or invasion of private premises or land of another. Criminal trespass is entering or remaining on or in any land, structure, or vehicle by one who knows he or she is not authorized or privileged to do so. This includes remaining on property after permission to do so has been revoked.
- *Burglary*—entering a vehicle or building or occupied structure (or separately secured or occupied portion thereof) with purpose to commit a crime therein, at a time when the premises are not open to the public and the perpetrator is not licensed or privileged to enter.
- *Larceny*—the unlawful taking and carrying away of property of another with the intent to appropriate it to use inconsistently with the owner's rights. Theft is a popular name for larceny. Larceny-theft includes offenses such as shoplifting, pocket-picking, auto theft, and other types of stealing during which no violence occurs.
- *Sabotage*—in commerce, sabotage includes the willful and malicious destruction of employer's property or interfering with the employer's normal operations, such as during a labor dispute. This act could also be perpetrated by a disgruntled employee or ex-employee seeking revenge or by a business competitor.
- *Espionage*—the crime of gathering, transmitting, or losing information regarding the national defense with intent or reason to believe that the information is to be used to injure the United States or to the advantage of any foreign nation; could also be perpetrated by a business competitor engaging in industrial espionage.
- *Arson*—the malicious burning of another's house. This definition has been broadened by some state statutes and criminal codes to include starting a fire

or causing an explosion with the purpose of (a) destroying a building or occupied structure of another; or (b) destroying or damaging any property, whether one's own or another's, to collect insurance for such loss. Other statutes include the destruction of property by other means.
- *Disorderly conduct* can be considered a threat to people or property depending on the nature of the offense.

Security threats to both people and property include fire, bombs, riots, civil disorder, hazardous materials, chemical and biological weapons, nuclear attack, and natural disasters. Some of these threats may involve terrorism. An *act of terrorism* means an activity that involves a violent act or an act dangerous to human life, or the threat to commit any crime of violence with the purpose to terrorize another or to cause evacuation of a building, place of assembly, or facility of public transportation, or otherwise to cause serious public inconvenience, or in reckless disregard of the risk of causing such terror or inconvenience.

Fire Life Safety Threats

In the high-rise setting, life safety threats include:

- Fires
- Workplace violence
- Hostage and barricade situations
- Medical emergencies
- Trip, slip, and falls
- Power failures
- Elevator malfunctions and entrapments
- Traffic accidents
- Labor disputes, demonstrations, riots, and civil disorder
- Bombs and bomb threats
- Hazardous materials, chemical and biological weapons, and nuclear attack
- Aircraft collisions
- Natural disasters

Again, some of these threats may involve terrorism. The September 11, 2001, attacks on the New York World Trade Center and the Pentagon using hijacked commercial aircraft, and the subsequent mailing of anthrax-tainted envelopes on the United States East coast, were acts of terrorism each using different means to carry out diabolical objectives.

''The most critical risks in high-rise structures include fire, explosion and contamination of life-support systems such as air and potable water supply. These threats can be actualized accidentally or intentionally and because they can propogate rapidly can quickly develop to catastrophic levels'' (POA, 2000, p. 19-98).

In addition to the aforementioned threats, an individual may exhibit aberrant behavior such as that caused by substance abuse. Such conduct may be a threat not only to the personal safety of the individual involved, but also to other persons.

There is also the chance that people may attempt to deliberately injure themselves or take their own lives. Because of the height of high-rise buildings, the possibility exists that people may jump, particularly if they are able to reach the roof.

High-rise buildings, particularly major ones, may attract people who view them as a means to gain attention for themselves. For example, protesters may attempt to drape large banners promoting their *raison d'être* over the front of a building, or daredevils may perform outlandish feats to achieve notoriety.

Summary

High-rise buildings contain many valuable assets. The terms security and fire life safety are synonymous but can be addressed separately for the purposes of systematic analysis and discussion. There are many potential security and life safety threats to the people who use these facilities on a daily basis and to the business, property, and information contained within them.

References

Black's Law Dictionary, 6th ed. (West Publishing, St. Paul, 1990).

Fischer, Robert J., and Gion Green, ''Origins and development of security,'' *Introduction to Security*, 6th ed. (Butterworth–Heinemann, Stoneham, 1998).

New Webster Encyclopedic Dictionary of the English Language, 1980 Edition, Editor-in-Chief, Virginia S. Thatcher (Consolidated Book Publishers, Chicago).

POA, ''High-rise structures, Section A, Life safety considerations,'' *Protection of Assets Manual*, vol. III. Editor, Timothy J. Walsh (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887, 2000).

Post, Richard S., and Arthur A. Kingsbury, ''What is security?'' *Security Administration: An Introduction to the Protective Services*, 4th ed. (Butterworth–Heinemann, Boston, 1991).

Webster's College Dictionary, 1992 Edition (From Random House Webster's College Dictionary by Random House, Inc. Copyright 1995, 1992, 1991, by Random House, Inc. Reprinted by permission of Random House, Inc., New York, 1992).

This Page Intentionally Left Blank

3 *Security and Fire Life Safety Uniqueness of High-Rise Buildings*

Security of High-Rise Buildings versus Low-Rise Buildings

From a security perspective, high-rise office buildings differ from low-rise buildings in two ways. First, the existence of multiple, occupied floors, one on top of another, means a higher concentration of occupants and therefore more personal and business property to be damaged or stolen compared with that in low-rise buildings. The potential for theft is increased by the fact that the concentration of property makes the site more attractive to a criminal; also, the greater the concentration of people, the better the chances of a thief's anonymity. Second, the more individuals assembled in one location at any one time, the higher the possibility is of one of these persons committing a crime against another. One of the difficulties in making the aforementioned statements* is the lack of crime pattern analyses for high-rise buildings. The incidence of crime in any building, whether it is a high-rise or low-rise, largely depends on the design and construction of the building itself, the neighborhood in which it resides, and the security program that is in place.

Note: All NFPA material in this chapter is used with permission from the National Fire Protection Association, Quincy, MA, 1997.

*Kitteringham (2001, p. 24), commenting in his Masters of Science in Security and Crime Risk Management thesis on these statements made in the first edition of this book, points out that ''previous studies involving low and high-rise residential buildings draw a correlation that the higher the building the higher the crime rate, however the author fails to provide data that would either prove or refute any of the statements he made in regard to commercial structures.'' Kitteringham defines ''*crime analysis* as a law enforcement agency function whereby data relating to crime [is] collected, collated, analyzed and disseminated . . . .*crime pattern analysis* is a process that encompasses a number of techniques, all of which can assist crime risk management. It is therefore best regarded as a generic term, covering a number of approaches and techniques for analyzing the incidence and distribution of crime'' (2001, p. 12).

Fire Life Safety of High-Rise Buildings versus Low-Rise Buildings

From a fire life safety perspective, high-rise buildings differ from low-rise buildings in the following ways:

1. The existence of multiple, occupied floors, one on top of another, means a greater concentration of occupants and therefore a greater concentration of personal and business property; hence, a greater potential fuel load of the building.
2. The probability of a large uncontrolled fire moving upward is an ever-present danger in a high-rise building because it is a vertical structure.
3. The more individuals assembled in one location at any one time, the more likely it is that some of these people could be injured or killed, particularly by an incident occurring close to them.
4. Depending on the location of the incident, there may be a delay in reaching the area to provide assistance. For example, a medical emergency that occurs on the uppermost floor of a skyscraper will require considerably more travel time for the responding medical team than a similar incident occurring in a building lobby.
5. Evacuation of occupants when an emergency occurs is hampered by the fact that large numbers of people (sometimes hundreds, but possibly thousands) cannot all leave the structure at once via elevators and emergency exit stairwells.
6. Access by the fire department—from both outside and inside the building—may be restricted. According to the International Fire Service Training Association (IFSTA) (1976, pp. 57–60), external access may be limited by the following:

   - Setback of the building from public access roads and driveways; landscaping, berms, and fountains; and surfaces covering under-building or subterranean parking garages that will not support the weight of fire-fighting vehicles. These may restrict the proximity to the building that fire department aerial ladder apparatus can attain.
   - External features of the structure such as decorative walls, sunscreens, and building offsets (where an upper floor is set back from the floors beneath it) may inhibit the use of aerial ladders.
   - Fire department aerial ladders have a limited reach. ''The usual height limitation for aerial ladder operations is about 75 feet'' (Egan, 1978, p. 214).

   Internal access may be restricted to the use of stairwells and elevators that are approached through the building lobby or lower levels such as basements. Internal access may be complicated by the time required for fire department personnel to reach, and equipment to be transported to, an incident occurring in the upper levels of a structure.

   The effectiveness of the response to an incident, such as a fire, may be affected by the availability of fire department personnel and equipment—hoses, forcible entry tools, breathing apparatus, lights, and power supplies. Only the largest fire departments are able to provide the several hundred firefighters that may be necessary to control an advanced high-rise fire. The number of fire department staff required for response will depend on the type of tenancy and pattern of use of the building, the size and type of fire, its location within the structure, and whether an extensive search of the building needs to be conducted. Much of this information will be ascertained on-site, when fire department personnel have had an opportunity to evaluate the incident. ''Also, the delivery of personnel and equipment to the fire may be blocked by very hazardous falling glass which may cut hose lines and injure personnel. The glass hazard may make evacuation from the building impossible'' (Brannigan and Brannigan, 1995). Because modern high-rise building floors are often very large, interior hose lines run from stairwells by fire fighters may not reach every part of a floor.

7. According to Caldwell (1997, p. 9-18),

> The high-rise building often has natural forces affecting fire and smoke movement that are not normally significant in lower buildings. Stack effect and the impact of winds can be very significant, and very different, in high-rise buildings.
>
> The stack effect results from the temperature differential between two areas, which creates a pressure differential that results in natural air movements within a building. In high-rise buildings, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect capable of moving large volumes of heat and smoke uncontrolled through the building.
>
> No manual fire-fighting techniques are known to counter stack effect or to mitigate its effect during a fire.

Security of Modern High-Rise Buildings

The changes in the design and construction of high-rises since their first appearance have impacted the security needs of these facilities. Modern high-rise buildings have inherent security hazards different from those of the earliest high-rises because of the following:

- Open-style floors with little compartmentation and fewer individual offices that can be secured have made it easier for a potential thief to gain access to business and personal property. The advent of modern telecommunications with portable telephones, voice-mail, and answering services has meant that the presence of a tenant receptionist to screen persons entering the office is now not always the standard. The open-style floor has made it easier for an unauthorized person, having once gained access, to move unchallenged throughout the entire floor.
- The concealed space located above the suspended ceiling on each floor of many high-rises has provided a possible means of ingress to a tenant office. This space could also be used to hide unauthorized listening or viewing devices such as microphones or cameras. The central heating, ventilating, and air-conditioning (HVAC) system has provided a similar means for unauthorized listening and viewing.
- The higher number of occupants per floor in a modern high-rise means a greater concentration of business equipment and personal items and therefore a more desirable target for a potential thief.
- The greater number of occupants per floor means the increased potential for these individuals to be perpetrators or targets of a crime, and an increased

likelihood that some of these people could be injured or killed, particularly by an incident occurring close to them.

In addition to these changes, other factors have added to the security risks of modern high-rise buildings. For one thing, the tenant offices in modern high-rises are often the headquarters of highly successful corporations that have designed and furnished their places of business in a style to reflect their status. This has resulted in very high-quality furnishings, including, in some instances, expensive works of art and state-of-the-art business systems. The tenant employees themselves are generally well paid, often carry cash and valuables, and tend to drive and park expensive vehicles in the building parking garage. Hence, these facilities are a potential target for criminal activity.

Next, the computer revolution, with its proliferation of compact business machines (such as personal data assistants and personal and notebook computers), has resulted in equipment and proprietary information that can be carried away relatively easily by a potential thief. The computer has presented a unique set of risks because crimes can now be committed without the perpetrator ever setting foot on the premises where information is stored.

Finally, the development in the mid-1950s of completely automatic control systems for the operation of elevators eliminated the need for elevator attendants and, in effect, did away with an important access control and screening measure for high-rise buildings. With the elevator attendant gone, it is often possible for people to travel unchecked throughout a structure once they have entered an elevator. Such unchecked travel can be curtailed by the use of other security measures such as security personnel, locking off certain ''secured'' floors from elevator access, and the installation of modern electronic access control systems in elevator cars and lobbies.

The technological advances that have occurred in the security field, particularly over the past 40 years, have mitigated some of the aforementioned security risks. Centralized, microcomputer-based control of security and elevator systems has considerably extended and improved the application of basic security measures such as the following:

- Locks and locking systems
- Access control devices—electronic keypads, card readers, and biometric readers
- Lighting systems
- Communication systems—intercoms, handheld radios, pagers, and portable telephones
- Closed-circuit television systems and audio/video recording equipment
- Intrusion detection systems
- Patrol monitoring devices
- Better-trained security officers to oversee the operation of these systems and equipment

These changes have all contributed to improved and better-designed security programs.

Impact of New York World Trade Center Terrorist Attacks on Building Security

Before leaving the subject of the security of modern high-rise buildings, it is appropriate to discuss the impact of the February 26, 1993, and the September 11, 2001, terrorist attacks on the Twin Towers of the New York World Trade Center. (The incidents are detailed in Chapter 10.) Understandably, the incidents, particularly ''911,'' have created a heightened awareness throughout the United States and the world of the vulnerability of high-rise buildings to such acts of terrorism.

New York World Trade Center Profile[*]

The New York World Trade Center was located on New York City's lower west side, next to the Hudson River at the southern end of Manhattan. The World Trade Center (WTC) was on a 16-acre site with seven buildings (WTC 1 through WTC 7) grouped around a 5-acre plaza (Figure 3.1). The WTC complex consisted of these buildings, the Port Authority Trans-Hudson (PATH) and the New York Metropolitan Transit Authority (MTA) WTC stations, and associated concourse areas.

Of the 110-story Twin Towers, the north tower (WTC 1), 1368 feet (417 meters) in height, was completed in 1972, and the south tower (WTC 2), 1362 feet (415 meters), was completed in 1973. Each of the buildings had 99 elevators. The WTC towers were the fifth and sixth tallest buildings in the world. WTC 3 was the 22-story Marriott Hotel, WTC 4 and 5 were nine-story office buildings, WTC 6 was an eight-story office building, and WTC 7 was a 47-story office building. Underneath a large portion of the main WTC Plaza and WTC 1, 2, 3, and 6 was a six-story subterranean structure.

The Port Authority of New York and New Jersey, a public agency, developed the WTC complex. It owned and operated it up until 2001 when a private party, Silverstein Properties, acquired a 99-year capital lease for the complex. The WTC provided approximately 12 million square feet of rentable office space for government and commercial tenants. Many of the commercial tenants were prominent in the financial and insurance industries.

About three blocks southeast of the WTC Complex is the New York Stock Exchange and the Wall Street financial district. In addition to the World Financial Center (WFC) complex, surrounding the site were other prominent buildings such as the Bankers Trust building, the 1 Liberty Plaza building, the Verizon building, and a historic Cass Gilbert–designed building at 90 West Street.

February 26, 1993, Bombing

As a result of the 1993 bombing in the subterranean parking garage of the WTC, over the next 7 years the WTC spent $60 million in capital funds to

[*]Information obtained from FEMA 403, *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations, Federal Emergency Management Agency* (FEMA,Washington, DC, May 2002, pp. 1-3–1-4).

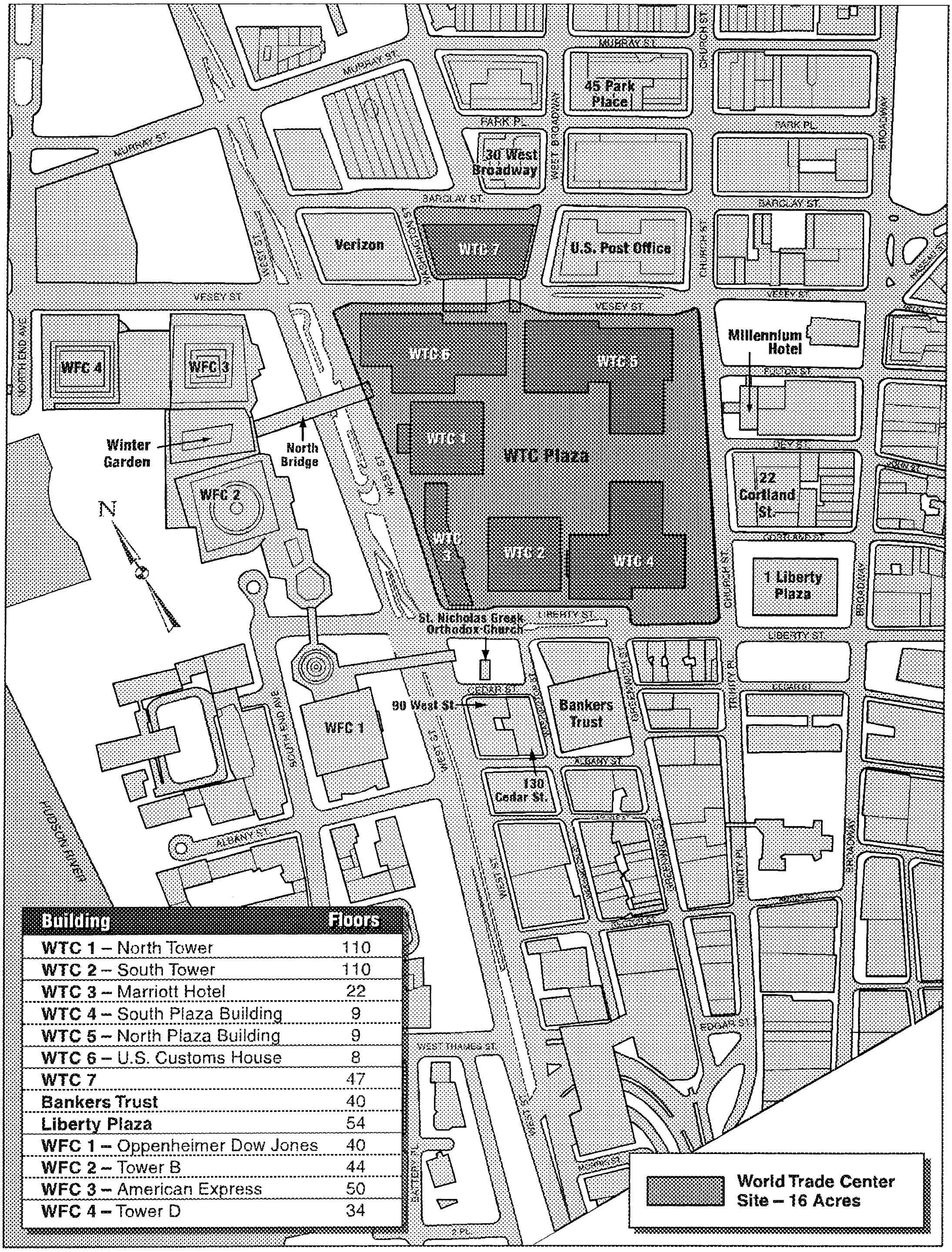


Figure 3.1 New York World Trade Center site and surrounding buildings. (FEMA, World Trade Center Building Performance Study, FEMA 403, p. 1-3, with permission.)

upgrade the security of the complex (Gips, May 2000, p. 11). According to Doug Karpiloff, the late Security and Life Safety Director for the World Trade Center, ''Prior to the bombing, the WTC was an open building during the day, but closed at night. After the bombing, the Center was relegated to a closed facility, in which public parking was completely eliminated'' (''Security soars to new heights,'' September 1997, p. 21). As reported by *SECURITY* (''Never again!'' July 2000, pp. 19–20), the security upgrades included the following measures:

- Forming a ring of 250 ten thousand–pound steel-reinforced planters surrounding the WTC complex, with a custom movable gate that permitted emergency vehicle access to the plaza. Then, according to Karpiloff, ''If the gate is opened, the CCTV cameras lock onto the gate and can't be moved until the gate is closed.'' Once the gate was closed, the cameras unlocked and resumed regular surveillance. According to *Access Control & Security Systems* (''Towering team leader,'' September 2000, p. 42), bomb-resistant trash containers were also provided as part of the perimeter protection system.
- Providing total closed-circuit television (CCTV) coverage of the plaza and perimeter of the WTC.
- Restricting parking beneath the WTC to authorized tenants with special vehicle identification. According to *Access Control & Security Systems* (''Towering team leader,'' September 2000, p. 42), the parking access control system utilized auto vehicle identification (AVI) tags on car windshields and driver's proximity cards to make sure that both the vehicle and the driver were authorized to enter the garage.
- Equipping the underground parking garage with bullet-resistant guard booths, anti-ram barriers, and bomb-sniffing dogs.
- Stopping trucks one block from the buildings for inspection (after being cleared to proceed to the truck dock, the drivers were photographed along with their driver's license, bill of lading, and registration information for storage in the WTC main server).
- Installing a stopped vehicle detection system to sense cars stopping around the perimeter and within the WTC plaza. (When a stopped vehicle was sensed, the CCTV cameras locked onto that area, the WTC police were alerted, and a video print of the vehicle could be taken. The cameras did not unlock until the vehicle was moved. This information was stored on the WTC server at the Security Command center.)
- Creating a ''closed'' building, whereby all people entering the building had to pass through an optical turnstile or register at the visitor's desk. At all times, all tenants and visitors were required to carry a photo ID proximity card. Visitors had to be authorized by a WTC tenant to enter the building. Once authorized, the visitor was photographed and issued an ID card to be used one time, or for 1 day or 1 week or up to 6 months. (If someone jumped over the waist-high optical turnstile, CCTV motion detectors in the lobby caused CCTV cameras to lock onto the violator, the WTC police were alerted, and a video print of the jumper was taken. This information was stored on the WTC server at the Security Command Center.)
- Color coding of all photo proximity cards for tenants and visitors: green for tenants, red for long-term visitors, and yellow for contractors. (When a tenant failed to bring their access card to work, they were issued a visitor's card. If the tenant's regular access card was presented for entry on the same day as the visitor's card was issued, it would not work.)

- A ''mystery shopper'' program using an outside contractor to test at various points if security could be breached (''Towering team leader,'' September 2000, p. 46).
- A key control system with electronic coding and tracking capabilities (''Security soars to new heights,'' September 1997, p. 20).
- Using optical fiber cable to provide high-speed security transmissions with ''limitless bandwidth, long distance, low-loss transmission, immunity to electromagnetic interference and radio frequency interference and long-term stability'' (''Security soars to new heights,'' September 1997, p. 20). (The fiberoptic cable was run in a ring in two directions and was therefore completely redundant. According to Alan Reiss, Director of the WTC at the time, ''If there is a fiber that is severed or cut somehow, you don't shut down the whole system, it automatically switches to an alternate path.'')
- Providing, in case of an emergency, duplicate security command and operation centers that ran the WTC security systems.

Other measures were undertaken to secure the WTC, according to Michael Gips' article ''Building in Terrorism's Shadow'' (2000, p. 11),

> With its $60 million security upgrade since the 1993 bombing, the World Trade Center has set the standard for building security. When determining what security measures should be in place for a given building in the post-bombing environment, Doug Karpiloff, manager of life safety and security at the World Trade Center, says that one must now ask whether the building is a significant or signature structure in the city where it resides. For example, is it the tallest building in the city, is it a symbol of the city itself, or does it house an organization whose activities are inimical to a large group of people? ''If you answer yes to any [of these],'' Karpiloff says, ''visitors and tenants may expect more security than would normally be provided.'' Karpiloff says that he would advise such properties to commission a comprehensive threat assessment and master plan for the building, which would weight threats and risks and explore vulnerabilities.

Although the destruction of the WTC was not a building security issue, Doug Karpiloff's words still ring loud and true. To evaluate the security of any high-rise building, one needs to identify what assets are at risk, what are the threats to those assets, and what are the vulnerabilities or weaknesses of that particular facility. Only then can real countermeasures be devised to eliminate or mitigate the identified risks.

> Today, many high-rise owners and managers are looking for concrete suggestions to relieve their fears and those of their tenants. Many concerns can be addressed by going back to basics and conducting a security survey [described in Chapter 4] to determine a building's security status, then making recommendations for improvements. Before conducting this survey, its scope needs to be clearly defined. What exactly is to be achieved by surveying the building, and what are the underlying reasons for it? Are we assessing the potential for a terrorist threat, or are we just unnerved by what has happened in society? If it is a terrorist threat that we are concerned with, then part of the process should be to evaluate the building and its tenants to determine if either may draw attention from extremist groups. Only after the real motivating factor has been identified can a meaningful review be conducted. (Pinkerton/Burns/Securitas, September 2001)

September 11, 2001, Catastrophe

The loss of the WTC has changed the face of high-rise building security. Before the incident, access controls in multiple tenant buildings were generally loose during normal business hours, Monday to Friday, although they usually tightened up after hours. Since this incident, many high-rise office buildings throughout the United States, particularly major facilities, some of which could be considered as ''significant or signature structures'' in the cities where they are located, have implemented strict access controls 24 hours per day, 7 days per week. Such controls include the following:

- Vehicle drivers who do not have an electronic access card that enables them to enter building parking garages are asked to state their destination within the building to a security officer or a parking attendant and are then directed to a valet parking service.
- Visitor vehicles are not permitted to park in under-building or subterranean parking garages. Parking is restricted to tenants and building users who have pre-authorization (for some sensitive facilities, a background check is required of these drivers before permission is granted).
- Security officers are positioned at the entrance to under-building parking garages to visually inspect passenger vehicles (including their trunks or boots) for suspicious items before their entry; visually inspecting the undercarriage of each vehicle for explosive devices using a small mirror* attached to a 3- to 4-foot long metal pole.
- Delivery vehicles are visually inspected and their manifests checked before their entry to loading docks. Loading dock doors and gates are kept closed between deliveries and pickups.
- CCTV cameras with video motion detector capabilities are installed to view a building's perimeter and neighboring streets; cameras are positioned at building parking garage entrances and exits to facilitate recording of close-up images of the driver and license plate of every vehicle entering and the license plate of all vehicles exiting these areas. (If an incident occurs, this helps identify vehicles that may have been involved.)
- Passenger elevators are placed on card access and tenants are required to use electronic access cards to gain access to their floors (some major buildings have installed optical turnstiles in their main lobbies to screen persons before granting access to building elevators).
- Visitors are asked for photo identification and screened by security personnel in building lobby reception areas (including, in some buildings, the establishment of a separate visitor center to process visitors) before being signed in, given a temporary identification card,† and permitted entry. In some cases, to reduce processing time, the tenants give prior authorization in the form of a letter, memorandum, e-mail, or by using a Web-based visitor management system. In other cases, building security telephones the tenant to request permission for the person to enter; then either the tenant or building security

---

*Also available for viewing under vehicles is an all-weather video camera fitted with a wide-angle lens. The camera is on wheels and can be moved under a vehicle using a multi-angle pole. The image can be viewed using a head mounted video monitor (Sperry West, 2002).

†The nature of temporary access cards varies from adhesive paper to the more sophisticated light-sensitive TEMPbadge® that expires automatically in 1 day, 1 week, or 1 month (http://www.tempbadge.com).

escorts the visitor to the tenant, or building security ''cards up'' (by using an electronic access card, building security selects the floor that the person is authorized to access) the visitor in an elevator to the floor they are authorized to visit.

- Couriers and delivery persons are asked for photo identification, and the tenant gives authorization before the person is given a temporary access badge and permitted to perform the delivery. (In some buildings, security staff retains the photo identification document of the person until the person is ready to exit the site; in other buildings, staff employed by a contract security or courier company with messengers dedicated to the building perform deliveries to and pickups from the tenants on behalf of outside courier and delivery services.)

In addition, some buildings have prohibited parking of vehicles close to the building, including enforcement of no-stopping zones of vehicles on streets and driveways adjacent to the building (sometimes requesting permission from the local city authority so that security staff are authorized to write parking violation tickets) and elimination of taxi stands; established a perimeter 'stand-off' area outside the building using concrete barriers or steel bollards; increased security staffing to implement additional security measures, including building perimeter patrols, and provide an increased visible security presence; utilized a mobile x-ray vehicle to screen, prior to entry, entire vehicles, including trucks, for explosives; installed x-ray machines to screen incoming parcels and packages; positioned walk-through metal detectors in building lobbies and loading docks for all pedestrians entering the building to pass through; applied security window film on glass windows on lower floors; reinforced exposed building columns in areas such as loading docks; and deployed undercover police officers, armed plainclothes civilians, and bomb-sniffing dogs.

The nature of subsequent events that occur in society will determine the permanency and pervasiveness of many of these measures. In addition, the future design and construction of high-rise buildings, including their ability to withstand explosions, will be under scrutiny. Even the very need to continue to build tall structures will be debated.

Fire Life Safety of Modern High-Rise Buildings

The following features often distinguish third-generation* buildings built since World War II, as compared with pre-1945 buildings:

- Fireproofing insulation† is sprayed directly onto steel columns, floor beams, and girders to protect these structural members from distortion due to heat (Figure 3.2). It is applied in accordance with the requirements of the local building code. If the insulation is not correctly applied (for example, if the steel

*Three generations of high-rise buildings are detailed in Chapter 1.

†''Unlike the earlier generation of skyscrapers, which used concrete and masonry to protect the structural steel, many of the newer buildings employed sheetrock [gypsum plasterboard between paper sheets] and spray-on fire protection. The spray-on protection generally consisted of either a

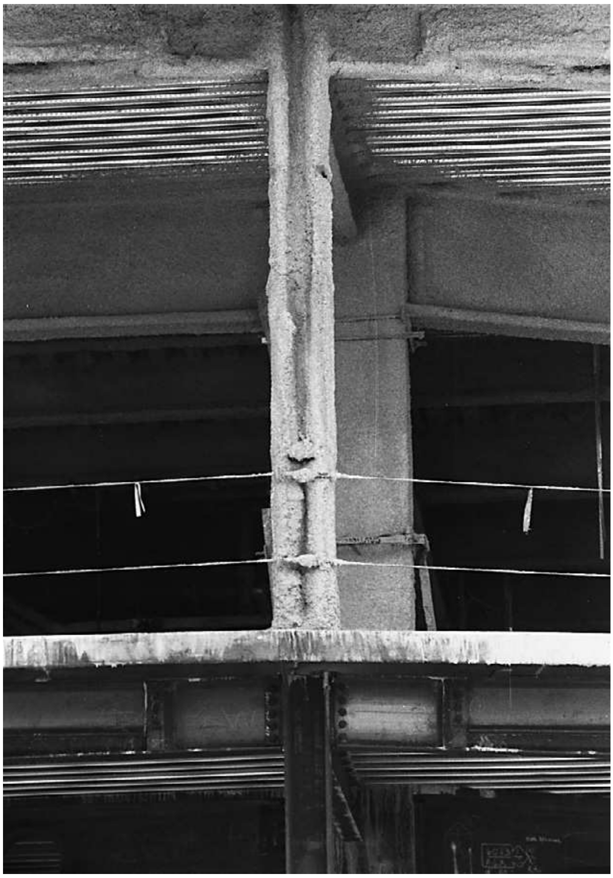


Figure 3.2 Floors of a steel-frame high-rise building exposed during construction. Note the corrugated-steel decks and sprayed-on fireproofing insulation. Photograph by Stephen Lo.

is rusted and the surface has not been properly prepared or if the insulation has not been applied at the specified thickness or density) or if the insulation has been dislodged during construction or high winds, heating an exposed steel floor beam to high temperatures can cause vertical deflection (because the secured beam has no space to move horizontally when it elongates) and failure of the connection used to secure the beam to other beams or to the main girders. In pre-1945 buildings, ''structural steel components were encased in concrete'' (Abbott, 1994, p. 5-17).

- Skin-type curtain walls that do not support any of the weight of the building are usually found on the outside of core construction high-rises. ''They are like a shower curtain—designed to keep the rain out. These curtain walls are usually glass and stone cladding supported on the structure by lightweight metal frames. Skin-type refers to a continuous wall that covers the surface like skin on a body'' (Gorman, 2002). In pre-1945 buildings, ''exterior walls were of masonry construction'' (Abbott, 1994, p. 5-17).
- Curtain walls are attached to the exterior wall columns, sometimes creating an empty space (of width varying from 6 to 12 inches) between the interior of these walls and the outer edges of the floors. If there is such a gap, it is usually

cement-like material that resembles plaster or a mineral-fibre spray, such as the one used to protect the floor joists in the World Trade Center'' (Seabrook, 2001, p. 67).

filled with fire-resistant material to restrict the vertical spread of fire. However, according to Brannigan and Brannigan (1995), ''the reliability of much perimeter firestopping is open to serious question.'' In pre-1945 buildings ''exterior walls were substantially tied to all floors'' (Abbott, 1994, p. 5-17).

- Suspended ceilings, the most common type of ceiling in high-rise office buildings, create a concealed space that often extends throughout an entire floor area. Apart from mandatory firewalls extending from a base floor slab to the floor slab of the floor above, and in restrooms and corridors where fire-rated plasterboard ceilings are used for fire protection, these ceilings lack firestopping material. This uninterrupted space is about 30 in deep and consists of noncombustible acoustical ceiling tiles that are supported in a metal grid hung on metal hangers attached to the floor above. It often is used to house electrical, plumbing, and ducting systems, as well as telephone wiring conduits and computer wiring for that particular floor (Figure 3.3). In some buildings it is also used as a return plenum for the HVAC systems. ''Hotels are one [type of] building that often do not have a suspended ceiling—the concrete floor slab above is the ceiling below and all the electrical is cast in the slab'' (Gorman, 2002). ''Plenum type ceilings are generally not found in pre-1945 buildings'' (Abbott, 1994, p. 5-17).
- Floor beams and girders are often covered with corrugated steel panels or plates and are then covered with a layer of concrete to form the floor itself. ''The floors in most of the high-rise buildings erected since the sixties are much lighter in weight than the floors in the older buildings. In a typical high-rise office floor, three to four inches of concrete covers a corrugated-steel deck, whose weight is supported by I-beams or, in the case of the [WTC] Twin Towers, by long 'trusses'—lightweight strips of steel that are braced by cross-hatched webs of square or cylindrical bars, creating a hollow space below each floor surface. This space allows builders to install heating and cooling ducts within the floors, rather than in a drop [suspended] ceiling below them—an innovation that means the developer can increase the number of floors in the entire building'' (Seabrook, 2001, p. 67).
- Multiple stairwells provide primary and secondary means of egress and are often equipped with automatic stairshaft pressurization and smoke evacuation systems. Because these stairwells are located in the central core area, they are less distant from each other than those in pre-World War II buildings in which ''stairways were remote from each other, located at the opposite ends of the building'' (Abbott, 1994, p. 5-18).
- Stair and elevator shaft openings are equipped with protective assemblies, and horizontal openings are protected.
- Floor areas tend to be larger and generally open-plan design, with little compartmentation using floor-to-ceiling walls and barriers. Aluminum-framed, cloth-covered foam partitioning is often used to construct cubicles to be used as individual offices. This partitioning is cheaper than the hardwood partitioning used in the past, and just as effective as a sound barrier. However, it is more combustible. Pre-1945 buildings were ''well compartmented with slab to slab partitions of at least 2 hour fire rating'' (Abbott, 1994, p. 5-17).
- The number of occupants tends to be high, and this results in a high concentration of business and personal property, and hence high fire or fuel load. Much of this property (including office supplies, plastic wastepaper baskets, files, paper, floppy disks, compact discs, cartridges, and the personal computer systems that now equip most work-stations) is made of synthetic materials that are flammable and, in a fire, produce toxic gases that become components in

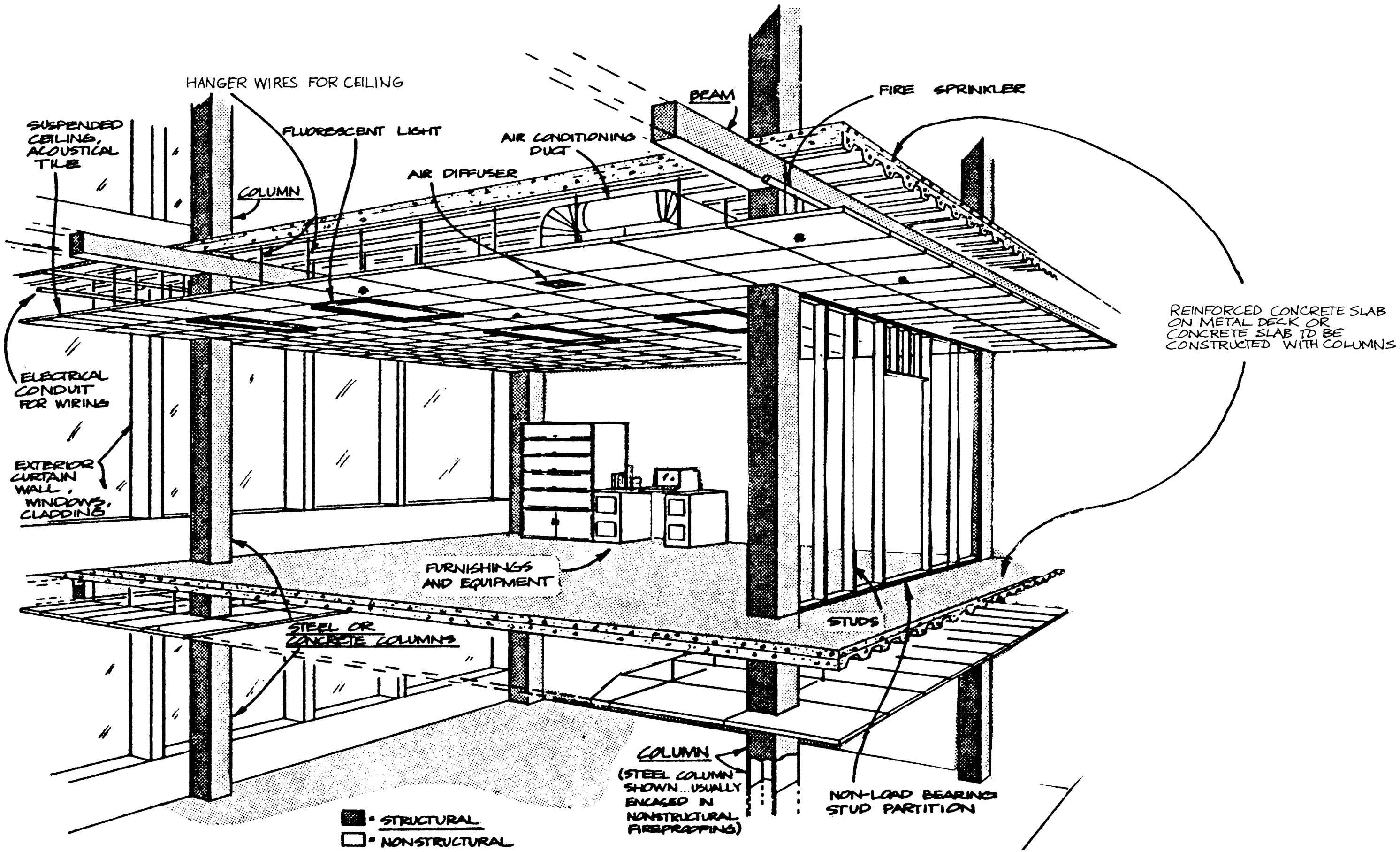


Figure 3.3 Nonstructural portions (including every part of a building and all its contents except the structure) and structural portions of a typical building. (Courtesy of The Southern California Earthquake Preparedness Project [SCEPP], revised for the second edition by the Bay Area Regional Earthquake Preparedness Project, Reducing the Risks of Nonstructural Earthquake Damage: A Practical Guide [Los Angeles: SCEPP, 2nd ed., 1983], p. 2, a Federal Emergency Management Agency [FEMA]-sponsored project.)

the resulting smoke and gas.* As Bathurst writes, ''Over the past several years, there have been many changes in the furnishings put into buildings. At one time, desks and chairs were routinely made of wood. Then metal became popular. Now, any combination of wood, metal, thermoplastics, and foamed plastics can be found. In addition, the increased use of computers has also added fuel load'' (1997, p. 9-34). To mitigate this threat to life safety, office furniture and interior furnishings in all offices, conference and waiting rooms, and reception and assembly areas should be of fire-resistive quality and treated to reduce combustibility.

- Heating and air conditioning is usually by a central HVAC system that serves multiple floors. Pre-1945 buildings are ''usually not centrally air conditioned . . . normally [they are] steam heated'' (Abbott, 1994, p. 5-17).
- There is the potential during fires for the stack effect described earlier in this chapter. Brannigan notes of pre-World War II buildings: ''Windows could be opened in buildings of this era. This provided local ventilation and relief from smoke migrating from the fire. The windows leaked, often like sieves, therefore there was no substantial stack effect'' (1992, p. 459). Modern high-rise building windows provide some resistance to heat and are often made of tempered safety glass; they usually cannot be opened and are well insulated. ''There are no manual fire fighting techniques known to counter stack effect or to mitigate its effect during a fire'' (Caldwell, 1997, p. 9-18). Caldwell goes on to say that, due to building height and the temperature differential that exists between areas, the only way to reduce the potential of stack effect is to change building design and construction techniques to those that minimize the effect.
- Automatic fire detection systems and automatic fire suppression systems are often incorporated into building design. As Brannigan and Brannigan (1995) state:

> Most new high-rise office buildings are sprinklered. The huge losses suffered in such fires as Philadelphia's One Meridian Plaza and Los Angeles' First Interstate Tower [First Interstate Bank Building] leave little room for argument. But there is still much opposition to any requirement for retroactive installation of sprinklers in existing buildings. While much of the opposition is financial, the specious argument that such requirements are unconstitutional has found some favor. This argument is without merit with respect to United States law. Much of the cost, particularly of a retroactive installation, is caused by hiding the sprinkler system. If the argument of overall sprinkler cost is an issue, the opposing argument is that safety requires only the cost of a bare bones system. Aesthetic costs such as hiding the sprinklers and the piping are the option[s] of the owner, not a fire protection requirement.

Modern High-Rises Are Less Fire-Resistive

Both Francis L. Brannigan, in *Building Construction of the Fire Service,* and John T. O'Hagan, in *High-Rise/Fire and Life Safety,* put forth the opinion that modern high-rise buildings are less fire-resistive than those of the previous generation. Brannigan defines a fire-resistive building as one ''that to some degree will resist fire-caused collapse'' (1992, p. 11). He further defines the limits of

*''Smoke is defined as the total airborne effluent from heating or burning a material. Thus, expressions such as 'smoke and toxic gases' are, by this definition, redundant'' (Clarke, 1997, p. 4-8).

fire resistance by stating, ''Fire resistance is intended to provide, within limits, resistance to collapse by structural members and floors, and resistance to the passage of fire through floors and horizontal barriers'' (1992, p. 452). He goes on to say that buildings built after World War II have poorer fire protection features (1992, p. 458).

O'Hagan (1977, p. 28) believes modern high-rise buildings are less fire resistive than the previous generation because of their lightweight steel construction, their greater potential for bigger fires because of open-floor design, and their greater heat retention because of better insulation. Add to these factors the greater fuel loads caused by a higher concentration of business and personal property, and it looks as though modern high-rise buildings are higher-risk occupancies.

Brannigan further asserts that modern high-rise buildings are lighter than previous generation high-rises: ''The Empire State Building [a second-generation building] weighs about 23 pounds per cubic foot. A typical modern high-rise weighs approximately eight pounds per cubic foot'' (1992, p. 462). He also states, ''The development of fluorescent lights and air conditioning helped to remove limits to the floor area. Thus, building populations could be enormously increased. As a result, many floors have substantial areas beyond the reach of hand hose streams'' (1992, p. 462).

The destruction of the WTC has added considerable weight to the arguments put forth by Brannigan and O'Hagan.

John Seabrook, writing in *The New Yorker*, notes that,

> One indication that older high-rise buildings may be more fire-resistant than the newer high-rise buildings is the performance of the twenty-three-story building at 90 West Street—a Cass Gilbert-designed building, finished in 1907 (Gilbert also designed the Woolworth Building), whose structure was protected by concrete and masonry—compared with the performance of 7 World Trade Center, an all-steel building, from the nineteen-eighties, that had spray-on fire protection. Both buildings were completely gutted by fires on September 11th, but 90 West Street is still standing, and may eventually be restored. 7 World Trade, which had a gas main beneath it, collapsed after burning for seven hours. (November 19, 2001, p. 67)

Other Fire Life Safety Features

Although modern high-rise buildings may be considered less fire-resistant than previous generation buildings, from a life safety standpoint the picture may be different. Modern steel-frame buildings that have properly designed, installed, operated, tested, and maintained automatic fire detection and suppression systems, and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes and automatic smoke control systems to restrict the spread of smoke—do have the necessary early warning systems to quickly detect fires and warn occupants of their presence and the necessary automated sprinkler systems to quickly extinguish a fire in its early stages.

Fire detection systems trace their origin to the mid-19th century. Since then, the performance and reliability of ''a number of mechanical, electrical, and electronic devices [that] have been developed to mimic human senses in detecting the environmental changes created by fire'' (Moore, 1997, p. 5-12) has constantly improved.

Also, ''since they were introduced in the latter part of the 19th century, the performance and reliability of automatic sprinklers have been improved continually through experience and the efforts of manufacturer and testing organizations'' (Isman, 1997, p. 6-124).

One of the key issues here is the presence or absence of sprinklers. ''The probability of a serious fire in any given office building or other building with many occupants is extremely low. It is also a fact, however, that in the typical unsprinklered glass-enclosed office building with interior stairways and a substantial fire load, the consequences of a serious fire during working hours could be very severe—with multiple fatalities'' (Brannigan, 1992, p. 570).

Fire Life Safety History

In discussing fire risk in high-rise buildings it is helpful to analyze fire incident data* for the four property classes (office buildings, hotels and motels, apartment buildings, and hospitals [and other facilities that care for the sick]) that dominate high-rise buildings.

A study by Dr. John Hall, Jr., of the National Fire Protection Association's (NFPA) Fire Analysis and Research Division, using statistics from the U.S. Fire Administration's National Fire Incident Reporting System (NFIRS), stated that from 1987 to 1991, office buildings, hotels and motels, apartment buildings, and facilities that care for the sick, averaged 13,800 high-rise building fires per year and associated annual losses of 74 civilian deaths, nearly 720 civilian injuries, and $79 million in direct property damage. However, most of these high-rise building fires and associated losses occurred in apartment buildings (Hall, 1994, pp. 47–53). Dr. Hall added that for this period:

- More than half of the high-rise office building fires occurred in buildings that were not equipped with sprinklers or any other automatic suppression equipment.
- High-rise buildings generally tend to have a larger share of fires that start in halls and corridors than other types of buildings.
- Only a small proportion of high-rise building fires spread beyond the room of origin, let alone the floor of origin.

*''Tracking of the fire experience in high-rise buildings, however, has been less than systematic, because the nationally representative fire incident data bases did not originally include reporting of height of structure. Reasonably good reporting began with 1985 fires . . . . NFPA and other analysts have long used lists of particularly memorable incidents to study the high-rise fire problem, but these and other available special data bases are heavily weighted toward larger and more severe incidents'' (Hall, September 2001, p. 1).

- The causes of high-rise building fires are not very different from the causes of fires in other buildings. In high-rise office buildings, electrical distribution system fires rank first in causes of fire-related property damage.

The 1985 to 1998 study by Dr. Hall (1998 is the most recent year for which data is available) shows that ''in 1998, high-rise buildings in these four property classes combined had 10,000 reported structure fires and associated losses of 37 civilian deaths, 680 civilian injuries, and $41.1 million in direct property damage'' (Hall, September 2001, p. 3). From these statistics Dr. Hall concludes that from 1985 to 1998, ''the trends in high-rise fires and associated losses are clearly down if inflation is taken into account'' (p. 42). This verifies Hall's aforementioned findings that ''most high-rise building fires and associated losses occur in apartment buildings.... only a small share of high-rise building fires spread beyond the room of origin, let alone the floor of origin'' (pp. 4, 42).

The Institute of Real Estate Management (1990, p. 111) states:

> Two of the leading causes of office building fires are electrical problems and arson, with a third major cause being careless workers. In office buildings, fires originate in tenant spaces 28 percent of the time, usually occurring between 7:00 AM and 6:00 PM on weekdays when the building is full. Another 21 percent of building fires occur in electrical and mechanical rooms, with a similar proportion of fires starting in common areas and other building areas.

The Concrete and Masonry Industry's Firesafety Committee (1991, p. 1) states:

> The number of lives lost in high-rise building fires has historically been lower than for other types of structures. Each year approximately 5,000 people die in building fires in the United States. Over the last three decades, however, based on fire incidents reported to the NFPA, an average of fewer than 28 fire-related deaths per year have occurred in high-rise building fires (excluding those involving grain elevators and silos). If the MGM Grand and DuPont Plaza hotel fires are excluded, the death toll is approximately 22 per year.

Emergency Planning Essentials

In modern high-rise buildings, special fire protection requirements (automatic sprinklers, detection and alarm systems, and compartmentation features associated with fire-resistive construction) are reflected in strict laws, codes, and standards. These special requirements, although they are designed to provide sufficient time for occupants to escape, are not in themselves sufficient: The life safety of occupants also depends critically on how ready they are to react appropriately at the time of an incident. If building management has provided a sound fire life safety program, then a building can be considered well prepared. A sound fire life safety program will assist all building staff and occupants to be in a constant state of readiness to react to an emergency, particularly one that involves fire, in a way that will help provide for everyone's safety.

Impact of New York World Trade Center Terrorist Attacks on Building Safety

Before leaving the subject of the fire safety of modern high-rise buildings, it is appropriate to discuss the impact of the February 26, 1993, and the September 11, 2001, terrorist attacks on the Twin Towers of the New York World Trade Center. (The incidents are detailed in Chapter 10.)

February 26, 1993, Bombing

As a result of the 1993 bombing in the subterranean parking garage of the WTC, improvements to the evacuation plan for the towers included the following measures:

- Providing four levels of power—the primary power source, emergency diesel generators, battery back-ups, and back-up power from the State of New Jersey—to provide power to the command centers, one freight elevator in each building, emergency radios, and emergency lighting (''Towering team leader,'' September 2000, p. 44).
- Installing battery back-up lighting systems on stairwell landings at every second floor (Prouix and Fahy, 2002) and in each elevator.
- Installing glow-in-the-dark photo-luminescent paint on all stairwell stair treads, railings, doors, and evacuation signs as a backup to primary and emergency lighting in the stairwells.
- Adding ''bright [directional] arrows to guide people along corridors to stairway connections'' (Cauchon, 2001, p. 4).
- Providing, in case of an emergency, duplicate security command and operation centers that ran the WTC security systems (''Never again!'' July 2000, pp. 19–20).
- Retrofitting the fire system with new fire protection devices such as smoke detectors, strobe lights in public and tenant spaces, a new public address system (that reached beyond common area hallways into office areas), new floor warden telephones, and fully sprinklering the retail mall (Litwak, October 1999, p. 57).
- Giving every disabled person an evacuation chair that could accommodate the person carried by two others (Cauchon, 2001, p. 4).
- Providing well-planned and executed fire life safety training of all building occupants, particularly in emergency evacuation procedures. Evacuation drills* were conducted every 6 months (Cauchon, 2001, p. 4).

The WTC had egress stairways that were ''much better than required by building codes—both when it was built 30 years ago and now. Each tower had three stairwells. New York City building codes require two'' (Cauchon, 2001, p. 4).

*In the city of New York, fire codes for office buildings require that ''Fire drills shall be conducted, in accordance with the Fire Safety Plan, at least once every three months for existing buildings during the first two years after the effective date of these rules, or for new buildings during the first two years after the issuance of the certificate of occupancy. Thereafter, fire drills shall be conducted at least once every six months'' (RCNY 1625 6-30-91).

A consequence of the 1993 bombing was that system designers of mega-high-rise* buildings gave renewed attention to providing zoning and redundancy of life safety systems, so that if one portion of a building was destroyed, critical life safety systems would not fail in the entire building. For example, emergency and standby electrical power, emergency lighting, fire suppression, and mechanical smoke evacuation systems could be zoned so that their controls are not isolated to one particular area of a building.

September 11, 2001, Catastrophe

The collapse of the World Trade Center towers has caused much concern among owners, developers, architects, engineers, code officials, and firefighters regarding the safety of high-rise buildings and their vulnerability to such acts of terrorism. In the light of the collapse of the Twin Towers of the WTC, and considering the aforementioned discussion of ''Modern High-Rises Are Less Fire-Resistive,'' one could argue that had the towers been more fire-resistive and able to remain standing longer, then fewer people would have died.

As reported in *The New Yorker* (Seabrook, 2001, p. 2), Guy Nordenson, a New York structural engineer and a Princeton professor, wrote a letter to the Times, ''praising the towers' structural design for keeping them standing as long as they did, and allowing some twenty-five thousand people to escape.'' In response, Leslie E. Robertson, the structural engineer who, with his then-partner, John Skilling, was largely responsible for the structure of the Twin Towers, wrote an e-mail message to Nordenson (2001, p. 2) that read,

> Your words do much to abate the fire that writhes inside It is hard (sic)
> But that I had done a bit more . . .
> Had the towers stood up for just one minute longer . . . It is hard.

Since September 11, many other issues have been raised. For example, the question has been asked as to whether tall buildings should continue to be built in the future and whether they should be designed to resist explosions (a topic raised after the 1993 World Trade Center and the 1995 Oklahoma City bombings). There are implications to change high-rise building design to include lower heights, more stairwells, lower occupancies, upgraded refuge areas, and safe elevators (Fahy and Prouix, 2002) that could be used during emergencies such as fire. Even the threat from the air led to a policy change in Chicago—approved by the Federal Aviation Administration—expanding ''the 'no-fly zone' over the city to an area significantly larger than that mandated by the FAA immediately after September 11. This expansion was temporary, and

*A *mega-high-rise* building is defined in the NFPA Fire Investigation Report on the 1993 New York World Trade Center bombing (Isner and Klem, 1993, p. 55) as ''a large, tall (greater than 50 stories), densely populated structure where emergency evacuation is difficult or impractical. They are further characterized in that the ordinary fuels which they contain may result in rapid fire growth, development, and spread because of their geometric arrangement, and in extensive smoke spread throughout the structure which threatens occupants in remote areas from the fire origin. Further, the time required for fire fighters to establish effective fire fighting operations can be extensive because of the vertical arrangement of the structure.''

the area has since been reduced (Archibald, Medby, Rosen, and Schachter, 2002, p. 53).

A Clear Message

One clear message that applies to all high-rise buildings, whether they are evaluated to be at risk to a terrorist event or not, is that all tenants should be well trained in evacuation procedures. ''In each tower, 99% of the occupants below the crash survived*'' (Cauchon, 2001, p. 1). In each tower there were people who perished on the floors that sustained the direct impact of the aircraft and those who were inextricably trapped above the crash site because all three stairwells in the north tower and two stairwells in the south tower were made inaccessible, and elevators were made inoperable, by the impact, explosions, and ensuing fires. The World Trade Center had a comprehensive, well-executed fire life safety program and emergency plan that helped prepare building emergency staff and occupants to react appropriately to the catastrophic events that unfolded on September 11. All indications are that the occupants who were able to evacuate did so in an orderly and competent manner. According to *USA TODAY* (Cauchon, 2001, p. 2),

> The evacuation was a success. Nearly everyone who could get out did get out. The Port Authority had revised its evacuation plan for the buildings after a terrorist bomb exploded in the Trade Center garage in 1993. On September 11, those changes saved hundreds, possibly thousands, of lives. The buildings, sturdily constructed, exquisitely engineered, and equipped with stairwells bigger than building codes require, stood just long enough to give potential survivors a chance to get out.

Summary

From a security and fire life safety standpoint, high-rise buildings have unique requirements that distinguish them from low-rise buildings. There are ways that the security and fire life safety of modern high-rise buildings differ from earlier-generation high-rises. The September 11, 2001, destruction of the New York World Trade Center has changed forever the world of building security and fire life safety. It has raised questions among owners, developers, architects, engineers, code officials, and fire service personnel, as to the safety of modern high-rise buildings and their vulnerability to such acts of terrorism. It has also reinforced the supposition that the life safety of occupants of high-rise buildings depends critically on how well trained they are to evacuate when an emergency occurs.

*''Almost everyone in WTC 1 and WTC 2 who was below the impact areas was able to safely evacuate the buildings, due to the length of time between the impact and collapse of the individual towers'' (FEMA 403, 2002, p. 1-4).

References

Abbott, Richard J., ''Comparison of design and construction techniques class 'E' high rise office buildings,'' *Fire Science Institute Office Buildings Fire Safety Directors Course* (Fire Science Institute, New York, 1994).

Archibald, Rae, Jamison Jo Medby, Brian Rosen, and Jonothan Schachter, ''Security and Safety in Los Angeles High-Rise Buildings After 9/11'' (RAND Documented Briefing, Santa Monica, CA, April 2002).

Bathurst, Donald G., ''Business occupancies,'' *Fire Protection Handbook,* 18th ed. Arthur E. Cote, Editor-in-Chief (National Fire Protection Association, Quincy, MA, 1997).

Brannigan, Francis L., *Building Construction for the Fire Service,* 3rd ed. (National Fire Protection Association, Quincy, MA, 1992).

Brannigan, Francis L., and Maurine Brannigan, ''Building Construction for the Fire Service'' (Letter to the author from Francis Brannigan, March 16, 1995).

Caldwell, Carol, ''Occupancies in special structures and high-rise buildings,'' *Fire Protection Handbook,* 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Cauchon, Dennis, ''For many on Sept. 11, survival was no accident'' (*USA TODAY*, McLean, VA, December 20, 2001). Contributing: Barbara Hansen, Anthony DeBarros, and Paul Overberg.

Clarke, Frederick B., ''Fire hazards of materials: an overview,'' *Fire Protection Handbook,* 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Concrete and Masonry Industry, ''Fundamentals of fire safety,'' *Fire Protection Planning Report* (Concrete and Masonry Firesafety Committee, Skokie, IL, 1991).

Egan, David W., ''Tall buildings,'' *Concepts in Building Firesafety* (John Wiley and Sons, New York, 1978).

Fahy, Rita, and Guylene Prouix, ''A Comparison of the 1993 and 2001 Evacuations of the World Trade Center'' (Presentation to the NFPA World Safety Congress and Exhibition, Minneapolis, MN, May 21, 2002).

FEMA 403, *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations, Federal Emergency Management Agency* (FEMA, Washington, DC, May 2002).

Gips, Michael A., ''Building in terrorism's shadow,'' a May 2000 *Security Management* magazine article re-published in *Counterterrorism and Contingency Planning Guide* (A special publication from Security Management and ASIS International, Arlington, VA, post-September 11, 2001).

Gorman, Mark, Structural Engineer, URS Corp. Comments to the author in an e-mail message regarding the core and tube construction of high-rises (Los Angeles, CA, March 2002).

Hall, John R., ''U.S. high-rise fires: the big picture'' (*NFPA Journal,* National Fire Protection Association, Quincy, MA, March/April 1994).

Hall, John R. Jr., *High-Rise Building Fires* (National Fire Protection Association, Quincy, MA, September 2001).

Institute of Real Estate Management, ''Fires,'' *Before Disaster Strikes: Developing an Emergency Procedures Manual* (IREM, Chicago, 1990).

International Fire Service Training Association, ''Access problems,'' *Fire Problems in High-Rise Buildings* (Fire Protection Publications and Oklahoma State University, Stillwater, OK, 1976).

Isman, Kenneth E., ''Automatic sprinklers,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Isner, Michael S., and Thomas J. Klem, ''Discussion,'' *Fire Investigation Report, World Trade Center Explosion and Fire* (National Fire Protection Association, Quincy, MA, 1993).
Kitteringham, Glen W., ''A study of two types of vertical crime pattern analysis in the commercial, multi-tenanted high rise structure'' (Masters of Science thesis in Security and Crime Risk Management, the Scarman Centre for the Study of Public Order, Canada, February 2001).
Kitteringham, Glen, ''A pattern for crime: an overview of the two dimensional mapping process for crime risk evaluation'' (*Canadian Security*, Facility Management Supplement, November 2001, Canada).
Litwak, David, *Keeping the Twins Safe* (Security Technology & Design, Cumming, GA, 1999).
Moore, Wayne D., ''Automatic fire detectors,'' *Fire Protection Handbook,* 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
''Never again!'' (*SECURITY*, Highlands Ranch, CO, July 2000).
O'Hagan, John T., *High Rise/Fire and Life Safety,* 2nd printing (Fire Engineering, A PennWell Publication, Saddle Brook, NJ, 1977).
Pinkerton/Burns/Securitas, ''High-rise building security: the world has changed,'' article by Geoff Craighead, CPP (Pinkerton/Burns, A Securitas Company, September 2001).
Prouix, Guylene, and Rita Fahy, ''A Comparison of the 1993 and 2001 Evacuations of the World Trade Center.'' (Presentation to the NFPA World Safety Congress and Exhibition, Minneapolis, MN, May 21, 2002).
RCNY 1625, 6-30-91, 6-01, ''Fire drill and evacuation in office buildings and buildings classified as occupancy group E (Business), (d)'' *Drills* (1) (New York).
Seabrook, John, ''The tower builder, why did the World Trade Center buildings fall down when they did?'' (*The New Yorker*, November 19, 2001).
''Security soars to new heights,'' (*SECURITY*, Highlands Ranch, CO, September 1997).
Sperry West, Undercar Video Viewer Spyder®scope (Sperry West, Inc., San Diego, CA, http://www.sperrywest.com).
TEMPbadge®, Systems for Visitor Control (TEMPbadge®, Suffern, NY; available at: http://www.tempbadge.com).
''Towering team leader,'' (*Access Control & Security Systems* magazine, Atlanta, GA, September 2000).

Additional Reading

NFPA Fire Analysis and Research Division, *One-Stop Shop* (National Fire Protection Association, Quincy, MA 02269-9101). An excellent source for fire incident databases.
Brannigan, Francis L., *Building Construction for the Fire Service*, 3rd ed. (National Fire Protection Association, Quincy, MA., 1992).
O'Hagan, John T., former Fire Commissioner and Chief of the New York City Fire Department, *High Rise/Fire and Life Safety,* 2nd printing. (Fire Engineering, A PennWell Publication, Saddle Brook, NJ, 1977).

4 *Security and Fire Life Safety Surveys*

The security and fire life safety needs of any facility, whether it be a high-rise building or not, are determined by ''identifying specific assets, the threats against those assets, and the risk[*] of those threats materializing. Also of vital importance, if selected solutions are going to be effective, is an understanding of the possible constraints (for example, culture, operations, economic factors, and codes and standards). The survey is the tool used to collect the data for the analysis of security and life safety requirements and to identify vulnerabilities'' (Aggleton, 2001, p. 1).

Security Survey

A security survey is defined as ''a critical on-site examination and analysis of an industrial plant, business, home, or public or private institution to ascertain the present security status, to identify deficiencies or excesses, to determine the protection needed, and to make recommendations to improve the overall security'' (Momboisse, 1968, p. 13).

Fischer and Green (1998, pp. 168–169) further state:

> A security survey is essentially an exhaustive physical examination of the premises and a thorough inspection of all operational systems and procedures. Such an examination or survey has as its overall objective the analysis of a facility to determine the existing state of its security, to locate weaknesses in its defenses, to determine the degree of protection required, and ultimately to lead to recommendations for establishing a total security program. . . . In the process of risk analysis that proceeds from threat assessment (identifying risk) to threat evaluation (determining the criticality[†] and dollar cost of that risk) to the selection of security countermeasures designed to contain or prevent that risk, one of management's most valuable tools is the security survey.

A security survey may focus on different aspects of a high-rise facility. It may include the area and businesses in the surrounding neighborhood, the facility

[*]As defined by Walsh, ''risk is the exposure to a probable, unfavorable event or condition'' (Walsh, 1999). ''Before any risk can be eliminated (or for that matter, reduced) it must be identified. One proven method of accomplishing this task is the security survey'' (Broder, 2000, p. 41).

[†]Criticality is determined by the impact that a threat would have if it actually occurred at a facility.

itself, a tenant in the facility, or defined aspects of the security operation such as certain policies, procedures, and equipment. It may also be used as a tool to investigate a particular incident or a security problem that has occurred or is occurring. In addition, an opinion survey may be conducted among security staff to measure their morale or elicit their ideas regarding the effectiveness of the overall security program and certain procedures and equipment; such an opinion survey also may be conducted among building staff (management, janitorial, parking, and engineering) and building tenants. An opinion survey of tenants is an important tool enabling building management to evaluate the tenants' perception of the security program, to identify areas that need to be changed or improved, or to evaluate the anticipated reaction of tenants if changes were to be made to the security program.

There is no real shortcut in carrying out effective security and fire life safety surveys. Thomas Edison made the famous statement that ''genius is 1 percent inspiration and 99 percent perspiration'' (Israel, 1994, p. 13). It may not take a genius to conduct a survey—although technical expertise and experience are important aspects of the process—but there is no doubt that to make a thorough analysis of the security or fire life safety aspects of a facility, a considerable amount of work is required. To make the work as orderly as possible, it is helpful to use a standardized approach. This will make it more likely that vital areas are adequately covered and a uniform standard in surveys repeatedly conducted is maintained and will assist the surveyor in efficiently conducting the survey itself.

How to Conduct a Physical Security Survey

A physical security survey can be as extensive or as restricted as the surveyor determines. A formal documented survey basically will involve two major tasks: the fact-finding investigative process, and writing the report that reflects the findings.

Fact-Finding Process

The fact-finding process may include the following:

1. Discuss with those commissioning the survey the scope of the survey, identify the individual(s) with authority to implement the survey recommendations, designate the time period in which the survey will be conducted, and determine to whom the final survey report will be presented. To help protect disclosure of the survey findings, the report may be commissioned by the legal firm representing the building owner or manager. By so doing, the survey becomes ''Privileged and Confidential'' information.
2. Review codes and standards pertaining to required security measures.
3. ''Obtain incident reports of all incidents that have occurred on the property for the past (minimum) three years or (preferred) five years'' (Kaminsky, 2001, p. 104). Also, depending on the scope of the survey, it may be useful to conduct a crime pattern analysis examining ''criminal activity in an effort to find patterns in the physical environment that makes it easy for a crime to occur.

This tool has been used by police for a number of years . . . its implications can be important in conducting a security evaluation of a specific location. The old-style, two-dimensional mapping process—using floor plans, stacking* plans and colour-coded labels [to indicate crimes and attempted crimes]—can be very helpful to facility and security managers who choose to conduct their own analyses'' (Kitteringham, 2001, p. 19).

4. Interview the crime analysis officer or community relations officer of the local police or sheriff's department to request crime statistics for the site and the neighboring area. (Although not all police agencies are willing to release such data, if possible, statistics should be obtained for the previous 3 to 5 years.)†
5. Interview representatives of nearby businesses or observe the immediate neighborhood and areas surrounding the site to determine what security measures other businesses, particularly similar businesses, have implemented. Benchmarking is the process by which the security program at a facility can be compared with the best practices that exist for similar types of facilities. ''Benchmarking . . . serves as a barometer for determining what works best under comparable circumstances'' (Dalton, 1998, p. 55).
6. Review any previous surveys conducted at the site (such documents, if available, can provide background information and details of the follow-up on previously noted deficiencies).
7. Review available documentation that is relevant to the survey. This could include a description of the building and its construction features (sometimes this can be found in marketing material for the site, or from architectural documents), site and floor plans, plans for changes at the site, annual reports, records, tenant leases, security services agreements, data, files, organizational charts, job descriptions, manuals, policies, and operating procedures (including security instructions, standard operating procedures, or post orders).
8. Conduct a profile of tenant businesses to ascertain which ones may constitute a high risk from a security perspective and be a potential target for international terrorists (for example, a foreign embassy or major financial center), domestic activist groups (for example, a furrier), or criminals seeking high-value merchandise (for example, a jeweler). This profile may include the building itself. For example, due to its being the tallest building in a city, a historic landmark or an embodiment of the economic strength of the nation, is the building considered a target for an act of international terrorism? (Likewise, buildings located in proximity to such a facility may be at risk of suffering collateral damage.)
9. Interview persons who have knowledge of the site. These individuals may include architects, structural engineers, building management, building engineers, janitors, security and parking staff, couriers, elevator technicians, and the vendors of the security equipment currently in place or planned for installation.

---

*A stacking plan is ''basically a side view of the [facility] showing the entire building, including all floors and a list of tenants inhabiting these floors'' (Kitteringham, 2001, p. 19).

†In the United States and Canada, a source of information to complement police data is a crime prediction model that assesses Crimes Against Persons and Property (*CAP Index*). ''By combining surrounding social characteristics, survey information and other databases with known indicators of crime, the CRIMECAST™ model is able to provide precise scores indicating a site's risk of crime in comparison to national, state and county averages. . . . CRIMECAST™ data include current, past and projected scores for Crimes Against Persons (rape, robbery, homicide, aggravated assault) and Crimes Against Property (burglary, larceny, motor vehicle theft)'' (CAP Index, Inc.).

10. Visit the site at different times during the day and night, business and non-business hours, to become familiar with the following:

    - Principal activities and usage
    - Physical layout, including the ingress and egress points, construction, and landscaping
    - Occupant and visitor traffic flow patterns and how access is controlled
    - Lighting and locking systems
    - Electronic security systems
    - Security program in operation

    These visits may include testing various aspects of the security program. To check the operation of systems, particularly to determine whether certain procedures are being implemented as they were designed to be, such testing might be done clandestinely.
11. In addition, insurance policies for the site may need review to determine whether the coverage adequately covers present risks. For high-profile, signature* buildings, insurance is particularly important in view of the September 11, 2001, terrorist acts that destroyed the Twin Towers of the New York World Trade Center. ''Prior to the events of September 11, 2001, property and casualty, and general liability insurance policies typically covered damages resulting from acts of terrorism,† although most excluded damages relating to acts of war . . . By now, most states have permitted insurers to exclude terror insurance from their general property and casualty coverage'' (IREM, 2002, p. 3). Commercial property owners requiring terrorism insurance have to purchase it from insurance underwriters. ''Those policies have high deductibles, low limits and very high premiums. Property owners who succeed in obtaining terrorism coverage often do so by covering a large portfolio, thereby spreading the risk'' (Gottlieb, 2002, p. 10). Of course, only a qualified risk manager or insurance advisor should conduct an in-depth review of insurance policies.

Systematic Approach

To approach the viewing of the site in an orderly fashion, it is helpful to consider that ''the classical approach to perimeter security views a property in terms of rings. The property boundary is the first ring. The building is the second, and the specific interior spaces are the third'' (Healy, 1983). ''This

*A building is considered a *signature building* based on its size and height, its status, or the nature of its tenants. Doug Karpiloff, when manager of life safety and security for the New York World Trade Center, defined a significant or signature structure by posing the questions, ''Is it the tallest building in the city, is it a symbol of the city itself, or does it house an organization whose activities are inimical to a large group of people?'' (Gips, May 2000, p. 11).

†''Before Sept. 11, the risk of terrorist attacks was borne by the insurance industry. Covered by 'all risk' policies generally required by lenders, commercial business owners insured for this risk as part of ordinary business practice. From the insurer's viewpoint, the cost of providing this coverage was not significant. After all, there had been only two significant acts of terrorism in the United States. One, the Oklahoma City bombing, involved a federal building that was self-insured by the government. So the only domestic act of terrorism that had resulted in an insurance payout was the 1993 bombing of the World Trade Center. The landscape has changed drastically since Sept. 11. The insurance industry has withdrawn terrorist insurance from 'all risk' policies'' (Creamer, May 6, 2002, pp. 1, 12).

scheme needs only a slight variation to fit the high-rise building: The building line is usually the first ring since, in an urban environment, the building line is adjacent to a public sidewalk, access to vertical transportation (stairs, escalators and elevators) is the second and individual floors or floor sections are the third'' (POA, 2000, p. 19-115).

The Protection of Assets Manual further states that within the high-rise structure there are ''three classes or types of interior spaces:

1. *Public access or common areas.* These include street-level entrance lobbies, main elevator lobbies, access routes to retail sales spaces [and restaurants, etc.] in the structure, promenades, mezzanines, and[,] increasingly in new buildings, atria.
2. *Rented or assigned occupancies* [i.e., tenant areas]. These are leased or owner-occupied spaces on the various floors. Depending on the occupant, such spaces may be open to public access during building hours, or may be restricted to identified and authorized persons.
3. *Maintenance spaces*. These include mechanical rooms and floors, communications and utilities access points, elevator machine rooms, janitorial closets and other spaces with strict limited access.'' (POA, 2000, p. 19-115)

Survey Checklist

To assist in the fact-finding process, it is helpful to use a checklist of areas to be covered. Such a checklist for a physical security survey is provided in Appendix 4-1. The main sections in this checklist are general information; site perimeter; building and building perimeter; maintenance spaces and communication/utility closets; loading dock/shipping and receiving areas; vehicular movement and parking areas; tenant offices; office computers*; cafeteria, kitchen, and dining areas; intrusion detection and duress alarms, closed-circuit television (CCTV), access control systems, metal detectors, and x-ray machines; key controls, locking devices, and containers; janitorial operation; security operation; security education; and insurance.

Every facility, organization, and site, however, is different, and therefore no generic checklist can possibly cover all aspects of the facility being surveyed. In carrying out the fact-finding process for the particular area being surveyed, one may select as much, or as little, of the suggested checklist as one needs. The scope or extent of the survey being conducted will determine the amount selected. As Gleckman (1995, p. 4) summarizes,

> A checklist should be made up by the survey team (for extensive surveys there may need to be more than one surveyor) in preparation for the actual inspection. This checklist will be used to facilitate the gathering of pertinent information. The checklist is considered to be the backbone of the security survey or audit.
> This checklist will serve to systematically guide the survey team through the areas that must be examined.

The fact-finding process should include taking notes or using a small voice recorder; also, it may be helpful to photograph various aspects of the site,

*Because a high-rise tenant may have a computer data center, Appendix 4-3, *Sample of an Appropriate Computer Security Program*, is included for informational purposes. If an in-depth review of computer systems is required an information systems professional should be consulted.

particularly problem areas. (Digital cameras are extremely useful because quality images can be easily obtained, digitally stored, and imported into a written report.) Before taking photographs, permission should be obtained from the appropriate building representative.

The fact-finding process, including planning the survey, will probably take 30 to 40 percent of the total time spent conducting the survey, while the other 60 to 70 percent will be spent writing the report.

Writing the Report

Writing the report will involve assembling the ideas and information obtained in the fact-finding investigative process. Weaknesses in the security program should indeed be pointed out and accompanied by recommendations to address them, but security strengths also should be identified. If a word processor is used to create the report, changes, modifications, and additions can be carried out in a relatively effortless manner. A standardized approach such as the following will help to properly organize this information into a logical and understandable format. Again, every facility, organization, and site is different, as is the scope of each survey, and individual surveyors will have their own specialized approaches. Hence, the suggested format is just that—a suggested one.

Title Pages

A typical title page indicates the confidentiality of the report, the name of the organization for whom the report is produced, the name of the site surveyed, the name of the person(s) by whom the survey and report is compiled, the date, and a notation of the copy number. The next page should list the number of copies of the report and to whom each copy is distributed.

Cover Letter

The cover letter should be addressed to the individual who commissioned the report. It includes a brief statement of the scope of the survey, thanks to individuals who assisted with the report, a mention of anything pertinent to this particular report, and where to direct any inquiries regarding the report's content.

Table of Contents

The table of contents is a listing by page number of all pertinent sections of the report.

Introduction

The introduction briefly states who commissioned the survey, why it was performed, and its scope. An example is as follows:

> Mrs. Shirley Thomas, Asset Manager, Pauley and Partners, requested this survey and report. The primary objective for conducting the survey was to review

strengths and weaknesses in the security program at the Pacific Tower Plaza high-rise complex, with reference, in particular, to after-hours access control of building occupants and the control of business and personal property leaving the site after normal business hours.

Method of Compilation

The method of compilation includes a description of how information was obtained for the survey, the names of individuals interviewed, a list of documents reviewed, and the period in which the survey was conducted. For example,

> The survey was conducted October 4–14, 2002, using information obtained from interviews with management personnel of Pauley and Partners; managers and supervisors of the security, engineering, janitorial, and parking departments; individual security staff members; and a representative of Columbus Insurance Company. In addition, information was obtained by reviewing the current security instructions, security incidents reported since January 1, 2002, police crime statistics for the general area surrounding the site, a Tenant Information Manual (issued to tenants by building management to explain building policies and procedures), and crime coverage insurance policies in effect at the site.

Identification of Assets

The tangible and intangible assets of the site should be identified with an estimation of their value and financial impact if they were to be lost, made inaccessible, or destroyed. Tangible assets include the people using the facility, the building itself, its fittings, and its equipment. In addition, within offices there will be equipment such as telephones, computers, word processors, printers, typewriters, fax machines, photocopiers, audio-visual equipment; general-use items such as coffee machines, vending machines, refrigerators, microwaves, ovens, and furniture; and sometimes antiques and works of art, cash, and negotiable instruments. Also, vehicles parked in the building's parking garage are tangible assets. Intangible assets include the livelihood of building users; intellectual property and information stored in paper files, reference books, photographs, microfilm, x-rays, and within computer systems and peripherals; and the reputation and status of the facility, including the ability of tenants to conduct business.

Description of the Site, Building, and Surrounding Areas*

The report should include a description of the site's size, zoning, boundaries, and landscaping; a description of the building, including any overpasses or subterranean passageways; the building's square footage, principal

---

*"Security programs for business establishments are often built around the existing physical design features of the building. . . . Design characteristics of the building will either increase or decrease the ability and opportunity of employees and customers to steal" (Post and Kingsbury, 1991, pp. 177, 178). This concept is commonly referred to as *crime prevention through environmental design* or

activities and usage, operating hours, and building population; nature of the surrounding area and occupancies; proximity to freeways, major roads, and public transportation terminals and stations; and the location of or expected response times from the nearest police and fire stations. Any available maps, floor plans, or site photographs may be noted at this point. The following is a sample description of a high-rise building and its surrounding area.

> Pacific Tower Plaza is a prestigious, multiple-tenant, multiple-use high-rise complex used primarily for commercial office purposes. It is typically operational from 7:00 AM to 7:00 PM, Monday to Friday, and 9:00 AM to 2:00 PM on Saturday. It has restricted access at all other times. It is located in Toluga Hills, a major downtown financial district. It occupies one half of the city block bounded by Mount Waverley, Poppyfields, and La Perouse Boulevards and is located close to the Southwestern Freeway. The Toluga Hills Police Department has a main station within 2 miles of the complex, and Toluga Hills Fire Department Station 3, located within three city blocks, has an expected response time of 3 minutes. A high-rise residential building, a low-rise hotel, and a high-rise office building surround it.
>
> Pacific Tower Plaza consists of a fully sprinklered 36-story office tower with a three-level subterranean parking garage. The tower has 600,000 square feet of rentable office space, 7000 square feet of rentable retail space, and 6000 square feet of rentable storage space. The approximate size of each floor plate (the plate being the entire floor area including the public access or common areas, tenant areas, and maintenance spaces) is 18,500 square feet. The perimeter of the building consists of sculptures, fountains, an open-air restaurant, and large planters containing small trees and flowers. The entrance to the building is through a large main lobby. The building has an approximate population of 2400 occupants and 500 daily visitors. The on-site parking structure can accommodate up to 600 cars and connects to a subterranean pedestrian tunnel under Mount Waverley Boulevard.
>
> The tower of Pacific Tower Plaza consists of steel-frame and concrete construction with metal stud partitions. It has a conventional curtain wall of glass in aluminum frames. The structural steel frame supports lightweight concrete floor slabs resting on metal decks atop horizontal steel beams, which are welded to vertical steel columns. The building is supported on a foundation of structurally reinforced concrete. The tower is designed with a concrete-reinforced center core that houses the electrical, plumbing, and communications systems; the heating and air-conditioning (air supply and return) shafts; 17 passenger elevators; one service/freight elevator; three parking shuttle elevators; and two major enclosed stairwells. Both stairwells provide egress to the street level and access to the roof (the doors are locked at the roof). The stairwells are pressurized and protected by fire-rated doors and walls.

CPTED—pronounced *sep-ted*. ''In its purest sense, CPTED is the passive use of the physical environment to reduce the opportunity for and fear of predatory stranger-to-stranger crime—burglary, robbery, assault, larceny, murder, rape, even bombing. CPTED relies on three main strategies: natural surveillance, natural access control, and territoriality—establishing boundaries and transitional spaces. CPTED looks at siting, landscaping, foot-prints, window schedules, facades, entrances, lobbies, layouts, lighting, materials, and traffic and circulation patterns'' (Post, 1995, p. 19).

Identification of Threats and Review of Past Incidents

Security and fire life safety threats to the assets are identified. This process should include a review of security-related incidents that have occurred at the site over a designated period. Daily activity and incident reports generated by security staff and police crime statistics for the reporting district encompassing the area should be considered.

In examining threats, consideration should also be given to those of neighboring facilities. For example, if an adjacent facility is a signature building at risk of an act of terrorism, this constitutes an indirect threat to the site being surveyed.

Security Measures and Recommendations

This section reviews the security measures currently in place to safeguard the assets. Areas that may be reviewed, depending on the scope of the survey, include perimeter barriers and fences; building construction and layout; lighting; intrusion detection and duress alarms; CCTV; mobile patrols; access control of vehicles, people, and property; identification badges; locking and key controls; trash removal procedures; personnel security; written procedures and policies; and communications. Strengths and weaknesses or vulnerabilities should be pointed out to provide a balanced view of the security program. Also, the security measures should be benchmarked, or evaluated relative to those measures commonly found in commercial office buildings, particularly those of neighboring ones. Recommendations should then be made for modifications or changes that reduce the risks to the assets. (Also, depending on the scope of the survey, monetary costs, if any, of the proposed recommendations might be included).

The following is an example of a security measure with associated recommendations for improvement.

> Access control of building occupants after normal business hours is determined by visual recognition of the tenants by the lobby security officer who then asks individuals authorized to enter to print their names, the name of the tenant by whom they are employed, and the date and time, and to sign their names on the after-hours building register. If the officer does not recognize an individual, a file of tenant occupants authorized for after-hours access is checked. If the individual is not listed there, a call is made to the tenant suite to ask if anyone can authorize the entry of the individual. If no tenant is available, the individual is denied access. This procedure has caused continual problems because of the repeated denial of entry to occupants who otherwise had permission from their employers to work in the building after hours. Two reasons for this have been the failure of tenants to provide up-to-date listings of employees authorized to work after normal business hours and the high turnover of security personnel leading to many staff lacking familiarity with building users.

Recommendations:

- Building management approach all tenants who are not providing up-to-date, after-hour authorization lists to re-emphasize the need for such critical information.

- Building management request that every tenant provide a list of key personnel who can be contacted after hours before any of their employees is denied after-hours access.
- Design an after-hours building access card and request that tenants issue the completed card to all their employees who need after-hours access.
- Obtain quotations from vendors to install a card access control system at the building.
- Investigate why the turnover of security staff is high.

Summary of Recommendations

This section is optional but may be included to summarize the findings of the survey. The recommendations for each security measure may be separately listed, for example, according to monetary cost, those planned for immediate attention, and those to be addressed at a future time. Also, there could be a ranking of the recommendations, listing first those which, if implemented, would result in the greatest overall improvement in the effectiveness of the security program; or the recommendations could be grouped into those providing low, medium, and high levels of security. Determining whether a particular security measure should be implemented will largely depend on the perceived vulnerability to the threat that the measure is designed to address and the anticipated consequences if the threat were actually to occur.

Executive Summary

This section is a summary of the report itself and should appear at its beginning. It provides the reader with a quick review of the survey and report by drawing attention to important items. A sample executive summary for Pacific Tower Plaza follows:

> The survey was conducted October 4–14, 2002. The primary objective for conducting this survey was to review the strengths and weaknesses in the security program at the Pacific Tower Plaza high-rise complex; in particular, reference is made to after-hours access control of building occupants and the control of business and personal property leaving the site after normal business hours.
>
> Interviews were conducted with management personnel of Pauley and Partners; managers and supervisors of the security, engineering, janitorial, and parking departments; individual security staff members; and a representative of Columbus Insurance Company.
>
> The survey revealed that building security staff has rigidly enforced after-hours access control procedures of the building. This has resulted in very few unauthorized persons gaining after-hours access to tenant offices but has led to the repeated denial of entry to occupants who otherwise had permission from their employers to work in the building after hours. The survey also revealed that there has been little control of business and personal property leaving the site after normal business hours. This factor is thought to have contributed considerably to the thefts of personal computers from secured tenant offices that has occurred since the building was opened on January 1, 2002.

These are some of the recommendations stemming from this survey for improving the effectiveness of the security program at Pacific Tower Plaza:

- Have building management approach all tenants who are not providing up-to-date, after-hour authorization lists to re-emphasize the need for such critical information.
- Have building management request that every tenant provide a list of key personnel who can be contacted after hours before any of their employees is denied after-hours access.
- Design an after-hours building access card and request that tenants issue the completed card to all their employees who need after-hours access.
- Obtain quotations from vendors to install a card access control system at the building.
- Design a property removal system to control the movement of business and personal property from the building. This system should be implemented as soon as possible after all tenants have been thoroughly informed of the new policy and their cooperation has been solicited in supporting it.
- Encourage tenant representatives to inventory office equipment and to identify it clearly.
- Encourage tenants to anchor items—personal computers and fax machines—using devices such as metal plates or steel cables. Also, laptops should be secured when they are not being used.
- Investigate why the turnover of security staff is high.

Building management representatives have indicated that they are very supportive of providing a sound security program for the tenants at Pacific Tower Plaza. They also appear willing, within reasonable cost constraints, to take whatever steps are necessary to achieve this goal.

Appendixes

Any back-up documentation to which the survey refers, reference material that may help support the suggested recommendations, floor plans, maps, diagrams, forms, and photographs may be included here to substantiate the work of the surveyor.

Presentation of the Report

Once the report is written it should be presented in an understandable manner that professionally reflects the work that has gone into preparing it. Each major section of the report should be tabbed and any photographs and drawings neatly mounted and labeled. The report should then be placed in a three-ringed binder or professionally bound.

If at all possible, the survey report should be personally presented to the parties requesting the project. Depending on the time allotted, one can be thorough or brief in presenting the material. For a formal presentation one may elect to use computer screen displays, overhead transparencies, slides, or simply a page-by-page review of the report. Such presentations can be of immense value in making salient points clear and understandable. Also, the opportunity for questions and clarification of issues will increase the chance that the recommendations and suggestions will be successfully implemented.

Fire Life Safety Survey

A fire life safety survey has very similar objectives to a security survey. Its aims are ''to ascertain the present [life safety] status, to identify deficiencies or excesses, to determine the [fire and life safety] protection needed, and to make recommendations to improve the overall [fire life safety]'' (Momboisse, 1968, p. 13) of the facility under evaluation.

A fire life safety survey also can be as extensive or as restricted as the surveyor determines. Like a formal security survey, a fire life safety survey will involve two major tasks: the fact-finding investigative process and the writing of the report that reflects the findings. Much of the work involved is the same as for a security survey. However, the fire life safety survey is predominantly concerned with life safety threats; it tends to focus on preventive measures to reduce the risk of such threats occurring.

Fact-Finding Process

The fact-finding process for the fire life safety survey resembles that of a security survey, with the following items being of particular importance:

1. The type of occupancy and classification of the facility, its principal activities, and the usage of the site are critical elements from a fire life safety perspective. For example, if the building has large numbers of occupants with disabilities, it may not be practical to rapidly evacuate them using stairwells.
2. A review of state and local building and fire prevention laws and codes for mandated fire life safety requirements is necessary to determine if the facility is in full compliance.
3. In reviewing documentation, the testing records of fire life safety equipment and systems and the Building Emergency Procedures Manual (described in Chapter 11) should be reviewed. The testing records need to be checked to ensure that testing is adequate, according to accepted practices, and is being conducted in a timely manner by certified persons or companies. The Building Emergency Procedures Manual should be examined to ascertain if it is accurate, up-to-date, and adequately covers all emergencies that have occurred or are likely to occur at the site.
4. Insurance policies need to be reviewed to determine whether present or planned fire life safety measures are of an acceptable level and the fire life safety systems and equipment meets the standards as outlined in the policies.

Survey Checklist

To assist in the fact-finding process it is helpful to use a checklist of areas to be covered. Such a checklist, emphasizing fire prevention, is provided in Appendix 4-2. The National Fire Protection Association's *Fire Protection Handbook* (Cote, 1997, p. xv) is organized around six major fire safety strategies in designing building fire safety: prevention of ignition, design to slow early fire growth, detection and alarm, suppression, confinement, and evacuation of occupants. The fire prevention survey checklist in Appendix 4-2 touches on these areas. However, it does not specifically address the design or fire-resistive construction aspects of a high-rise building, nor does it purport to cover all branches of the Fire Safety Concepts Tree used as a model by the National Fire Protection Association (NFPA 550, 1995 Edition). If other fire life safety surveys are to be conducted, the checklist will need to be modified to make it appropriate. The local fire department may require or recommend a particular form of inspection.

The fire prevention survey checklist in Appendix 4-2 is intended for use by a fire safety director, life safety manager, risk manager, security director, or other member of building management who desires to evaluate the fire prevention program in place at their high-rise facility. It may be used for several reasons:

1. To assist in analyzing the fire prevention program with respect to certain incidents that have occurred at the site
2. In preparation for a visit by the city or state fire marshal, a fire prevention inspector of the fire department having authority over the building, or a representative of the insurance company providing coverage for the building owner
3. As part of a regular self-inspection program carried out by the building's Fire Safety Director to ensure that the building's fire prevention program is adequate and properly maintained

If a more extensive analysis of the building fire life safety program is required, an outside consultant or specialist, such as a registered fire protection engineer, should be considered. Consultants or specialists will be discussed in detail later in this chapter.

In the fact-finding process, a thorough building walkthrough should be conducted with those individuals most knowledgeable of the building and its fire life safety systems. This person will probably be the Building Engineer and/or the Fire Safety Director. Start the walkthrough on the roof of the structure and proceed down the stairwells and throughout each floor of the building. The reason for starting on the roof is that it is easier to walk down than to walk up a high-rise building, particularly if one is surveying a 60-story skyscraper! When walking a floor, one usually will restrict the survey to public access or common areas such as the elevator lobbies and corridors, or maintenance spaces such as mechanical rooms, communications and utilities access points, elevator machine rooms, janitorial closets, paint rooms or paint storage rooms, and other spaces with strictly limited access. One will not tend to venture inside the tenant office space unless there is a particular reason to do so. Sufficient reasons would include past incidents of a fire life safety nature reported in the tenant space, a spot check of tenant housekeeping and storage of combustible materials, or a structural build-out or alteration of tenant space that has occurred. The primary emphasis of the walkthrough is to observe any obvious fire prevention problems or violations of fire life safety practices.

The main sections in this high-rise fire prevention survey checklist are general information; building information; building layout and exits;

cafeteria/kitchen; building emergency exit and evacuation signage; fire protective signaling systems; smoke control systems; fire suppression systems; other fire suppression systems; portable fire extinguishers; emergency and standby power and lighting systems; testing and maintenance of fire life safety systems; surface finishes of interior ceilings, floors, and walls; general housekeeping, storage procedures, and adherence to safety; fire guard operations; building emergency procedures manual or fire life safety plan; fire life safety education; and insurance. (See Appendix 4-2 for complete details.)

Once again, every facility, organization, and site is different and therefore no generic checklist can possibly cover all aspects of the facility being surveyed. During the fact-finding process one may select as much, or as little, of the suggested checklist as one needs. Depending on the scope of the survey, the final checklist may even be a combination of both security and fire life safety checklists.

Writing the Report

Writing the report will involve assembling the ideas and information obtained in the fact-finding investigative process. Weaknesses in the fire prevention program will be pointed out, with suggested recommendations to address them, but strengths also will be identified. The suggested format previously outlined for writing the security survey also can be adapted for writing the fire prevention survey.

Word of Caution

A word of caution, learned through the bitter school of experience: The surveyor should reserve professional opinions as to the state of the overall security and fire life safety programs until the fact-finding process and the writing of the report is nearing completion. Of course, there are exceptions to the rule, but, particularly with major surveys, one needs to assimilate the mountains of information collected before thoroughly understanding what is happening within the security and fire life safety programs. Often one aspect of the survey is closely interwoven with another. For example, in conducting a security survey to investigate theft occurring at a building, one may immediately conclude that the solution to the problem is to implement a strict screening procedure in the building main lobby to control property removal. At the time this may appear to be the complete solution to the problem. However, at a later stage in the survey it may be discovered that building tenants can use passenger elevators at any time to exit their floor and travel directly down to the under-building or subterranean parking garage, thereby bypassing the building main lobby and being able to walk unobserved to a vehicle. In this case, property removal controls in the building main lobby will not be totally effective unless other measures are incorporated into the security program. Such measures may include reprogramming the elevators, particularly after normal business hours, to descend from the tower and terminate service in the main lobby. Other elevators can be programmed to serve the lower parking levels. This arrangement will cause occupants to pass through the building's main lobby and thereby permit an effective property removal control procedure to be instituted in that area.

Use of Consultants and Specialists

In carrying out security and fire life safety surveys it may be advisable at times to use a consultant or specialist to conduct the survey or to analyze specific areas of the security and fire life safety programs. The International Association of Professional Security Consultants defines a consultant as ''a person who provides security advice, information, and recommendations to management'' (Sennewald, 1996, p. 6). A consultant or specialist is a person who, through some combination of study and experience, has acquired expertise in a particular discipline or area.

Reasons for Engaging a Consultant or Specialist

Some reasons for hiring a consultant or specialist to conduct a survey or to analyze specific areas of the security and fire life safety programs follow:

1. The consultant or specialist is very knowledgeable in state-of-the-art security or fire life safety systems and code compliance issues and is experienced in conducting surveys or analyses of the specific areas in which objective professional advice is required. According to David Aggleton, CPP, president of Aggleton & Associates, New York City,

   > My area of business is analyzing client's security needs and developing applicable solutions to their vulnerabilities, mostly in the area of security technology.... As technology gets more complex, the security directors, human resources directors, facilities directors, whoever is responsible for security, don't keep up with the technology applications and need help to understand what is out there and how it should be applied.... In my opinion, the role of consultants is to educate them to understand what the process is, how they analyze what they need, how they get where they want. They need someone in their corner to help them do that. (''The care and feeding of a security consultant,'' 1998, p. 69)

2. The consultant or specialist is already employed by the manufacturers or distributors of the security or fire life safety equipment installed or planned for installation or by the security contractor supplying personnel at the building. This person may be well acquainted with the site and the issues that need to be addressed. Of course, if manufacturers or distributors of equipment or the contract security provider employ the consultant or specialist, there is always a risk that the person may not be completely objective and may present recommendations not specifically geared to the client's needs.
3. At the time the survey or analysis is needed, there may be no person within the building operation who has the expertise or time to perform the task within the required period.
4. The individuals who have the authority to implement the recommendations of a survey or analysis have previously been made aware of what is needed but, for whatever reasons, do not want to accept the advice of the person(s) who brought these matters to their attention. Also, it may be that a particular security or fire life safety problem with several possible solutions has

provoked disagreement within management as to what is the best course of action.

5. The consultant or specialist has a well-established professional relationship with local law enforcement or the fire authority having jurisdiction, and therefore is able to achieve certain objectives that others cannot.
6. The consultant or specialist may have certain professional qualifications or certifications that would qualify him or her to be called, in the event of future litigation, as an expert witness to testify on behalf of the building owner.

Issues to Consider

Those who hire a consultant* or specialist to conduct the survey or to analyze specific areas of the security and fire life safety programs should adhere to the following procedures:

1. Request a resume of the consultant or specialist and review his or her education, qualifications, professional experience, and professional affiliations. Examine any potential conflict of interest on the part of the consultant or specialist. Check client references.
2. Determine if the consultant or specialist has the necessary skills to carry out the project.
3. Be sure the scope of the project is clearly communicated to the consultant or specialist by the individual(s) requesting the project.
4. Have the consultant or specialist submit a written proposal of how the project is to be carried out, how long it is expected to take, and what form the final written report will take. This proposal should also address how costs of the project will be handled. (A total fixed cost may be proposed for the project, or hourly or daily costs may be quoted; in addition, transportation, accommodation, and administrative costs may be specified for separate billing. A retainer fee may be stipulated on acceptance of the proposal or commencement of the work, with additional regular payments scheduled during the project.)
5. When the terms of the agreement are accepted, draw up a written contract, including the above proposal and incidental items such as a confidentiality agreement. Once the contract is fully executed, the work should commence as outlined in the agreement.

Sources of Consultants and Specialists

A consultant or specialist may be selected from a number of sources. There are individuals and consulting firms that specialize in providing consulting services. Also, there are professional groups—ASIS International, the National Fire Protection Association (NFPA), the Society of Fire Protection Engineers (SFPE), the International Association of Professional Security Consultants (IAPSC), the Society of Certified Fraud Examiners (SCFE), and the International Professional Security Association (IPSA) incorporating the Institute of Industrial Security—whose members are consultants. With the exception of

*__Note:__ An excellent reference for information on consultant's fees, expenses, proposals, and contracts is *Security Consulting*, 2nd ed., by Charles A. Sennewald (1996).

the last group, which primarily serves security interests outside of the United States, these groups can be contacted through local chapters. Others such as the Institute of Real Estate Management (IREM) and the Building Owners and Managers Association International (BOMA) are also sources within the high-rise building community.

Publications such as ASIS *Security Management* and the NFPA *Fire Journal* are filled with articles written by security and fire safety practitioners, some of whom provide consulting services. The ASIS *Security Industry Buyers Guide* provides consulting services listed by business sector and primary specialty. The NFPA *Journal Buyer's Guide* lists fire protection consultants arranged by state and country and designates specialties. Local, county, and state law enforcement and crime prevention departments, local and county fire prevention departments, and the local fire marshal will be most amenable to providing information and possible lists of consultants and specialists.

Referrals of consultants or specialists may also come from the manufacturers and distributors of security and fire life safety equipment, or from representatives of the contract security company providing services at the building. A careful screening process can drastically reduce the risk that such persons may not be fully objective and totally geared to the client's needs. Finally, personal recommendations of a consultant or specialist may come from other security directors, fire safety directors, risk managers, building owners and managers, and insurance agents.

Summary

Security and fire life safety surveys are invaluable in helping high-rise building owners, managers, security and life safety directors, and consultants effectively and safely operate high-rise buildings, and thereby reduce premises liability. The survey is an essential tool to identify specific assets and the threats to those assets, assess vulnerabilities or weaknesses to such threats, and devise measures to counter such weaknesses. To conduct a thorough analysis of a facility, it is helpful that it be carried out in a methodical fashion. If the expertise for such a task does not exist on site, the selection of a professional consultant or specialist is vital.

References

Aggleton, David G., comments in ''Review of Proposal for Revisions to *High-Rise Security and Fire Life Safety*'' (November 2001).

ASIS, *Security Industry Buyers Guide,* 2002 Edition (American Society for Industrial Security, 1625 Prince Street, Alexandria, VA 22314).

Broder, James F., *Risk Analysis and the Security Survey*, 2nd ed. (Butterworth-Heinemann, Woburn, MA, 2000).

CAP Index, Inc., Information Brochure (CAP Index, Inc., 150 John Robert Thomas Drive, Exton, PA 19341; available at: http://www.capindex.com).

''The care and feeding of a security consultant,'' moderated by Steve Lasky, publisher/editor, *Security Technology & Design Magazine* (Cumming, GA, December 1998).

Cote, Arthur E., *Fire Protection Handbook*, 18th ed. Editor-in-Chief, Arthur E. Cote, Managing Editor, Jim L. Linville (All NFPA material in this chapter is used by permission. National Fire Protection Association, Quincy, MA, Copyright 1997).

Creamer, David E., ''Are the terrorists winning?'' (*California Real Estate Journal*, Los Angeles, May 6, 2002).

Dalton, Dennis R., *The Art of Successful Security Management* (Butterworth–Heinemann, Woburn, MA, 1998).

Fischer, Robert J., and Gion Green, ''Risk analysis and the security survey,'' *Introduction to Security*, 6th ed. (Butterworth–Heinemann, Stoneham, MA, 1998).

Gips, Michael A., ''Building in terrorism's shadow,'' a May 2000 *Security Management* magazine article re-published in Counterterrorism and Contingency Planning Guide (A special publication from *Security Management* and ASIS International, Arlington, VA, post September 11, 2001).

Gleckman, Mark, *The Security Survey* (Security Management Services, Acton, CA, 1995).

Gottlieb, Michael, ''High profile'' (*California Real Estate Journal*, Los Angeles, April 8, 2002).

Healy, R. J., *Design for Security*, 2nd ed. (John Wiley & Sons, New York, 1983), see especially Chapter 3. As quoted in ''High-rise structures, Section B, Security considerations,'' *Protection of Assets Manual*, vol. III. Editor, Timothy L. Williams (Used with permission of POA Publishing, LLC, Los Angeles, 323/663-4887. Original copyright from the Merritt Company, 1991).

IREM, ''Terrorism insurance'' (Institute of Real Estate Management, Chicago, IL, 2002).

Israel, Paul, *Life Lessons from Thomas Alva Edison*. Interview of the associate editor of the Thomas A. Edison Papers at Rutgers University by Bottom Line. (Boulder, CO, April 15, 1994). (Volumes I and II of the Edison papers are available from the Johns Hopkins University Press, Baltimore.)

Kaminsky, Alan, *A Complete Guide to Premises Security Litigation*, 2nd ed. (American Bar Association, Chicago, 2001).

Kitteringham, Glen, CPP, ''Pinpointing problems: using two-dimensional mapping to determine security risks at a multi-use highrise complex'' (*Canadian Security*, Canada, December 2001).

Momboisse, Raymond M., *Industrial Security for Strikes, Riots and Disasters.* (Charles C. Thomas, Springfield, IL, 1968).

NFPA *Journal Buyer's Guide* (National Fire Protection Association, Quincy, MA. Copyright 2002).

NFPA 550, *Guide to the Firesafety Concepts Tree* (National Fire Protection Association, Quincy, MA. Copyright 1995).

POA, ''High-rise structures, section B, security considerations,'' *Protection of Assets Manual.* (Used with permission of POA Publishing, LLC, Los Angeles, 323/663-4887. Original copyright from the Merritt Company, 1991).

Post, Nadine M., ''More than merely cops and robbers,'' *Engineering News-Record* (The McGraw-Hill Construction Weekly, May 1, 1995).

Post, Richard S., and Arthur A. Kingsbury; revised by Richard S. Post with Arthur A. Kingsbury and David A. Schachtsiek, *Security Administration: an Introduction to the Protective Services*, 4th ed. (Butterworth–Heinemann, Stoneham MA, 1991).

Sennewald, Charles A., *Security Consulting*, 2nd ed., (Butterworth–Heinemann, Newton, MA, 1996).

Walsh, Timothy J., ''Security and managing risk,'' *POA Bulletin* (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887, May 1999).

Additional Reading

Broder, James F., *Risk Analysis and the Security Survey*, 2nd ed. (Butterworth–Heinemann, Woburn, MA, 2000).
Sennewald, Charles A., *Security Consulting*, 2nd ed. (Butterworth–Heinemann, Boston, 1996).

Appendix 4-1 Physical Security Survey Checklist

Facility name
Address (including zip code)
Client representatives and telephone numbers
Position and title of persons interviewed
Survey date

I. General Information

Name of building owner and/or management company (names and telephone numbers)
Name, job title, and telephone number of person in charge of security
Principal activities
Operating hours
Number of tenants and building occupants
Approximate number of daily visitors
Nature of surrounding area and occupancies (noting any particular security hazards)
Proximity to freeways and major roads
Address and telephone number of police jurisdiction
Name and rank of police contact
Number of police personnel
Are crime statistics available and for what period?
Is there a business-community–based crime prevention program in place?
Of what does it consist?
Is the facility in general compliance with Americans with Disabilities Act (ADA) requirements?

Comments

II. Site Perimeter

1. Are there any bus terminals, train stations, and taxi stations close-by?
2. Acreage of site
3. What is the landscaping?
   Are there natural barriers present?
   Is shrubbery kept well pruned so as not to provide concealed hiding places?
4. Is there a perimeter barrier?
   What sort?
   Height
   Condition
   Distance of barrier from building
   Are there clear areas on either side of the perimeter barrier?
   Is there public parking and/or metered parking directly adjacent to the building?
   Are signs posted to make the public aware of towing policies and the planned removal of unauthorized vehicles?
5. What types of perimeter lights are used?
   Do they meet minimum requirements of local codes and ordinances?
   Are lights directed toward the perimeter?
   Are all exterior doorways, walkways, and entries properly illuminated?
   Are exterior guard posts properly illuminated?
   Are there dark areas where criminals may conceal themselves?
   What additional lighting is required to illuminate these areas?
   Is lighting on an automatic timer system?
   Are the lights in operation during all hours of darkness?
   Is exterior lighting protected against theft and vandalism?
   Are any obstructions, such as tree branches, blocking the lighting?
   Is the lighting system regularly checked?
   By whom?
   Is there an emergency lighting system for use in the event of a power failure?
6. Are there perimeter intrusion detection systems?
   What types are they?
   Does the system function properly?
   Is it adequate?
   Who monitors these alarms?
   What is the response procedure when an alarm occurs?
   Whose responsibility is it to switch the alarm system off and on?
   When alarm points are bypassed are there procedures in place to ensure that they are later returned to service?

7. Is CCTV used?
   Are cameras black and white or color?
   Are cameras analog or digital?
   List the camera positions
   Do any cameras need to be relocated?
   What cameras are equipped with auto iris and with pan, tilt, and zoom mechanisms?
   Are outside cameras enclosed in weatherproof casings?
   Are cameras adequately secured to deter theft or interference?
   Is lighting adequate for cameras?
   Who is responsible for monitoring the cameras?
   Are cameras linked to recording equipment?
   What type of video recording equipment (videocassette recorder [VCR] or digital video recorder [DVR]) is used?
   If a VCR is used, is there an adequate library of videotapes? For how long are tapes kept?
8. Is there access control of vehicles and pedestrians?
   Are sign-in and sign-out logs, identification badges, or electronic access systems used?
   If used, describe these logs, identification badges, or access control systems.
   Is there a process for allowing tenants to provide advance notification of visitors?
9. Are visitors, delivery persons, and contractors issued identification badges?
   Are these badges easily distinguished?
   If time-sensitive temporary badges (for example, those that automatically fade when their expiration period is reached) are not used, how are temporary badges collected from the users?
   Are these people escorted?
10. What patrols are conducted of the site perimeter?
    During what hours?
    What is their frequency?
    Who conducts the patrols?
    Are the patrol personnel in uniform?
    Are they equipped with portable two-way radios?
    Do they require flashlights?
    Are the patrols recorded?
    How are the patrols recorded (notebooks, reports, guard tour systems)?
    Who reviews the records of these patrols?
    Are the objectives of the patrols clearly outlined in written instructions?
11. How is trash stored and removed from the site?
    Are transparent trash bags used?
    Are boxes and cartons flattened before being removed?
    Is trash removal supervised?
    By whom?
12. Is a property removal pass system used?
    How does it work?
    Who issues property removal passes?
    Who is authorized to sign passes?
    Are the passes checked to ensure they are correctly filled out?
    Who reviews the passes when property is being removed?
    Is the pass system effective?
13. Is there a control system for property brought onto the site?
    How does it work?
    Is it effective?
14. Is there a package control system for packages brought onto the site?
15. How is lost and found property handled?
    Where is found property stored for safe keeping?
    For how long is it stored?
    How is it disposed of?

Comments

III. Building and Building Perimeter

1. Height
   Number of floors (above and below ground level)
2. Total square footage of building
   Typical floor size in square feet
3. Type of construction
   Is it frame construction?
   Is it tube construction?
4. Presence of atriums, mezzanines, etc.
5. Are ''Right to Pass by Permission. Permission Revocable at Any Time''–type signs or sidewalk plates installed?
6. Description of perimeter entrances and exits (including tunnels or overhead walkways)
   Construction of doors, door frames, and hinges

State of door locking mechanisms
Are they self-closing?
If they have automatic closing devices, do they function correctly?

7. Are outside power transformers and other utilities properly secured?
8. Are heating, ventilating, and air conditioning systems accessible from outside the building?
9. Are ground floor windows protected?
10. Number of stairwells and configuration
Is there roof access for each stairwell?
11. Are stairwell doors self-closing and self-latching?
Are all stairwell doors on upper floors kept closed and locked from inside the stairwell?
Which doors are locked and which are permanently unlocked?
Are stairwell doors equipped with door position switches to indicate when doors are in the opened or closed position?
Are stairwell doors (particularly those at the ground or exit level) equipped with audible exit alarms?
Are the doors at the ground or exit level equipped with time-delayed lock release mechanisms?
What is the time delay?
Do CCTV cameras with recording capabilities monitor these doors?
12. Is there a common interconnected locking system on the stairwell doors?
If so, does it automatically unlock during a fire alarm (i.e., is it a fail-safe system)?
Are there manual controls for unlocking all stairwell doors simultaneously? Where are these manual controls located?
13. Are there emergency telephones or intercoms located inside the stairwells?
On what floors?
14. Are public restrooms kept locked at all times?
Who controls access to them?
Are doors equipped with self-closing and self-latching devices?
15. Is access to building windows possible from adjacent rooftops?
Is access from the roof possible?
Is there a helipad or heliport?
Is there notification of incoming flights?
What type of lighting is used?
16. What types of perimeter lights are used?
Do they meet the minimum requirements of local codes and ordinances?
Are lights directed toward the perimeter?
Are all exterior doorways, walkways, entries, and elevator lobbies properly illuminated?
Are there any dark areas where criminals may conceal themselves?
What additional lighting is required to illuminate these areas?
Is lighting on an automatic timer system?
Are the lights in operation during all hours of darkness?
Is exterior lighting protected against theft and vandalism?
Are there any obstructions, such as tree branches, blocking the lighting?
Is the lighting system regularly inspected?
By whom?
17. Is the interior lighting of the building adequate?
Is there adequate lighting in corridors, exits, and stairwells?
18. Is there an emergency lighting system for use in the event of a power failure?
What lights are on it?
19. Are all exits and entrances supervised (including shipping and receiving/loading dock and basement areas)?
If not, how are they controlled?
Are sign-in and sign-out logs, identification badges, or electronic access systems used?
If used, describe these logs, identification badges, or access control systems.
Is there a process for allowing tenants to provide advance notification of visitors?
Are visitors, delivery persons, and contractors issued identification badges?
Are these badges easily distinguished?
If time-sensitive temporary badges (for example, those that automatically fade when their expiration period is reached) are not used, how are temporary badges collected from the users?
20. Are there intrusion detection systems?
What types are they?
Who monitors the alarms?
What is the procedure on receipt of an alarm?

Whose responsibility is it to switch the alarm system off and on?
When alarm points are bypassed are there procedures in place to insure that they are later returned to service?

21. Is CCTV used?
    Are cameras black and white or color?
    Are cameras analog or digital?
    List the camera positions
    Do any cameras need to be relocated?
    What cameras are equipped with auto iris and with pan, tilt, and zoom mechanisms?
    Are outside cameras enclosed in weatherproof casings?
    Are cameras adequately secured to deter theft or interference?
    Is lighting adequate for cameras?
    Who is responsible for monitoring the cameras?
    Are cameras linked to recording equipment?
    What type of video recording equipment (VCR or DVR) is used?
    If a videocassette recorder (VCR) is used, is there an adequate library of videotapes? For how long are tapes kept?
22. What patrols are conducted of the building perimeter?
    During what hours?
    What is their frequency?
    Who conducts the patrols?
    Are the patrol personnel in uniform?
    Are they equipped with portable two-way radios?
    Do they require flashlights?
    Are the patrols recorded?
    How are the patrols recorded (notebooks, reports, guard tour systems)?
    Who reviews the records of these patrols?
    Are the objectives of the patrols clearly outlined in written instructions?
23. Presence of internal staircases, dumb-waiters, and rubbish/trash chutes?
24. Elevators and their configuration
    Can elevators be placed ''on security'' to deny access to specific floors?
    Are elevators equipped with electronic access control devices (card readers)?
25. How is trash stored and removed from the site?
    Are transparent trash bags used?
    Are boxes and cartons flattened before being removed?
    Is its removal supervised and by whom?
26. Is a property removal pass system used?
    How does it work?
    Who issues property passes?
    Who is authorized to sign passes?
    Are the passes checked to ensure they are correctly filled out?
    Who reviews the passes when property is being removed?
    Is the pass system effective?
27. Is there a control system for property brought into the building?
    How does it work?
    Is it effective?
28. How is lost and found property handled?
    Where is found property stored for safekeeping?
    How long is it kept?
    How is it disposed of?

Comments

IV. Maintenance Spaces and Communication/Utility Closets

1. Is access to these areas controlled?
2. What sorts of controls exist?
   Are escorts provided for outside vendors accessing these areas?
   Is a sign-in and sign-out procedure used?
3. Who controls this access?
4. Who periodically checks the adherence to these controls?
5. Are regular checks made of these areas?

Comments

V. Loading Dock/Shipping and Receiving Areas

1. Are shipping and receiving areas physically separated?
2. Is the platform height sufficient (usually 48 inches or 1.2 meters) so the truck bed is closely parallel to the dock?

Is there an adjustable height (mechanically or electrically operated) dock leveler?

3. Is a supervisor present whenever the areas are open?
   Are these staff rotated to deter possible collusion with or favoritism to delivery persons?
4. Are all vehicles logged in and out?
5. Are vehicles inspected before entering under-building or subterranean loading docks?
6. Who is permitted to move vehicles?
   Are persons who move vehicles properly trained and licensed?
   Are persons who move vehicles covered by adequate vehicle insurance?
7. Are keys left in vehicles?
   If not, where are they secured?
8. Are the movements of vehicle drivers and delivery people restricted in this area?
   Are pedestrians allowed to enter these areas?
9. Are rest areas, toilet facilities, pay phones, etc., provided?
   Are restrooms kept locked?
   Who controls access to them?
   Are doors equipped with self-closing and self-latching devices?
10. Are drivers and delivery persons allowed to enter the building to carry out deliveries?
    Are these persons required to leave some identification such as a driver's license?
    Are these persons required to wear special ID tags when in the building?
11. What vehicles, other than those for delivery and pick-up, are permitted to park in these areas?
12. Is the dock area properly secured after normal business hours?
13. Are vehicles or deliveries received after closing hours?
    If so, how is this achieved?
14. Is lighting provided for the dock areas?
    What types of lights are used?
    Are all exterior doorways, walkways, entries, and elevator lobbies properly illuminated?
    Is the dock area painted in light colors to enhance reflection?
    Do dark areas need additional lighting?
    What additional lighting is required to illuminate these areas?
    Is lighting on an automatic timer system?
    Are the lights in operation during all hours of darkness?
    Is exterior lighting protected against theft and vandalism?
    Is the lighting system regularly inspected? By whom?
    Is there an emergency lighting system for use in the event of a power failure?
15. Is CCTV used?
    Are cameras black and white or color?
    Are cameras analog or digital?
    List the camera positions
    Do any cameras need to be relocated?
    Are there cameras located at ingress and egress points of the dock areas?
    If so, do these cameras provide images of vehicle license plates?
    What cameras are equipped with auto iris and with pan, tilt, and zoom mechanisms?
    Are outside cameras enclosed in weatherproof casings?
    Are cameras adequately secured to deter theft or interference?
    Is lighting adequate for cameras?
    Who is responsible for monitoring the cameras?
    Are cameras linked to recording equipment?
    What type of video recording equipment (VCR or DVR) is used?
    If a VCR is used, is there an adequate library of videotapes? For how long are tapes kept?

Comments

VI. Vehicular Movement and Parking Areas

1. Is there a parking structure or parking area?
   Is it a public or private parking area?
   Who operates the facility (the building owner or manager or a parking contractor)?
2. Are entrances and exits limited in number as practicable and always attended when open?

Are all exterior doors securely locked in compliance with local building and fire life safety codes?
Are the ground floor and second floor (if accessible) completely enclosed?
Do trees allow access to upper levels?
Is shrubbery kept well pruned so as not to provide concealed hiding places?

3. Are there designated parking areas for tenants, employees, visitors, contractors, couriers, and disabled persons?
   Is the correct use of these designated spaces enforced?
   Are there designated parking spaces for building executives with their names displayed (names should not be displayed)?
   Are parking areas well marked for easy recognition by drivers as to where their vehicles are parked?
   Estimated number of vehicles parked daily
4. How is vehicle access controlled?
   Is the parking operation self-parking, attendant or valet parking, or both?
   Are there any height or weight restrictions?
   Are access cards, tickets, passes, or decals used?
5. Are vehicles inspected on entry or exit?
6. Does the garage have automatic opening and closing doors?
   If so, within how many seconds of a vehicle passing through do the doors begin to close?
   Is this considered safe in restricting unauthorized vehicle or pedestrian access?
7. Are security officers or law enforcement officers involved in directing traffic?
8. Are speed bumps installed?
   Are speed dots installed to deter vehicles from straying into the path of oncoming vehicles, particularly at corners and curves?
9. Are speed limit signs posted?
   What is the speed limit?
10. Are stairwell doors self-closing and self-latching?
    Are stairwell doors on upper levels kept locked from the stairshaft side?
11. Is lighting provided for the parking areas?
    Does it meet minimum requirements of local codes and ordinances?
    What types of lights are used?
    Are all exterior doorways, walkways, entries, and elevator lobbies properly illuminated?
    Is the interior of the structure painted in light colors to enhance reflection?
    Are there dark areas where criminals may conceal themselves?
    What additional lighting is required to illuminate these areas?
    Is lighting on an automatic timer system?
    Are the lights in operation during all hours?
    Is exterior lighting protected against theft and vandalism?
    Is the lighting system regularly inspected? By whom?
    Is there an emergency lighting system for use in the event of a power failure?
12. Are security mirrors used for drivers to view vehicles around corners or obstacles?
    Are they in the correct locations?
13. Is CCTV used?
    Are cameras black and white or color?
    Are cameras analog or digital?
    List the camera positions
    Do any cameras need to be relocated?
    Are there cameras located at all ingress and egress points of the parking areas?
    If so, do these cameras provide images of drivers and vehicle license plates?
    What cameras are equipped with auto iris and with pan, tilt, and zoom mechanisms?
    Are outside cameras enclosed in weatherproof casings?
    Are cameras adequately secured to deter theft or interference?
    Is lighting adequate for cameras?
    Are cameras properly monitored?
    Are cameras linked to recording equipment?
    What type of video recording equipment (VCR or DVR) is used?
    If a VCR is used, is there an adequate library of videotapes? For how long are tapes kept?
14. Are there emergency intercoms or call stations in the parking garage or parking areas?

What are their locations? Are there sufficient numbers in strategic locations (including stairwells)?
Are signs prominently posted to depict their locations?
Are the intercoms or call stations readily accessible to disabled persons?
Are the parking cashiers' booths equipped with duress alarms?
To what area do these intercoms, call stations, or duress alarms report?
Are they constantly monitored?
How often is their operation checked and by whom?

15. What patrols of parking areas are conducted?
    Are they performed at irregular intervals?
    What is their frequency?
    If parking stalls are angled, are patrols in a direction that permits a maximum view between parked vehicles?
    Who conducts the patrols?
    Are these personnel in uniform?
    Are they equipped with portable two-way radios?
    Are the patrols recorded?
    How are the patrols recorded (written reports, guard tour systems, etc.)?
    Who reviews the records of these patrols?
    Are the objectives of the patrols clearly outlined in written instructions?
16. What is the policy for handling abandoned vehicles?
17. What is the policy for assisting persons who lock themselves out of their vehicles?
18. How is lost and found property handled?
19. If restrooms are provided, are they kept locked at all times?
    Are doors self-closing and self-latching?
    Who is allowed to use them? Who controls access to them?

Comments

VII. Tenant Offices

1. At which areas are receptionists controlling access?
   Have the receptionists been trained in security procedures and awareness, including how to handle threatening situations?
   Which entrances are not controlled and can be accessed?
   Is an after-hours sign-in register kept?
2. Is interior lighting adequate?
   Is there adequate lighting in corridors and exits?
3. Are duress alarms provided in reception and other sensitive areas?
   To what area do these alarms report?
   Who responds to these alarms?
   Are these alarms and response times regularly tested? By whom?
4. Is CCTV used?
   Are cameras black and white or color?
   Are cameras analog or digital?
   List the camera positions
   Do any cameras need to be relocated?
   What cameras are equipped with auto iris and with pan, tilt, and zoom mechanisms?
   Are the cameras adequately secured to deter theft or interference?
   Is lighting adequate for the cameras?
   Who is responsible for monitoring the cameras?
   Are cameras linked to recording equipment?
   What type of video recording equipment (VCR or DVR) is used?
   If a VCR is used, is there an adequate library of videotapes? How long are tapes kept?
5. Are tenant employees issued identification badges?
   Are they color-coded to denote authorized access to particular areas?
   Are employees required to visibly display them at all times?
   What is the procedure when employees forget to wear or lose their badges?
   When employees resign or are terminated, what procedure ensures badges are returned to the issuer?
   Is the inventory of additional badges stored securely?
6. Are visitors, delivery persons, maintenance people, and contractors required to sign in?
   Are they required to wear identification badges?
   Are these badges easily distinguished?
   If time-sensitive temporary badges (for example, those that automatically fade

when their expiration period is reached) are not used, how are temporary badges collected from the users?
Are these people escorted when inside the tenant space?

7. Are exterior, unsupervised doors kept closed during normal office hours?
   Is someone designated to ensure the exterior doors are all locked at the end of normal business hours?
8. Do perimeter walls, and interior walls leading to sensitive areas, extend from the floor to the ceiling?
   If not, is the space between the top of the wall and the floor above fitted with steel bars and/or intrusion detection alarms?
   If rods are used, is it required (and practical) to periodically inspect them, to ensure they are still in place?
9. Is it possible for an intruder to use heating, ventilating, and air conditioning ducts as a means of entering the tenant office or interior room?
   If so, are the ducts fitted with steel bars and/or intrusion detection alarms?
   If rods are used, is it required (and practical) to periodically inspect them, to ensure they are still in place?
10. For particularly sensitive areas, are heating, ventilating, and air conditioning ducts leading to the areas periodically checked for listening devices and surveillance cameras?
    Does the degree of security required justify fitting the area concerned with a separate heating, ventilating, and air conditioning system?
11. Is there a concealed space between the ceiling and the floor above?
    In particularly sensitive areas, is this space periodically checked for listening devices or surveillance cameras?
12. Is after-hours access to the tenant's office controlled?
    Who controls the issuance of keys, access cards, or electronic access codes?
    When employees are terminated, are keys and cards retrieved and codes changed?
    Are unused keys and access cards properly secured?
    Are sign-in and sign-out logs, identification badges, or electronic access systems used?
    If used, describe these logs, identification badges, or access control systems.
13. Does the freight/service elevator provide direct access to tenant offices?
14. Are individual interior offices kept locked when not in use?
    What is the state of door-locking mechanisms?
15. Are equipment rooms kept locked at all times?
16. Are common area restrooms kept locked at all times?
17. Does the tenant's office have intrusion detection alarms?
    Of what do they consist?
    Who monitors these alarms?
    Who responds to these alarms?
    Whose responsibility is it to switch the alarm system off and on?
    When alarm points are bypassed are there procedures in place to ensure that they are later returned to service?
18. Where is petty cash kept and how is its use controlled?
    Are unsigned and any pre-signed checks properly secured?
    At the end of daily business are petty cash and checks counted?
19. How and where is sensitive information stored and secured?
    What type of file cabinets and safes are used?
    Do they provide sufficient protection considering the sensitivity of the information stored within them?
    Are file cabinets and safes kept locked?
    Are safes located in areas where they can be easily observed?
    Are they properly bolted to the floor?
    Are there any intrusion detection systems to protect safes, cabinets, etc.? Who monitors and responds to them?
    How often is an inventory of sensitive information conducted and by whom?
20. Before leaving for the day, are employees required to clear desk and work surfaces?
21. Is there awareness by management of the importance of safeguarding sensitive proprietary information?
    Is there an established procedure for destroying sensitive information when it becomes trash?
    Who oversees this?

22. After meetings or conferences involving sensitive information is the meeting area cleaned of all working material and the trash properly discarded?
23. Are all new hires required to complete a ''confidentiality of proprietary'' information agreement?
24. Are pre-employment background investigations carried out for all personnel (including temporary employees)?
    What is the extent of these investigations?
    Who conducts these investigations?
25. Is a security orientation given to all new employees (including temporaries)?
    Who conducts this orientation?
    Is ongoing security education provided for employees (particularly regarding any changes in the security program and any criminal incidents or security problems of which they should be aware)?
    Are company security rules posted or distributed to all employees?
    Are they easy to understand?
26. On termination of employment are exit interviews conducted?
    Who conducts them?
    Is a check carried out to ensure all keys, identification cards, credit cards, pagers, mobile telephones, and all other company property has been retrieved? Are access codes belonging to this person immediately changed?
    Are other employees notified of the termination?
27. Are special security measures taken for tenant executives?
    Is access to the executive offices controlled?
    Are duress alarms installed in executive offices?
    Who monitors and responds to these alarms?
    Are these alarms and response times regularly tested? By whom?
    Do executives have an emergency escape route or access to a safe room?
    Are executives briefed on security precautions for home, travel, and business?
28. Are photocopiers and FAX machines equipped with recorders to monitor their usage?
    Can these machines be used after normal business hours?
    Are postage meters locked up after normal business hours?
29. Are telephone bills regularly reviewed for possible misuse?
30. Are after-hour escorts provided?
    Who conducts the escorts?
31. Is a property removal pass system used?
    How does it work?
    Who issues property removal passes?
    Who is authorized to sign passes?
    Are the passes checked to ensure they are correctly filled out?
    Who reviews the passes when property is being removed?
    Is the pass system effective?
32. Is there a control system for property brought into the tenant space?
    How does it work?
    Is it effective?
33. Is there a separate mailroom?
    Does the mailroom have a separate HVAC system?
    Are screenings conducted of mail envelopes, packages, and parcels?
    Are the screening procedures sufficient for the security risks involved?
    Are the mailroom staff properly trained in security procedures?
    Who trains the mailroom staff?
34. How is lost and found property handled?
    Where is found property stored for safekeeping?
    How long is it kept?
    How is it disposed of?
35. If there are security problems within the office, who handles them?

Comments

VIII. Office Computers

1. Is office equipment clearly and permanently identified and inventoried?
   Are high-value items physically secured?
   Are desktop personal computers anchored using devices such as metal plates or steel cables?
   Are desktop personal computers, laptop, and notebook computers kept locked up when unattended?
   Are passwords used to limit access?
   Are data files backed up daily?

Are copies of data backups, program backups, and forms kept at an off-site location?

2. Does the office have local area network (LAN) and wide area network (WAN) systems?
   Are there physical security measures to protect the workstations and the file server?
   Is privacy of user-ID and passwords maintained?
   Is a trusted, well-trained individual in charge of controlling access to programs and data?
   Do networks have dial-up access?
   Are compromises of the systems immediately and thoroughly investigated?
3. Does the office have a mainframe* computer installation?
   Is access to this area tightly controlled?
   How is it controlled?
   Is a trusted, well-trained individual in charge of controlling access to programs and data?
   How is processed information protected?
   How is the removal of property and information controlled?
   How is the destruction and disposal of material supervised?
   Are back-up records made of sensitive information, with copies stored on- and off-site?
   Is there a separation of staff working on system development and system operations?
   Are changes to the computer system formally controlled and authorized?
   Is there an Emergency Plan for the facility?
   Of what does it consist?

Comments

IX. Cafeteria, Kitchen, and Dining Areas

1. What are the cafeteria, kitchen, and dining area operating hours?
2. Who operates them and who has responsibility for their security?
3. How are cash, voucher tickets, etc., handled?
4. Are spot checks made of the cashiers?
5. If a safe is used to store cash and receipts, is it in an area where it can be observed easily?
   Is it bolted to the ground?
6. Are administrative offices locked after hours?
   Who has keys to them?
7. Are storage rooms and refrigerators properly secured, particularly after hours?
   How often is an inventory conducted and by whom?
8. Is anyone permitted to be in the dining area(s) after the cafeteria is closed?
9. How is the disposal of waste food trash handled?
10. Are periodic checks made to ensure ''good'' food is not being removed as trash?
11. Are all vending machines properly secured and their use strictly monitored?
12. Is there any equipment that needs to be monitored after hours to prevent food spoilage?
    Who monitors this equipment?

Comments

X. Intrusion Detection and Duress Alarms, Closed-Circuit Television, Access Control Systems, Metal Detectors, and X-Ray Machines

1. Are intrusion detection devices used?
   What are their types, locations, and manufacturers?
   Does leaving alarmed doors open defeat the security system (for example, magnetic contacts on stairwell doors)?
   How are these alarms monitored (local, central station type, etc.)?
   What is the established procedure when an alarm is received?
   Are up-to-date lists kept of personnel authorized to open and close alarmed areas?
   Are duress (or panic) alarms used?
   Where are they installed?
   How frequently are these alarms tested?

*Since a high-rise tenant may have a computer data center, Appendix 4-3, *Sample of an Appropriate Computer Security Program*, is included for informational purposes. If an in-depth view of computer systems is required, an information systems professional should be consulted.

3. Is CCTV used?
   Are cameras black and white or color?
   Are cameras analog or digital?
   What cameras are equipped with auto iris and with pan, tilt, and zoom mechanisms?
   Are outside cameras enclosed in weatherproof housings?
   Are cameras adequately secured to deter theft or being interfered with?
   Is lighting adequate for cameras?
   Who is responsible for monitoring the cameras?
   Are cameras linked to recording equipment?
   What type of video recording equipment (VCR or DVR) is used?
   If a VCR is used, is there an adequate library of videotapes? For how long are tapes kept?
4. Are mechanical and electronic access systems used?
   If so, describe these systems.
   Where are the devices located?
   If electronic access cards are used, what types are they (Magnetic Stripe, Barium Ferrite, Wiegand, Proximity, or Smart)?
   Do the cards have photographs?
   Does the access control system record unauthorized attempts to gain access?
   Who is responsible for programming and deleting cards?
   When employees resign or are terminated what procedure ensures badges are returned to the issuer?
   Is the inventory of additional badges stored securely?
5. Are biometric access control systems used?
   If so, describe these systems
6. Are intrusion detection, CCTV, and access control systems integrated?
7. Are intrusion detection, CCTV, and access control systems properly maintained (and equipment problems documented)?
   Are the security alarm, CCTV, and access control systems inspected and tested on a regular basis (and this documented)?
8. Is there dial-up access to the security systems software?
   If such access is available, is caller verification required?
9. Are metal detectors used?
   Are they properly calibrated?
   If so, is there a sufficient number of security personnel to operate them?
10. Are X-ray machines used?
    If so, is there a sufficient number of security personnel to operate them?
    Are these personnel properly trained?

Comments

XI. Key Controls, Locking Devices, and Containers*

1. Is there a grand master, master, and sub-master system in use? Describe it.
2. Is there a common interconnected locking system on emergency exit stairwell doors?
3. Are locks throughout the facility by the same manufacturer?
4. Is there a record of lock issuance?
5. Is there a record of key issuance and inspection?
6. How many grand master and master keys are in existence?
7. What is the security of grand master and master keys?
8. What is the security of the key cabinet or box?
9. Who is charged with handling key control?
   Describe the control system.
   Is the system adequate?
   What is the frequency of record and key inspections?
10. Are keys made at the site?
    Who makes them?
11. What is the type of lock used?
    Are all adequate in construction?
12. Would keys be difficult to duplicate?
    Are they marked ''DO NOT DUPLICATE'' to deter unauthorized duplication?
13. Are locks changed periodically at critical locations?
14. Are any ''sesame'' padlocks used for classified material storage areas or containers?
15. If a key-cutting machine is used, is it properly secured?
16. Are key blanks adequately secured?

*This list is adapted from James F. Broder, *Risk Analysis and the Security Survey,* 2nd ed. (Butterworth–Heinemann, Woburn, MA, 2000).

17. Are investigations made when master keys are lost?
18. Are locks immediately replaced when keys are lost?
19. Do locks have interchangeable cores?
    Are extra cores properly safeguarded?
20. Are combination locks the three-position type?
21. How many people possess combinations to safes and containers?
22. How often are combinations changed?
23. How are combinations chosen?
    Are lazy-man combinations used?
    Are birth dates, marriage dates, etc. used as combinations?
24. Are combinations recorded where they might be accessible to an intruder?
25. Have all faces of the container locked with a combination lock been examined to see if the combination is recorded?
26. Are combinations recorded and properly secured so that authorized persons can get them in an emergency?
27. Is the same or greater security afforded recorded combinations as that provided by the lock?

Comments

XII. Janitorial Operation

1. Who is responsible for the janitorial operation (name, job title, and telephone number)?
2. Are outside contract or building in-house employees used?
   Are their backgrounds checked (including, as a minimum, past employment and personal references)?
3. What are the hours of operation?
4. How are janitorial staff supervised?
   Are janitorial staff required to wear a distinctive uniform and photo ID cards?
   Is the supervision adequate considering the sensitivity of the area being cleaned?
   Are staff escorted when working in particular areas?
5. Do they possess keys?
6. How are keys controlled?
7. What method of cleaning is used (individual janitors assigned to particular areas or gang cleaning)?
8. Do the janitors lock exterior doors when they are working after hours in tenant offices?
9. Do the janitors lock interior doors when they have finished cleaning?
10. Are transparent trash bags used?
    Are spot checks made of trash bags?
11. How is trash removed from the floors?
    By whom?
12. Is trash temporarily stored at the site?
    How long is it stored?
13. Is the trash placed in a dumpster, compactor, etc.?
    Is the compactor properly secured when not in use (also a safety issue)?
    Is an escort provided for janitorial employees when they bring trash to the dumpster or compactor?
    Is the dumpster or compactor under CCTV surveillance?
14. How is trash removed from the site?
    Are boxes and cartons flattened before being removed?
    Is trash removal supervised and by whom?
    If billing is based on number of loads removed, is this spot checked against billings?
15. Are janitors permitted to use stairwells?
16. Where do they take meal breaks?
17. Are they permitted to go to their private vehicles during breaks?
    Do these vehicles provide unsupervised egress from the building or site?
18. Are janitorial supplies kept properly secured?
19. Does janitorial equipment being used always remain in the building?
20. Are the janitorial staff trained in security awareness?
21. Are janitorial supervisors informed in a timely manner of theft activity occurring in tenant areas?
22. Are janitorial staff searched and/or their personal belongings checked when they leave the site?

Comments

XIII. Security Operation

1. Are outside contract or proprietary (in-house) employees used?

2. If a contract company is used is it properly licensed?
   Does it carry adequate liability insurance?
3. Are security personnel properly licensed (including required state licenses to operate as a guard, or to carry a weapon, baton, mace, pepper spray, etc.)?
4. Do they wear uniforms?
5. Are the wages and benefits of security staff specified in the contract?
6. How are security staff selected?
   Are the requirements (such as physical and mental capabilities, special skills, and training) for security staff clearly defined and documented?
7. Are background checks conducted?
   If a contractor is used, do they certify that the required background checks have been conducted?
8. What are the posts?
   What are the hours of operation?
   How many security staff per shift (day, swing, and graveyard)?
   What duties do they perform?
   Is the level of staffing adequate?
9. Are there adequate written procedures, job descriptions, instructions, and reports?
   Do the instructions coincide with actual practices and accurately reflect building policy?
   Are the instructions sufficient in content and accuracy?
   Are the instructions current and subject to at least annual reviews?
   Are emergency contact lists kept up to date?
10. Are security-related incidents documented and logged?
    Is a database system used?
    Are reports (and logs) kept for sufficient periods of time?
    Are these reports regularly reviewed to ascertain any significant trends in activity?
11. How are security staff supervised?
    Are patrol monitoring devices utilized?
    Who checks them?
    How long are these records kept for possible future use?
12. If the security staff comprises contract employees, how much training do they receive before coming on-site?
    What type of initial training do security staff receive at the site?
    What type of follow-up and ongoing training do security staff receive?
    Does this training satisfy mandatory state requirements?
    How is the effectiveness of training measured?
13. If radios are used for communications, how effective are they?
    Do other departments share frequencies?
    Is there a channel designated for emergency communications?

Comments

XIV. Security Education

1. Do new occupants receive security education from the building staff or is this a tenant responsibility?
   If so, of what does this training consist?
2. What training do building management, engineering, janitorial, and parking staffs receive?
   Who conducts this training?
   How often is it provided?
3. Are building staff and tenants kept informed of changes in the security program and of criminal incidents or security problems of which they should be aware?

Comments

XV. Insurance

1. Has the insurance policy for the applicable area been reviewed?
2. Is the policy still in effect?
3. Is there satisfactory compliance with the conditions of the policy?
4. Is the insurance policy adequate in terms of the present risks?
5. What is the total coverage?
6. What is the deductible?
7. If the policy is a specified peril contract, are there any possible perils that have not been adequately covered?
8. What have been the claims over the past year?
9. Should the insurance policy be revised?

Comments

Appendix 4-2 Fire Prevention Survey Checklist

Facility name
Address (including zip code)
Owner (name and telephone number)
Client representative (name and telephone number)
Position and title of persons interviewed
Survey date

I. General Information

Building owner and/or management company (names and telephone numbers)
Fire Safety Director and alternate (names and telephone numbers)
When was the building constructed?
Principal activities
Operating hours
Number of tenants and building occupants
Approximate number of daily visitors
Special usage features (large numbers of occupants with disabilities, restaurant on top floor, etc.)
Nature of surrounding area and occupancies (noting any particular fire hazards)
Location of nearest street fire alarm box (if provided)
Location of fire hydrants in relation to the building
Address and telephone number of nearest fire department jurisdiction (first and second alarm responders)
Travel time for each fire department responder to the site
Is there a mutual aid agreement with other fire department jurisdictions?
Is site and building access both suitable and available for responding emergency personnel and vehicles?
Are address numbers adequate and plainly visible from the roadway the building faces?
Are building keys for fire department use kept in a locked container or rapid entry box?
When were the keys last inspected to ensure all keys are present and correctly tagged?
Where is the rapid entry box located?
Does the rapid entry box also contain building information?
What information?
Is a Building Emergency Procedures Manual readily available for fire department use?
Is the facility in general compliance with ADA requirements?

Comments

II. Building Information

1. Type of occupancy
2. Utilities (electricity, water, gas)
   Location of utility shut-offs
3. Heating, ventilating, and air conditioning system
   Type of heat (gas or oil)
4. Height
   Number of floors (above and below ground level)
5. Total square footage of building
   Typical floor size in square feet
6. Type of construction
   Is it frame construction?
   Is it tube construction?
7. Presence of atriums, mezzanines, etc.
8. Type of building exterior (conventional curtain wall?)
   What type of fireproofing is provided for the structure?
9. Certificate of occupancy
   Where is it posted?
   Certificates for places of assembly (list places and approved capacities)
   Fire department licenses or permits
   Are licenses and permits up-to-date?

Comments

III. Building Layout and Exits

1. Description of perimeter entrances and exits (including any tunnels or overhead walkways)
   Construction of doors and hinges
   Are all doors in good working condition?

State of door locking mechanisms
Do exits open out?
Are they self-closing?
If they have automatic closing devices, do they function correctly?

2. Are there exterior fire escapes with fire escape drop ladders, exterior fire towers, or enclosed stairwells?
   What are their locations?
   List the floors they serve (including roof access)
3. Are there two means of egress from each floor?
4. Are the emergency exit doors leading to fire towers or enclosed stairs kept closed?
   Are any objects, such as pieces of metal, wood, or doorstoppers, used to keep them open?
5. Fire-resistive rating of stairwell walls and doors? Hourly rating?
   Are stairwell doors in good working condition?
   Are stairwell doors self-closing and self-latching?
   Are there any obstructions of pathways leading to emergency exits?
   Inside the stairwells, are there any obstructions to egress or storage of any flammable materials?
6. Are all the emergency exit doors kept closed and locked from inside the stairwell?
   Which doors are locked and which are left permanently unlocked?
   Are emergency exit doors (particularly at the ground or exit level) equipped with audible exit alarm devices? How often are these alarms checked and by whom?
   Are these doors equipped with time-delayed lock release mechanisms at the ground or exit level?
   What is the time delay?
   Do CCTV cameras with recording capabilities monitor these doors?
7. Is there a common interconnected locking system on emergency exit stairwell doors?
   If so, does it automatically unlock during a fire alarm (i.e., is it a fail-safe system)?
   Are there manual controls for unlocking all stairwell doors simultaneously?
   Where are these manual controls located?
8. Is there a helipad or heliport?
   What type of lighting is used?
   Is there notification of incoming flights?
9. Are there handrails in the stairwells? Are they secure and smooth?
   What is the condition of stair treads?
   Is there glow-in-the-dark tape or photo-luminescent paint on stair treads, handrails, or the perimeters of stairwell doors?
10. Is there a telephone or another two-way emergency communications system located inside the stairwells?
    On what floors are they located?
    Who monitors these communication devices?
    Is their operation regularly tested?
11. What types of perimeter lights are used?
    Does it meet minimum requirements of local codes and ordinances?
    Are lights directed toward the perimeter?
    Are all exterior doorways, walkways, and entries properly illuminated?
    Do dark areas need additional lighting?
    What additional lighting is required to illuminate these areas?
    Is lighting on an automatic timer system?
    Are the lights in operation during all hours of darkness?
    Is exterior lighting protected against theft and vandalism?
    Are there obstructions, such as tree branches, blocking the lighting?
    Is the lighting system regularly inspected? By whom?
12. Is interior lighting of the building adequate?
    Is there adequate lighting in corridors, exits, and stairwells?
13. Is there an emergency lighting system for use in the event of a power failure?
    Are there any battery-operated lighting units that automatically activate on failure of power?
    Are these units in good working condition?
14. Are there any internal staircases, vents, dumbwaiters, etc.?
    Is their interior covering noncombustible?
    What is the condition of stair treads?
15. Layout of elevators and the floors they serve
    Are elevator lobbies enclosed with self-closing doors?
    Where are elevator control devices located (inside or outside the cab, Building Control Station, etc.)?

Is the operation of elevator emergency telephones or intercoms regularly tested? How often? By whom?

Comments

IV. Cafeteria/Kitchen

1. Where is it located?
2. What sort of fuel is used?
3. Are ovens, stoves, and fryers properly maintained and kept free of built-up combustible residues?
4. What is the condition of cooking equipment, hoods, vents, ducts, etc.?
   Are kitchen exhaust hoods properly protected?
   Are they clean?
5. What type of fire protection equipment is supplied?
   Are the cafeteria/kitchen staff trained in its use?
   Is the kitchen fire suppression system inspected and serviced annually?
6. Is refrigerating equipment used?
   How is it housed?
   What refrigerant is used?
   What is the condition of the refrigerator motor?
   Is the area properly vented?
7. Is the cafeteria/kitchen area maintained according to local fire safety codes and regulations?

Comments

V. Building Emergency Exit and Evacuation Signage

1. Where are building emergency exit and evacuation signs located?
2. Are there sufficient directional exit signs?
   Are any damaged or missing?
   Are there low-level exit signs?
   How are they illuminated (natural or artificial lighting)?
   Can they be read easily?
   Are there any lighted signs that are not working?
3. Are evacuation routes adequately posted?
4. Does signage inside the elevator lobbies display adequate information (such as floor plan, exit routes, what stairwells have roof access, building name and address, floor number, fire department and building emergency telephone numbers, fire alarm looks like and sounds like, symbols depicting locations of fire equipment and manual fire alarm stations, and a warning: ''IN CASE OF FIRE USE STAIRWAY FOR EXIT. DO NOT USE ELEVATOR'')?
   Is signage correctly mounted?
   Are there any defaced or missing signs?
5. Does signage inside the stairwell display adequate information (including stairwell number, floor number, and the upper-most and lowest floors the stairwell serves)?
   Is it correctly mounted?
   Are there any signs defaced or missing?
   At which levels are signs inside stairwells located (every floor)?
   Is the signage inside the stairwell designed and positioned in accordance with local codes and regulations?

Comments

VI. Fire Protective Signaling Systems

1. Fire alarm system type and manufacturer? Location?
2. Off-site monitoring of the fire alarm system?
   How?
3. Types of initiation devices (smoke detectors, heat detectors, manual fire alarm stations, water flow, special systems)?
4. Types of smoke detectors (ionization and photoelectric)?
   Where are they located?
   Does activation of an elevator lobby smoke detector automatically cause elevators serving that floor to travel to a predetermined floor? Which floor?
   If the elevator detector is activated on the floor to which it is designed to relocate, is there a secondary relocation floor?
5. Types of heat detectors (fixed-temperature, rate compensation, rate-of-rise, combination, etc.)?
   Where are they located?
6. Types of gas detectors, if any?
7. Manual fire alarm sending stations (manual fire alarm stations, manual pull stations, etc.)?
   Where are they located?

8. Types of waterflow alarms (mechanically or electrically operated)?
   Where are they located?
9. If there is a parking structure, are there roll-down gates and doors with fusible links located on each level?
10. Is there anything special about the fire protective signaling systems?
11. What is the sound of the local fire alarm (siren, slow whoop, gong, bells, horns, etc.)?
    Is there also a visual alarm signal such as flashing lights?
    On what floors does the alarm annunciate (example, on fire floor, one above and below, two above and below)?
12. Where do the building fire protective signaling systems annunciate (local, off-site central station)?
    Is there a Building Control Station, a Central Control Station, a Control Center, a Fire Command Center, or a Fire Control Room?
    Where is it located? What equipment and systems does it contain?
    Is annunciation of the alarm achieved by means of an audible signal and visual display (which indicates the floor or other designated area and the type of device from which the signal originated)?
    Who monitors the alarms? Are they monitored 24 hours per day, 7 days per week?
    What is the established procedure when an alarm is received (including when and how the fire department is notified)?
13. How are system trouble alarms handled?
14. Is the emergency notification list of personnel up-to-date?
15. What building voice communication systems are available (public address system, intercom, phone, etc.)?
    If there is a public address system, does it reach all areas of the building (public access or common areas, elevators, stairwells, parking areas, maintenance spaces, and tenant areas)?
    Are prerecorded tape messages used to notify occupants of building emergencies?
16. Do building management personnel have two-way radio communication, pagers, etc.?
17. What building communication system is available for responding fire departments (sound-powered phones, two-way electrically supervised phone system, radios)?

Comments

VII. Smoke Control Systems

1. Is there a heating, ventilating, and air conditioning (HVAC) or air conditioning and ventilating (ACV) system?
   Is it a complete system serving the entire building, or are there separate systems for zones or individual areas?
   Description of system
   Location of intakes
   What causes it to shut off?
   How are smoke and fire dampers controlled?
2. When a fire alarm occurs, does the air handling system automatically shut down?
   On what floor(s)?
   In what areas?
   Is the smoke vented out?
3. Are the stairwells automatically pressurized when a fire alarm occurs?
4. Is there a mechanical smoke removal system?
5. Can windows installed in the exterior walls be manually opened?
6. Are windows installed in the exterior walls fitted with tempered glass?
   Which ones?
   How are these windows identified?
7. Are there automatic closing fire assemblies for all elevator lobbies?

Comments

VIII. Fire Suppression Systems

1. Is there an automatic sprinkler system (or more than one)?
   What floors and areas does it serve?
2. What causes the activation of a sprinkler head?
   Is there any obstruction of sprinkler heads? (Material should be stored no closer than 18 inches or 0.5 meters from the ceiling.)

3. Is there anything special about this system (linkage to other systems which must activate before discharge occurs, etc.)?
   Is the system supervised? How?
4. What class of standpipe and hose system is installed (Class I, II, or III)?
   Where are the hose connections for these systems?
   What is the condition of hoses and nozzles?
5. What type of standpipe and hose system is installed (wet standpipe or dry standpipe)?
6. Are standpipe and sprinkler system control valves secured in the open position?
   Are these shut-off valves visible and accessible?
7. What are the locations of fire department connections to sprinkler systems and/or standpipe systems on the building's exterior?
   Are they accessible, clearly marked, and fitted with protective caps?
8. Where are the fire pumps located?
   What is the system pressure?
   What is the suction pressure?
   What engine drives the pump(s) (electric or internal combustion)?
   Is it in the automatic mode?
   If internal combustion, what type and quantity of on-site fuel supply is available?
   Is this supply acceptable to the fire authority having jurisdiction?
9. Are jockey pumps available to maintain system pressure?
   Where are they located?
10. What on-site water supply is available if the principal water supply fails?
    Is this supply acceptable to the fire authority having jurisdiction?

Comments

IX. Other Fire Suppression Systems

1. Are there other fire extinguishing systems (carbon dioxide, halon or halon substitute, dry and wet chemical, etc.)?
2. Where exactly are they located?
3. How are these systems monitored?

Comments

X. Portable Fire Extinguishers

1. What types of extinguishers are located in public access or common areas?
   Where exactly are they located?
   Are they in sufficient numbers?
2. What types of extinguishers are located in maintenance spaces?
   Where exactly are they located?
3. What types of extinguishers are located inside tenant areas?
   Where exactly are they located?
4. Are these types of extinguishers applicable for the type of hazard for which they would be used?
5. Is their type of use clearly marked?
6. Are sufficient numbers provided?
7. What is the condition of the extinguishers?
8. Can they be accessed easily?
   Are they properly mounted?
   Is there adequate clearance for all fire extinguishers?
   Do those housed in recessed cabinets have approved breakable fronts to deter vandalism and theft?
9. Is there a procedure for visually checking them monthly (or more frequently, if required by local code)?
   Are they checked annually to ensure that they are fully charged and operational?
   When were they last checked?
10. Are building emergency staff and occupants properly trained to use them?

Comments

XI. Emergency and Standby Power and Lighting Systems

1. What types of emergency and standby power systems are available?
   Location?
   What is the size of the generator?
   What systems and areas does the power system serve?
   What causes this alternate power system to operate? (Does it automatically transfer to emergency power?)
   How long after a power failure is it placed into operation?
   How long can this alternate power source provide power to its rated load without being refueled?

When was the alternate power system last submitted to a full load test?
2. Are there other separate battery-operated lighting units that automatically activate on failure of power?
   Are all these units in good working condition?
3. Does the emergency lighting adequately illuminate paths of egress?

Comments

XII. Testing and Maintenance of Fire Life Safety Systems

1. What are the current procedures for testing and maintenance of fire life safety systems?
   What systems are tested on a monthly basis?
   What systems are tested on a semiannual basis?
   What systems are tested on an annual basis?
2. Has the fire authority having jurisdiction approved the testing and maintenance procedures?
3. When were the fire life safety systems last tested?
4. Does a certified tester carry out testing?
5. Are adequate records being kept of this testing and maintenance?
6. What contracts are in effect for cleaning cooking equipment and hoods, for testing and maintaining the fire protective systems, and for testing and recharging fire extinguishers?

Comments

XIII. Surface Finishes of Interior Ceilings, Floors, and Walls

1. Are walls, ceilings, and floor finishes of proper rating?
2. Is fire-resistant acoustical ceiling tile used?
   Where is it used?
   Were any samples taken for testing?
   When the plenum space is part of the heating, ventilating, and air conditioning system, have any of the tiles been displaced to increase the flow of air to a particular area?
   Have tiles been removed and replaced with non–fire-resistant tiles?
   Have any of the tiles been damaged?
3. What type of covering is on the floor?
4. Are the wall coverings safe (no non-rated paneling, carpet material, straw or matting, fabric, etc.)?
   Were any samples taken for testing?

Comments

XIV. General Housekeeping, Storage Procedures, and Adherence to Safety

1. Are ''NO SMOKING'' signs posted?
   Are smoking areas clearly marked? Are they equipped with non-tip ashtrays, metal waste receptacles, and fire extinguishers?
   Are smoking rules and regulations being observed? (Are there telltale signs of cigarette butts in the stairwells?)
2. What is the general standard of housekeeping?
   Are areas kept neat and clean?
   What areas are not?
   Are accumulations of lint, dust, and grease removed?
   What areas have excessive amounts of combustibles?
3. Are flammable materials (including paints and oily rags) correctly labeled and safely stored in approved containers away from combustibles?
   Is combustible waste stored in proper and approved containers?
   Any materials stored on the exterior of the building?
   Any piles of refuse, waste paper, furniture, etc.?
   What locations were observed to have unsatisfactory housekeeping?
4. Are patrols conducted to inspect housekeeping?
   Are patrols conducted to inspect for electrical appliances such as coffee pots, portable heaters, cooking equipment, etc., left on?
   Are tenant spaces inspected at the end of each business day?
   What is their frequency?
   Who conducts the patrols?

Are the patrols recorded?
How are the patrols recorded (notebooks, reports, guard tour systems)?
Are the objectives of the patrols clearly outlined in written instructions?

5. Are maintenance spaces (particularly telephone closets, electrical, and mechanical rooms), corridors, and stairwells checked to ensure these areas are not being used for storage or as temporary offices?
6. Are there any obstructions of pathways leading to emergency exits (no storage of files, furniture, etc.)?
   Fire doors not wedged or blocked open, especially at stairwell?
   Inside the stairwells are there any obstructions to egress (obstacles, storage, debris)?
   Stairwells, corridors, and exits free of trip and slip hazards (no holes, loose tiles, torn carpeting, defective mats)?
7. Is there any obstruction of sprinkler heads (material should be stored no closer than 18 inches or 0.5 meters from the ceiling)?
8. Is there any poke-through construction in floors, ceilings, and walls, which has not been properly sealed with fire-rated material?
9. Are there examples of worn insulation on cords, cords under carpets or mats or running across doorways, missing or cracked face-plates, too many electrical cords for outlets (octopus), temporary wiring, or the incorrect use of electrical equipment?
   Are heat-producing appliances well ventilated?
   Is electrical equipment turned off when not in use?
   Is malfunctioning electrical equipment immediately reported or taken out of service?
   Is there adequate clearance of electrical power switch panels and power closets?
   Are electrical power panels, switch, and fuse cabinets in common areas properly secured?
   Are junction boxes covered?
10. How is rubbish/trash removed from tenant spaces?
    With what frequency?
    Are trash bags ever temporarily stored where they may obstruct elevator vestibule door closing devices?
    Is combustible trash placed in proper and approved containers?
11. Are rubbish/trash chutes used?
    Are the chutes properly vented?
    Are they enclosed with self-closing doors?
    Are they lined with noncombustible materials?
    Are fire protection signaling systems located in the chutes?
    Are there automatic sprinkler systems inside the chutes?
12. Are there covered metal containers provided for rubbish and other materials in the loading dock area?
13. Is a trash compactor provided?
    Is its operating mechanism kept locked when not in use?
    Is a fire extinguisher located close to it?
14. Are materials stacked so as not to tip or fall?
    Is there safe storage on top shelves (height, weight, and bulk restricted)?
    Are aisles between shelves kept clear?
    Are all welding activities strictly controlled to insure strict compliance with fire safety precautions?

Comments

XV. Fire Guard Operations

1. Does the authority having jurisdiction require fire guards?
   What are their hours of operation?
   How many staff per shift?
2. What fire protection duties do they perform?
3. Are patrols conducted and what is their frequency?
   Describe the patrols.
   How are the patrols recorded (written reports, guard tour systems, etc.)?
4. If a firewatch is required, how many floors need to be continuously patrolled over what period of time?
5. Are there written procedures, instructions, and reports?
   Are the instructions current and sufficient in content and accuracy?

6. How are the staff supervised?
7. If radios are used for communications, how effective are they?
   Is there a channel designated for emergency communications?
8. What type of training do staff receive?
   How is the effectiveness of this training measured?
9. If the staff comprises contract employees, how much fire protective training do they receive before coming on-site?

Comments

XVI. Building Emergency Procedures Manual or Fire Life Safety Plan

1. Does the building have a Building Emergency Procedures Manual?
2. If so, what material does it contain and is it sufficiently detailed?
3. Does it thoroughly describe building fire life systems and equipment?
4. Does it address each emergency that is most likely to occur at the site?
5. Does it outline the Building Emergency Organization?
6. Does it list the specific duties of each team member both during normal business hours and after normal business hours?
7. Is the manual up-to-date?
   Are floor warden positions fully staffed?
8. Has the local authority having jurisdiction certified the manual?
9. Where is it located for easy access by the responding fire department?
10. Who is responsible for implementing and maintaining the manual and plan?
    Is the plan regularly tested?
    Are training records maintained?
11. Whose responsibility is it to make emergency public address announcements to building occupants?
12. What is the established evacuation or relocation procedure?
    Which floors usually evacuate during a fire alarm?
    How many floors do occupants usually travel down?
    What are the designated safe refuge areas inside and outside the building?
    How is the evacuation of disabled persons handled?

Comments

XVII. Fire Life Safety Education

1. Are all new building occupants given fire life safety training?
   Of what does this training consist?
   Does it include instruction in the use of portable fire extinguishers?
   How soon after the occupant commences work at the building is this training available?
   Does it include instruction about the safe use of electrical appliances such as coffee pots, portable heaters, toasters, etc., and the need to comply with smoking regulations?
   Do the occupants receive printed instruction?
   What ongoing fire life safety training education is available for occupants?
2. Is a tenant floor warden program in place?
   Are floor warden positions fully staffed?
   Are there alternate floor wardens?
   Do the floor wardens receive printed instruction such as a Floor Warden Manual?
   Are they provided with distinguishing attire (armbands, vests, hard hats, etc.)?
3. How often are fire life safety records updated?
   How regularly is the list of floor wardens and alternates updated?
   How regularly are lists of non-ambulatory or disabled persons updated?
4. Are fire drills for all building occupants regularly conducted in accordance with local laws and codes?
   How often?
   When was the last drill conducted?
   Who conducts the drills?
   Are records maintained of these drills?
5. What training do building management, engineering, security, parking, and janitorial staff receive?
   Does it include instruction in the use of portable fire extinguishers?
   Do staff on all shifts receive training?
   Is it conducted in any foreign languages?

How often is it provided?
Who conducts this training?
6. Are the records of fire life safety training kept in a protected area?

Comments

XVIII. Insurance

1. Has the fire insurance policy been reviewed?
2. Is the policy still in effect?
3. Is there satisfactory compliance with the conditions of the policy?
4. Is the insurance policy adequate in terms of the present risks?
5. What is the total coverage?
6. What is the deductible?
7. Is insurance for business interruption included?
8. What have been the claims over the past year?
9. Should the insurance policy be revised?

Comments

Appendix 4-3 Sample of an Appropriate Computer Security Program

I. Physical Protection

A. Responsibilities. The manager of the facility in which a computer data center will be installed should be responsible for advising on the construction of the computer data center, including environmental security support systems. The manager of the computer data center also should be responsible for the proper maintenance of all security support systems.

B. Standard Practices

1. Location. A computer data center should be located away from outside walls, clear of any piping, and in areas of the building not subject to rising or falling water. If it is not possible to avoid locations containing such hazards, special precautions must be taken to protect the equipment.
2. Construction. A computer data center should be constructed in accordance with applicable building codes and the applicable NFPA standards. Partition walls and ceilings should be constructed of fire-retardant material. The primary access to the machine room should be from an anteroom under environmental control, rather than from a public corridor.

   If the machine room floor is constructed of raised metal panels, the panels should form a National Electrical Manufacturers Association (NEMA)–rated enclosure for electrical power cables and interconnection cables between computer system components. Machine rooms containing raised floors also should include a ramp to provide a means of installing and removing equipment and to meet Americans with Disabilities (ADA) requirements.
3. Air Conditioning. Air temperature, humidity, and flow for the enclosed area should be designed to conform with local codes for basic room office environments, as well as with the manufacturer's cooling/heat dissipation requirements for major components. If a vendor's requirements for temperature, humidity, or airflow are more stringent than the local codes, the vendor's specifications should apply.
4. Electrical Service. Electrical service should be provided from a central distribution panel dedicated to the computer room area. This panel should be located within the controlled access area. The sizes and locations of incoming service, panel, and breakers should conform with national and local electrical codes and the hardware vendor's specifications. Emergency Power Off (EPO) switches that can cause immediate power-down of the mainframe computer operation should be well labeled and equipped with protective covers to reduce the chance of accidental activation.
5. Telecommunications. Telecommunications services should be provided by a dedicated cable direct from the building distribution frame. No service for any telephones or equipment, other than those in the machine room, should be connected to this cable. In complex teleprocessing installations, a NEMA-rated metal enclosure should be provided to house the modems and interconnecting and access equipment.

Source: From ''Computer Security'' in *Security Managers Desk Reference* by Richard S. Post and David A. Schachtsiek (Butterworth–Heinemann, Stoneham, MA, 1986), pp. 348–356. Minor revisions and/or additions have been made to enhance or make the material more readable.

6. Fire Suppression. The manager of a computer data center should evaluate the need for permanent fire suppression equipment over and above local code requirements. However, acquisition of such equipment should be approved by the Director of Security and the Building Fire Safety Director. In addition to any permanent suppression equipment, a data center also should have portable extinguishers of the proper size and type according to NFPA guidelines.
7. Fire and Smoke Detection. Computer data centers also should be equipped with UL-listed smoke detectors installed in sufficient numbers to provide proper coverage based on local codes or manufacturers' recommendations, or one for each room smaller than the minimum protection area. The detection system must be connected to the building's fire life safety system. Fire detection and automatic suppression equipment must be interconnected as well.
8. Water Detection. Any raised floor areas and any machine room areas must be equipped with UL-listed water detectors (water damage is a high risk).
9. Housekeeping. The equipment rooms should be cleaned on a regular basis to prevent the accumulation of dust and debris that could harm the equipment. Further, any and all filters should be cleaned in accordance with the manufacturer's instructions. Waste materials must be discarded into fire-safe containers that should be emptied daily. No more than a 2-day supply of paper should be stored within the equipment room. Any paper that must be stored there should be in metal cabinets.

II. Access Control

A. Responsibilities. The manager responsible for the operation of a computer data center also should implement a security support system designed to control access to the computer room, data entry areas, off-site storage areas, and supporting equipment areas. The security support system should include the necessary controls and procedures to achieve required minimum levels of protection and to implement the required standard practices described in this section.

B. Standard Practices.

1. Required Minimum Levels of Protection.
   a. A computer data center should be located and equipped so that entry of unauthorized persons can be detected during both operating and nonoperating hours.
   b. Access to a computer data center should be restricted to the following authorized personnel:
      1) Employees having job assignments within the computer data center
      2) Employees having job assignments that require regular access to the computer data center
      3) Nonemployees, such as vendor maintenance personnel and couriers, who require entry to the computer data center on a regular basis
   c. Authorization for access should be effective only during those periods when a person legitimately requires access to the computer data center.
   d. Access to the computer data center by unauthorized persons should be approved on a visit-by-visit basis. Visitors should be recorded on a register and should be escorted by an authorized person at all times while in the data center.
2. Restricted Area. The computer data center (including computer room, data entry areas, off-site storage areas, and supporting equipment areas) should be designated as a restricted area.
3. Access Authorization Procedure. A formal procedure should be established for authorizing individuals to have access to the computer data center.
4. Access Authorization Identification. A method also should be devised so that persons controlling access know who has been authorized access and can positively identify these individuals.

C. Guidelines
   1. Construction. The location and construction of a computer data center should be such that some degree of destructive force is necessary for unauthorized, undetected entry. Consequently, avoid locating the data center adjacent to building windows, and avoid the use of glass in data center walls. Care also should be taken to ensure that the data center walls extend from the structural floor to the structural ceiling (i.e., from the base floor slab to the floor slab of the floor above). These issues should be addressed in the preconstruction phase.
   2. Detection Measures. Measures that can be taken to detect intrusion into the data center restricted areas should typically include use of CCTV cameras, motion detection devices, and/or scheduled checks by security officers.
   3. Restriction Methods. Access to the computer data center must be restricted to authorized persons. Choice of an access control method should be based on cost and appropriateness to the local situation. Some possibilities are:
      a. Visual recognition of authorized persons by an employee controlling computer data center entrances.
      b. Assignment of special ID badges to authorized persons.
      c. Installation of door locks opened only by keys, cards, or combinations issued under control to authorized personnel.
      d. Use of mantraps (especially where access is highly restricted). A mantrap or portal is a small holding area to which an authorized person is admitted, prior to being asked to submit to another form of access control before they are allowed to proceed further. For example, a mantrap may take the form of a small cubicle located at the entrance to the computer center. To enter the mantrap a person will, via a CCTV and two-way voice communication system, identify himself or herself to an operator located inside the computer center. If the person is authorized to enter the mantrap, the operator will remotely operate a door to admit them (the door closes behind them once they have entered, thereby isolating them inside the mantrap). The person then will be required to submit to further verification before being allowed to proceed into the computer center. Such an arrangement reduces the chance of unauthorized persons tailgating into the computer center. Tailgating or piggybacking occurs when a person who is authorized to enter an area is accompanied by another person who has not submitted to the access verification process.

III. Program Control

A. Responsibilities. The manager responsible for the operation of a computer data center must implement a security support system to protect computer programs from destruction, unauthorized use, and unauthorized revision. All programs (purchased, leased, or developed) that are used or controlled by the computer data center must be protected.

B. Standard Practices.
   1. Required Minimum Levels of Protection
      a. A current executable copy of all production programs, including systems software, must be maintained at a location remote from the computer data center.
      b. Source programs in machine-readable form or current copies of program documentation also must be maintained elsewhere.
      c. Use (execution) of programs must be restricted to authorized purposes (i.e., for company business, for production processing according to documentation, or for testing during maintenance or modification).
   2. Documentation. Program revisions must be documented according to predetermined and standard practices.
   3. Computer Usage. A record of all computer use must be maintained for verification of authorized execution. It should not be possible to interfere with

the audit log that provides a record of all computer activity. The printout of the audit log should be done in a secure location.

IV. Information Protection

A. Responsibilities. The manager responsible for the operation of a computer data center must develop and implement an information security support system to protect all computer-readable information processed in the center.

B. Standard Practices.

1. Information to be Protected
    a. Computer Input/Output. Computer-generated information on paper, carbon paper, microfilm, or other permanent visual media should be subject to special security standards. This includes all system documentation, procedures, and forms used for the application.
    b. Systems Operations. Information regarding the operation of systems in a computer data center must be restricted on a need-to-know basis.
2. Information Classification. All information processed or to be processed in a computer data center must be reviewed to determine the applicability of information classifications defined by security standards. This review will be performed in concert with Electronic Data Processing (EDP) or Automated Information Services (AIS) support groups and the organizations owning the information.
3. Stored Computer Information. All removable computer storage media containing restricted information must be externally labeled with the appropriate classification. Therefore, physical access controls also must be established to prevent removal of the storage medium.
4. Restricted Information.
    a. Processing. Restricted information must be processed on employee-controlled computers unless a contractor providing the service signs a legal proprietary agreement.
    b. Transmission. Transmission of restricted information must be controlled to limit access to authorized individuals.
    c. Destruction. Controls must be implemented for monitoring the destruction (including shredding, carting, etc.) of restricted information to ensure compliance with predetermined policy.
    d. Access Approval. Nonemployees must be denied access to all restricted information unless prior approval is obtained from the owner of the information.
    e. Access Records. A record of access to restricted information must be maintained so that authorized access can be tracked and verified.
5. Strictly Private Information. Information of this classification must be controlled according to requirements determined by its originator.
6. Information Sharing. Sharing information between systems controlled by different organizational units must be approved by the owner of the data.
7. Access Control. Access codes used to restrict access to protected information must not be printed or displayed on a terminal. If appropriate access controls are not available in operating software, they must be incorporated into appropriate, written application programs.
8. Separation of Duties. To prevent collusion, separate staff should work on system development and system operations. The system development staff should work on a system separate from the main ''live'' system.
9. Formal Change Control. Changes to the system, such as installing updates or patches or adding information, should be formally controlled and authorized.
10. Security Systems. Obviously, computer data centers that have equipment or operating systems with security capabilities must utilize those features in their security support systems.

V. Contingency Planning

A. General Information. Interruption of computer processing operations can be caused by a variety of conditions that result in interruptions lasting from a few hours to an extremely long period of time. Efficient recovery of the computer processing facility can only be accomplished by having established contingency plans. The degree of advanced preparedness has a significant impact on the efforts expended and on the cost, length of disruption, and security exposure incurred recovering from service disruptions. Consequently, standard operating procedures must be designed to respond to day-to-day minor operating problems as well as major disruptions and disasters.

B. Standard Practices.

1. Responsibilities. The manager responsible for the computer data center should be responsible for developing a contingency plan that details emergency measures covering all likely disruptions or disasters.
2. Contingency Plan Contents. The contingency plan should include:
   a. Emergency Response Plan. This details steps to be taken to protect life and property and to minimize the impact of any emergency threats such as sabotage, fires, explosions, bomb threats, natural disasters, power failures, water leaks, riots and civil disorder, and labor disturbances.
      1) Emergency procedures
      2) Emergency equipment
      3) Facility layout
      4) Responsibility and authority
   b. Administrative Action Plan. This details steps to be taken in case of a disaster. These plans should cover damage assessment, activation of disaster contingency plans (items c and d below), disaster organization structure, and a notification system.
      1) Emergency notification procedure
         a) Notification contact list
         b) Order of contact regarding decisions
      2) Damage assessment procedures
         a) Notify assessment team members from a predetermined contact list
         b) Specify place of assembly
         c) Assess site damage
      3) Backups and recovery implementation decision criteria
         a) Discuss decision-making process
         b) Criteria to attempt normal recovery
         c) Criteria to implement backup/recovery plan
      4) Responsibility and authority
         a) Decision-making authority
         b) Approval requirements
         c) Proposed action documentation
   c. Backup Processing Plan. In the event of a disaster, this plan should provide for alternate processing capabilities for all affected EDP and AIS applications at service levels commensurate with their predesignated criticality classification.
      1) Application criticality—processing priorities
      2) Configuration requirements
      3) Relocation procedures and schedule
      4) Starting procedures and schedule
      5) Organizational responsibility and authority
      6) Manning requirements/assignments
      7) Application recovery instructions
      8) Backup data file inventory
      9) Data recovery instructions
      10) Network recovery/reconnection.
   d. Recovery Plan. This provides for smooth and rapid restoration of an AIS database or EDP site following a disaster.
      1) Situation assessment
      2) Immediate protective/security measures
      3) Vendor contact list
      4) Recovery team members

5) Organizational responsibility and authority
6) Planning and implementation

e. Copies of routine pre-emergency procedures implemented in support of, and necessary for the initiation of, the contingency plan.
   1) Off-site file backup protection
   2) Operating and program documentation

f. Information required to execute the contingency plan, such as contact names and phone numbers, location and inventory of backup supplies, and so forth.

C. Classification of Service Disruptions. In a high-rise commercial office building each tenant company, and the building itself, may have their own policies regarding service disruptions.

1. Major Disruption. The disruption is classified as major when conditions exist that interrupt or disable critical demand processing but do not require physical recovery of equipment, media, and facilities.
2. Disaster. The disruption is classified as a disaster when conditions exist that totally disable computer processing services and require physical recovery of equipment, media and facilities. Conditions constituting a disaster include, but are not limited to, fires, explosions, water leaks, natural disasters, and riots or civil disorders.

D. Preparing a Contingency Plan.

1. General. A plan should be of a general enough nature to allow the interface of detailed plans during and after the disruption/disaster. It should specify actions to be taken, individuals or organizational functions responsible for those actions, and respective time relationships of the actions. Of major importance is the pre-identification of the recovery teams that will relocate application production and those who will recover the data center facility. Remember that this contingency plan also must satisfy the current requirements of both the user and the computer operations department.
2. Elements of the contingency plan for major disruptions. The following documentation in the contingency plan is provided primarily to ensure the continued processing or the resumption of processing in the event of a major disruption:
   a. Operational procedures. Establish written procedures to be followed when responding to major disruptions. Specify actions to be taken by operations management, vendors, and supporting functions such as power and air conditioning. Provide contact phone numbers (both office and home) and equipment lists that identify vendors and vendor maintenance personnel.
   b. Backup processing procedures. Under certain circumstances, the need for service level continuation in support of critical and semicritical systems will require initiating backup processing procedures during a major disruption. A procedure for backup processing must be established.
3. Elements of the contingency plan for disasters. The following documentation in the contingency plan is provided primarily to ensure personnel safety, continued processing capability, and physical recovery after a disaster:
   a. Emergency procedures. The safety of EDP and AIS personnel is the foremost response during the initial phase of a disaster. Formal emergency procedures are required to ensure a safe and proper evacuation of personnel.
   b. Interim production planning procedures. An interim production plan must be implemented immediately after a disaster to resolve disposition of processing load and minimize the impact on critical applications. The procedures for production demand planning must be predeveloped as an element of contingency planning.

c. Data center recovery planning procedure. Recovery of the data center must address equipment, software, and physical facilities. Because the initial concern will be continuity of computer processing, this plan normally will be implemented after the initiation of the processing demand plan. The procedure for data center recovery planning must be predeveloped as an element of the contingency plan.

4. Storage and distribution. Once developed, the plan should be maintained in a Contingency Plan Manual divided into two major sections: ''Major Disruption'' and ''Disaster.'' Further division of each section should be made as needed to address the subelements defined in this appendix. Copies of the manual should be distributed to members of the recovery team as well as maintained in off-site storage.

E. Data Center Recovery Team. The data center recovery team should comprise personnel from functional areas both within and outside the company who can assist in the efficient and timely recovery of the facility. Team members should be selected jointly by the Director of Security, the manager of the computer data center, and appropriate top management administrators.

5 *Security Systems and Equipment*

In high-rise office buildings, there are many types of security systems and equipment that can be deployed as potential solutions to address specific vulnerabilities. Their purpose is to help ensure that a building is safe to use and that protection is provided ''for materials, equipment, information, personnel, physical facilities, and preventing influences that are undesirable, unauthorized, or detrimental to the goals of the particular organization being secured'' (Post and Kingsbury, 1991, p. 1).

This chapter outlines the various systems and equipment that may be found in public access or common areas, rented or assigned occupancies, and maintenance spaces in a typical modern high-rise office building.

Monitoring of Security Systems

The focal point for the monitoring of the security systems for an entire building may be local annunciator and control panels built into an open-style desk arrangement in the main lobby, or a more complex and sophisticated Security Command Center housed in a separate room. There are two obvious drawbacks to the former system. First, the security staff monitoring the equipment may be required to monitor passing pedestrian traffic and assist building occupants and visitors with their inquiries and service requests. This detracts from the staff's effectiveness in monitoring annunciator and control panels. Second, the placement of the building security systems and equipment out in the open somewhat compromises overall security and makes it more susceptible to interference and (in a highly unusual but nonetheless possible situation) direct attack. However, equipment may need to be placed in an open-style arrangement (Figure 5.1) because there may not be enough activity to justify a Security Command Center, or budgetary constraints may not support extra security personnel to staff a Security Command Center and meet the needs of the lobby itself. If the Security Command Center is located in a separate room (Figure 5.2), access to it should be controlled at all times, and it should not be used for any other purpose than that for which it is designed.

The Security Command Center often contains the following equipment:

- Building and elevator keys
- Systems for remote locking and unlocking of emergency exit stairwell doors when doors are locked from the stairwell side, roller shutter doors and gates, etc.

Figure 5.1 An open-style Security Command Center. Photograph by Roger Flores.

Figure 5.2 An enclosed Security Command Center. Photograph by Roger Flores.

- Control systems for card access and biometric readers
- Telephones, portable two-way radio systems, public address (PA) systems, megaphones, intercom systems, and speaker systems
- Monitoring and recording systems for closed-circuit television (CCTV)
- Monitoring and control systems for intrusion alarms
- Key control systems
- Monitoring systems of fire detection, sprinkler control valve and water flow alarm devices, and other fire protection equipment (as discussed in Chapter 6)
- Monitoring and control systems for elevators (also discussed in Chapter 6)
- Controls for building lighting systems
- Operator terminals and printers for security and fire life safety systems and equipment

Some facilities permit commercial television sets to be installed in the Security Command Center. The reasoning behind this is that it allows the security department to be informed of news-breaking events, particularly those that may impact the building or surrounding community. Either the television remains on at all times, or it can be switched on when an incident has occurred or is expected.

All security systems should be listed as having met minimum standards of the Underwriters Laboratories Inc. (UL), FM Global,* Wernock Hersey International (WHI), or Electronic Testing Labs (ETL).

Before examining asset tracking, lighting, communication, CCTV, intrusion detection systems, and other security devices, it is appropriate to review the types of physical barriers, locks, and locking systems that may be found in a high-rise office building.

Physical Barriers

A security barrier is any boundary or obstacle that separates an area and is designed to deter, delay, or prevent access of persons or vehicles to that area. Barriers associated with high-rise buildings are described in the following sections.

Perimeter Landscaping, Walls, Fences, Sidewalks, and Pathways

All perimeter landscaping—including plants, trees, shrubs, ditches, and berms—should be chosen, located, and maintained so that it stops, deters, or delays an intruder, does not provide any concealing cover for surprise attacks on persons, cannot be used to gain entry to upper levels (such as promenades, walkways, etc.) and does not obstruct lines of sight, lighting, CCTV, or intrusion detection systems. Earth berms, in conjunction with lights, also may be useful to silhouette an intruder moving over the top of a berm.

Walls may be constructed of brick, masonry, stone, concrete block, or any other aesthetically pleasing materials. To discourage people from climbing

*Formerly known as Factory Mutual.

over them, walls should be at least 7 feet tall and may be topped, in areas where it is deemed fitting, with materials to prevent actual scaling of the wall. To deter graffiti, climbing ivy or prickly or thorny plants—cactus, boxwood, bougainvillea, quince, locust, or natal plum—can be planted at the base of the wall.

Fences may be of the wrought-iron type and should be constructed with as few openings as possible. (Chain link, barbed wire, barbed tape fences, and the like are usually not appropriate in the urban high-rise environment; however, fence cabling systems may be acceptable in some settings.)

Because high-rise office buildings usually are located in urban areas where real estate is at a premium, there may be little exterior landscaping and the perimeter may actually be the walls of the building itself. Pedestrian sidewalks and pathways should be well lighted and provide the most direct access possible to the building.

Fountains, Reflecting Pools, Sculpture, Boulders, Stairs, Park Benches, Concrete Planters, Concrete Barricades, and Bollards

Fountains, reflecting pools, large pieces of sculpture, sizable boulders, stairs, reinforced and anchored park benches, concrete planters, concrete barricades, and bollards strategically placed near a building can be used to deny vehicle access to vulnerable areas and maintain a spatial separation of vehicles (particularly explosive-laden trucks and car bombs) from a building's structure.

Heavy planters, made of glass-fiber reinforced concrete and strengthened with steel rebar (either a steel bar or rod) and placed about 3 feet apart (so that the opening between them is less than the width of a truck frame) can provide a very effective passive or immobile barrier. In some applications, one or more of the planters is designed in a manner that if special access is required, the planter can be temporarily moved aside using a heavy-duty mechanical platform.

Concrete barricades (Figure 5.3) can be used to establish a defensive perimeter around a building. For example, immediately following the September 11, 2001, terrorist attacks on the New York World Trade Center and the Pentagon, the 110-story Sears Tower in Chicago, the tallest skyscraper in the United States, and the 72-story Library Tower in downtown Los Angeles, the tallest building west of the Mississippi, erected temporary steel-reinforced concrete barriers outside of their buildings (Tawa, 2001, p. E-7). These barriers (sometimes referred to as ''*T-rails*'' or ''*Jersey barriers*'') are usually not rated as to the size and speed of the vehicle that they are designed to stop; however, interlocking and anchoring them to the ground increases their stopping power (True, 1996, p. 51).

The effectiveness of concrete barriers against a truck or a car bomb explosion largely depends upon their degree of spatial separation, or standoff distance,* from the building being protected, and the type and amount of explosives being used. For most existing high-rises, the use of barriers is impracticable or ineffective due to the lack of available space at the perimeter of these buildings. (However, using barriers to prevent a vehicle from crashing

*The aim is to keep a vehicle as far as possible from the building to reduce as much as possible the impact of an explosion.

Figure 5.3 Three-foot high steel-reinforced concrete barriers (commonly called ''T-rails'' or ''Jersey barriers'') outside of a building. To be more effective they should be joined together and anchored to the ground. This type of barriers does not fit with the architectural style of most high-rise buildings and are usually only temporary until aesthetically pleasing ones can be installed.

into a building, and restricting or eliminating parking of vehicles adjacent to a building, can reduce the risk and impact of a truck or car bomb attack.)

Bollards (Figure 5.4) can also be used for physical vehicle security. A bollard is a cylindrical post firmly anchored to the ground and usually constructed of heavy steel. Bollards can be fixed in position or hydraulically or pneumatically raised or lowered as needed (the latter commonly are called ''*pop-up*'' bollards). As with concrete barricades, for many existing high-rises the use of bollards as an effective barrier to truck bombs is impracticable or ineffective due to the lack of available space at the building perimeter.

When selecting an appropriate vehicle barrier it is critical that ''the security manager estimate the likely size and weight of an attack vehicle and the maximum speed that vehicle could achieve on the streets* leading to the building.... [Also], the security manager should ask to see the vehicle barrier crash certification, which should list the model of the barrier, the weight and speed of the vehicle it stopped, and the federal agency that supervised the [crash] test'' (True, 1996, pp. 50, 51).

*If possible, straight, level sections where an approaching vehicle could build up speed should be reconfigured or have obstacles placed on them in a serpentine pattern to force the vehicle to slow down.

Figure 5.4 A series of 2-foot high, aesthetically pleasing bollards that provide an effective physical barrier to vehicles. These bollards can be blended with the rest of a building's architecture by using ornamental steel trim attached directly to the bollard or cast sleeves of aluminum, iron, or bronze, which slip over the crash tube. Courtesy of Delta Scientific Corporation.

Parking Controllers and Barriers

The majority of barriers to vehicles entering and leaving parking areas consist of a railroad-crossing type mechanism with a wooden or plastic gate arm. These active barriers may be operated manually or automatically by a variety of methods including a vehicle presence detector embedded in the roadway; a parking attendant, a valet, or a security person using a remote control device or a key switch; or the driver pressing a button and pulling a paper ticket from a control unit, presenting an electronic access card to a reader installed at the control unit, operating a key pad, or using a radio control device. Such gate arms are usually not designed to physically stop vehicles (unless a steel or aluminum heavy-duty gate arm is used).

For higher security applications, particularly at the entry to under-building parking garages and loading docks of high-rise buildings, crash-rated steel barricades (Figure 5.5) can be mounted in either a level driveway or on a ramp.* These barriers can control the normal flow of traffic of authorized vehicles and also have the capacity in emergency situations to stop and disable a fast moving vehicle. The raising and lowering of the barricade can be controlled manually or automatically by a variety of methods including using a remote control device or a key switch; a key pad; presenting an electronic access card to a reader installed at the control unit; or a velocity sensing device (that senses an approaching high speed vehicle and can trigger an alarm or activate the barricade).

A word of caution about the use of such barricades is that sometimes operating staff can make mistakes and damage vehicles. ''In high traffic cycle operations, [staff] can make errors by pushing controls at the wrong

*These barriers can be either those that are set in the ground and designed to spring up when activated; or those that remain fully raised and drop down when an authorized vehicle is to enter. The advantage of the former is that since they are out of sight when not in use, they are more aesthetically pleasing (True, 1996, pp. 51–52).

Figure 5.5 A fully raised 2-foot high crash-rated, surface-mounted steel barricade is ''capable of taking axle loadings in excess of any permitted North American or European road transport vehicles'' (Delta Scientific Corporation). Courtesy of Delta Scientific Corporation.

time, lifting authorized vehicles. If vehicle-sensing loops are placed in the roadway directly in front and behind the barricade, the coupled loop detector will suppress accidental operation. The [staff] still have complete control using the emergency mode, which overrides the safety loop'' (Delta Scientific Corporation, 2002). ''Training of operating personnel is strongly recommended. In addition to general training of these employees, at least two key people should be trained in all aspects of the system so that if something irregular or unusual happens, the [building] has personnel that can help. For instance, the [building] may have a major power outage and might require that the barriers be operated manually during this situation'' (True, 1996, p. 53).

Building Exterior

Building Exterior Walls and Roof

The building's exterior walls should be of sufficient strength to make unauthorized entry difficult. Walls at least 8 inches thick are difficult to penetrate using hand tools. However, hand tools in conjunction with small amounts of explosives can be used to penetrate them.*

The roofs of high-rises vary due to the design and construction of the building. The roof is the site of building utilities and mechanical areas that may include cooling towers, air-intake or air-vent openings, elevator machine rooms, window-washing staging equipment, and telecommunications equipment, such as antenna farms. Also, there are one or more fire doors leading to the building's emergency exit stairwells.

Due to height, the roof is usually not considered an easy point of access. However, the presence of a helipad or heliport does make it more vulnerable. Openings and maintenance accessways should be strengthened to the degree of being as penetration-resistant as the rest of the roof (National Crime Prevention Institute, 1986, p. 63).

Building Openings

Openings in the building's exterior permit ingress and egress of pedestrians to lobbies, and utility and delivery vehicles to building loading dock areas. If there is a parking structure, openings are provided for passenger vehicles to enter and leave. In addition, there may be open roofs and openings in exterior walls of the parking garage for the purpose of providing natural light and ventilation; underground tunnels for utilities such as domestic water, electrical power, gas, and telephone; and drains, conduits, or sewers leading away from the building. Such openings, including windows and doors, should be properly secured as described in the following sections.

Doors

There are several types of exterior doors associated with high-rise buildings:

1. *Lobby Doors.* These doors are single or double, and can be constructed of tempered plate glass (at least ¼-inch thick) or stronger burglar-resistant glass or polycarbonate glazing material (both meeting UL standards). The glass often is secured in aluminum, stainless steel, or other metal framework. These doors are designed to swing out and are fitted with a door closer.†

In some high-rises, security revolving doors regulate the flow of pedestrian traffic in and out of building lobbies without exposing the building to outside elements. Each of these doors has several wings that separate the

---

*Structural design features, such as explosion resistance and blast deflection, traditionally are not incorporated into commercial office buildings. However, such counterterrorism features, and the reinforcing of building structural members (including, for example, critical support columns exposed in areas such as loading docks and shipping and receiving areas) are receiving more attention, particularly since events such as the 1995 Oklahoma City and the 1993 and 2001 World Trade Center incidents.

†In the United States, the Americans with Disabilities Act (ADA) requires these doors to be operable by a disabled person in a single effort, with no grasping motion; this requirement can be met by the provision of a low-energy powered door opener such as a push button or push plate switch, or by fully automatic operation with doors activated by motion detectors on the door transom or header bar, or floor pressure pads or mats. For other pedestrians, the door can open manually from the outside or inside.

door into quadrants or sections. Only one person at a time is permitted to occupy a single door section. ''In a properly designed security door system, when the door sensors detect two persons in the same section, at the same time, the door stops then slowly reverses automatically to back the two individuals out of the door. This is referred to as 'anti-piggybacking.' A security revolving door also prevents passage of unauthorized persons who attempt to get a 'free ride' in the opposite or adjacent section to the authorized user. Once again, system sensors will detect inappropriate use, stop the door and slowly reverse, backing both people out of the entrance. This feature is referred to as 'anti-tailgating.' '' (O'Leary, 1998, pp. 59, 60). The door's control system can also be interfaced with an access control system. Such doors are excellent for controlling access, particularly when no security staff is present.

Modern security revolving doors are designed so that in the event of a fire alarm or power outage, the door wings will automatically collapse to a book-fold position to provide two unobstructed lanes for occupants to exit and responding emergency personnel to enter the building (for older generation revolving doors, during an emergency the doors have to be manually collapsed to enable straight-through access). With revolving doors, many codes require an adjacent side-hinge swinging door to be provided.

2. *Stairwell Exterior Fire Doors.* These doors can be single or double. In high-rise buildings they are of solid-core construction, often with heavy-gauge sheet metal or steel plating. Door hinges should be designed so that they are not accessible from the outside; however, if they are accessible, the hinges should be of heavy-duty construction to resist destruction, and hinge pins made unremovable by being welded or flanged.

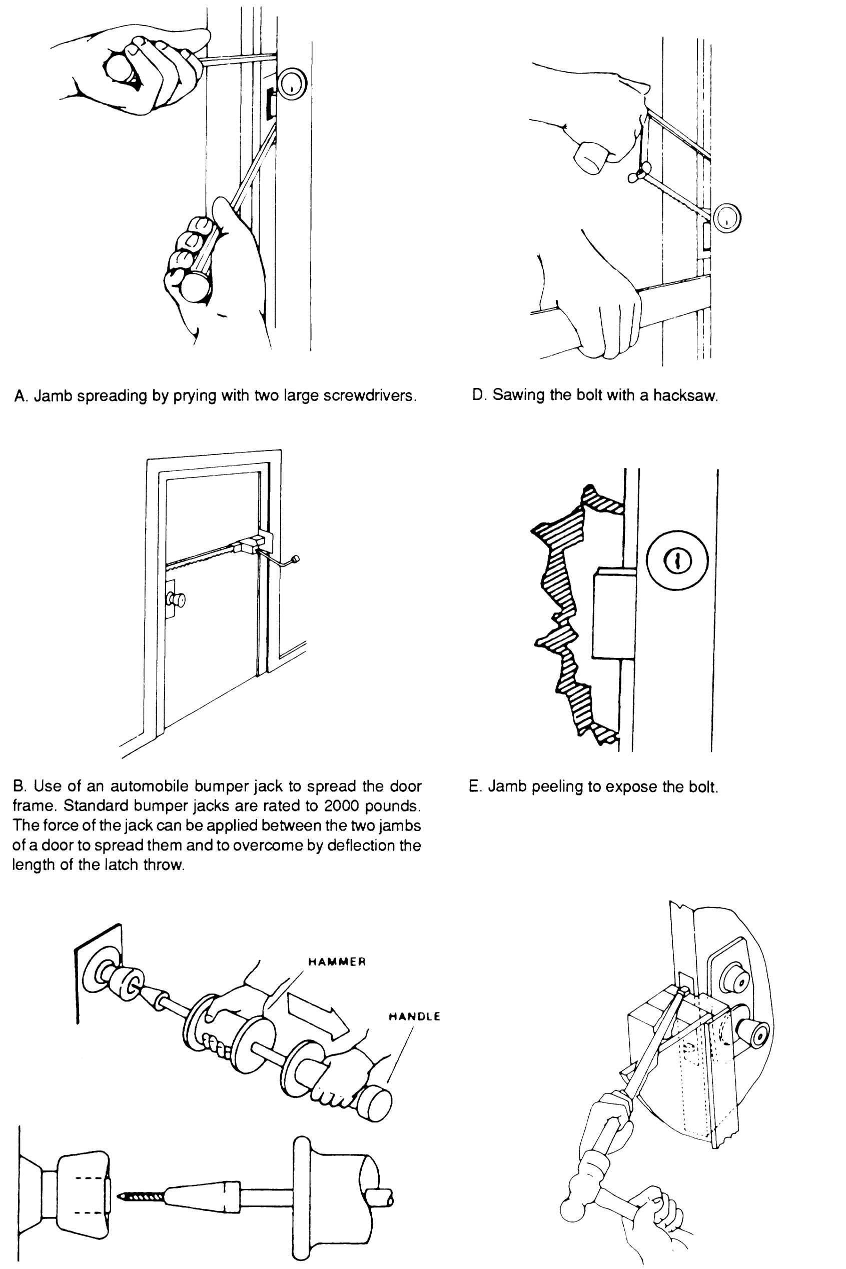
''Regardless of how the pin is protected, if the knuckle [the part of the hinge that holds the hinge pin] is exposed on the outside, it is generally possible to saw off or otherwise remove and/or destroy the assembly and thus gain entry by prying open the door from the hinge side'' (Gigliotti and Jason, 1989, p. 213). This statement is a compelling reason for never exposing door hinges in buildings, and its originators suggest a possible countermeasure to this vulnerability. This involves the use of a piano hinge that consists of a continuously interlocking hinge system running the full length of the door.

The actual frame in which a door is mounted should be secured to the wall in such a fashion that it resists penetration to at least the same degree as the door itself. Figure 5.6 shows common attack methods on doors and frames.

Turnstiles

In addition to single and double lobby doors and revolving doors, turnstiles are used to control pedestrian traffic. The most common type of turnstile deployed inside major high-rise building lobbies is waist-high* (Figure 5.7). As O'Leary (1998, pp. 60, 61) writes,

*Full-height security turnstiles are usually used to control pedestrian traffic in areas without the need for security staff.



A. Jamb spreading by prying with two large screwdrivers.

D. Sawing the bolt with a hacksaw.

B. Use of an automobile bumper jack to spread the door frame. Standard bumper jacks are rated to 2000 pounds. The force of the jack can be applied between the two jambs of a door to spread them and to overcome by deflection the length of the latch throw.

E. Jamb peeling to expose the bolt.

C. Cylinder pulling with a slam hammer.

F. Forcing the deadbolt with a drift punch and hammer.

Figure 5.6 Common attack methods on doors and door frames. Reprinted courtesy of the National Crime Prevention Institute, School of Justice Administration, University of Louisville, from Edgar et al., *The Use of Locks* (Butterworth–Heinemann, Boston, 1987), pp. 72–76.

Figure 5.7 Waist-high optical turnstiles. Courtesy of Mike Smith of Gunnebo Omega Inc., Concord, CA, www.gunnebo-omega.com.

Because waist-high turnstiles do not actually create a total physical barrier, they generally are considered as low- to medium-security devices. . . . There are three types of turnstiles currently used in facility security: tripod, proprietary barrier and optical. Tripod types come in a wide variety of shapes and sizes to suit virtually any application. Tripod turnstiles all use a three-pronged barrier wheel, which rotates as the user's leg presses against it to allow passage. . . . Proprietary barrier turnstiles include gates [and ''pop up'' barrier arms] and the devices which are generically referred to as turnstiles, but which may not turn at all. Optical turnstiles offer no physical barrier, but offer a route for pedestrian traffic and may be used for monitoring traffic flow, to provide signaling or may be part of a larger facility's management system which provides metal detection and loss prevention, [and] reads access cards.

Any waist-high turnstile can perform in a high-security application depending on the system designed around it and the personnel operating the facility. The turnstile can be used in a variety of modes: controlled entry/no exit, controlled entry/free exit or controlled entry/controlled exit.

Turnstiles typically are connected to access control, remote release and remote monitoring equipment to cause them to control access or report traffic flow rates. Options include: time-out relay, red and green indicator lights, extended arms, remote release button, out-of-use lock and electronic key bypass.

In major high-rise building lobbies with high pedestrian traffic and the need for controlled access, multiple optical turnstiles located near building elevators can be very effective. Tenants can effortlessly pass through the turnstile with a proximity access card on their person. If an invalid card is used or an unauthorized person attempts to pass through the turnstile, an audible signal will sound and supervising security staff can stop the individual concerned and question them as to their right to enter (or, additionally, as was the case at the New York World Trade Center, if someone jumped over the waist-high turnstile, CCTV motion detectors in the lobby caused CCTV cameras to lock onto the violator). Once the tenant has passed through the turnstile, he or she can then proceed to an access card–controlled elevator for travel to their authorized floor. Using an optical turnstile as a primary means of access control helps alleviate the problem of an unauthorized person proceeding directly to a building elevator car and then tailgating behind a tenant to gain access to upper floors.

Windows and Security Window Film

Windows in modern high-rise buildings are permanently fixed in place and typically are constructed of annealed (plate), tempered safety, or laminated glass. The glass itself is often the weakest part of the window because it can be broken or a section of it removed using a glasscutter, thereby affording access to a facility. Nevertheless, properly mounted plate glass is usually difficult to smash unless considerable force is applied.

Synthetic materials, such as polyester film (e.g., Mylar™), can be applied to plate glass. ''While it does not add strength to the glass, it creates a less lethal failure mode'' (Hinman, 1995, p. 35). ''Security window film is comprised of either optically clear, tinted or reflective layers of polyester film (from four mils to 15 mils thick) that can be adhered to the interior surface of existing glass. Typical film installations cover the visible portion of the interior surface of the glass all the way to the edge of the frame'' (Smith, 1999, p. 89). If the glass breaks (when subjected to storms, tornadoes, windblown debris, earthquakes, vandalism, and explosions), the pieces adhere to the coating to reduce the effects of broken glass and flying glass shards.

> Because security window film has the ability to stretch before tearing, it can absorb a significant explosive shock. As this explosive force moves towards the glass and pushes it inward, the glass eventually cracks and breaks. However, the security film applied to the rear of the glass continues to absorb the shock wave and stretches until it reaches the point that it can no longer bear the pressure, at which time it will burst.
>
> While strong enough to break the glass, the shock wave may not be strong enough to shear the security film. This results in glass not being broken but being held intact by the film. Not only are there reduced injuries, but there is also little damage to the property inside the building. If the shock wave is sufficient to break the glass and shear the film, often the glass collapses attached to the security film with minimal damage and injuries. In multi-story buildings, security film also may

> prevent glass from falling out of its frames to the street below, especially if it is anchored to the window frame'' (Smith, 1999, pp. 89, 91).*

Security window film is inexpensive to install (as compared with installing tempered safety or laminated glass) but may require replacement after 10 years. Some high-rise buildings, in preparation for turbulent events, such as planned protests and demonstrations outside of their buildings, have installed window film on windows near the ground level. For example, in August 2000, the Wells Fargo Center in Los Angeles, a major high-rise complex, undertook such measures to help protect against potential acts of vandalism involving broken glass during the 2000 National Democratic Convention (''Window film protects Wells Fargo Center,'' December 2000, p. 42).

Tempered safety glass is also found in modern high-rise buildings and has ''a greater resistance to explosions than annealed glass'' (Hinman, 1995, p. 35). If a tempered glass window breaks, it separates into small fragments. In most jurisdictions, building codes require tempered glass at the lobby level for the safety of persons if the glass should break, and on upper floors for the purpose of mechanical smoke ventilation (when the window is broken out). In Los Angeles high-rise buildings, tempered safety glass is required every 50 feet in upper-floor windows so windows can be broken out for smoke ventilation. This alleviates the danger of large pieces of glass dropping from the upper floors and seriously injuring people below, or cutting exterior fire hoses during a fire situation. The use of tempered safety glass also reduces the risk of injuries from broken glass during a major earthquake, storms, tornadoes, windblown debris, vandalism, and explosions.

Laminated architectural glass (laminated glass or laminated security glazing) ''is constructed by bonding a tough polyvinyl butyral (PVB) plastic interlayer between two pieces of glass under heat and pressure to form a single piece'' (O'Mara, 2000, p. 43). It has considerable resistance to impact and the glass tends to hold together by adhering to the plastic interlayer when cracked or broken. Laminated glass has ''a greater resistance to explosions than annealed glass'' (Hinman, 1995, p. 35). ''Laminated glass can reduce danger of flying or falling glass; resist penetration and forced entry; block out unwanted noise; be made in any color; and be used in a variety of applications, including protection against disaster, hurricane, earthquakes, commercial safety and security, bomb blasts, etc. In addition, some laminated glass provides ballistic protection'' (O'Mara, 2000, p. 43).

Blast-resistant windows can be made of tempered safety glass or laminated security glazing.

---

*''The August 1998 bombings at the American embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, killed 280 and injured more than 5,000 people. The bombs that destroyed these structures, like the one that brought down the Alfred P. Murrah building in the 1995 Oklahoma City bombing [described in Chapter 10], were of such strength that no window system would have been able to survive. However, the broken glass in adjacent buildings that injured thousands of people may not have done so had the windows in those buildings been protected by security window film'' (Smith, 1999, p. 88).

In areas where added expense could be justified by an insurance premium reduction, or where unauthorized penetration is expected, stronger burglar-resistant glass or bullet-resistant glass (both meeting UL standards) might be used. Burglar-resistant glass is of laminated construction. Bullet-resistant glass is classified according to its strength to withstand various weapons and bullet caliber. Sometimes, bullet-resistant glass is used for guard booths.

Wired glass is sometimes used for sidelights and transoms adjacent to and above doors. ''The glass, which consists of wire sandwiched between two layers of annealed glass, has a fire protection rating of 45 minutes'' (Reese, 1998, p. 75). It resists shattering and fragmentation on impact, but is not aesthetically appealing. ''Unfortunately, wired glass has its shortcomings. It has an industrial appearance some designers dislike, and isn't a particularly strong material. . . . When broken, the wire within the glass keeps it from shattering into sharp shards, but it can still cut and cause serious injuries'' (Reese, 1998, p. 78).

Another weakness of window openings is that the glass itself can be removed and replaced, often with no telltale sign. Either putty or molding is removed and on replacing the glass the original molding is reused, or putty of a similar color to the adjoining windows is used. Such surreptitious removal and replacement of glass is much more difficult to achieve if the glass has been secured in grooves in the window frame using an elastic glazing compound.

Openings for Vehicles

Overhead gates protecting vehicle openings to parking structures tend to be either rolled, corrugated steel shutters or metal, open-grille roll-down gates. (Open-grille gates—Figure 5.8—may suit exterior openings because they can be seen through. They also allow ventilation of vehicle exhaust fumes and, in the case of a fire, smoke and other products of combustion.) After normal operating hours when the parking structure is closed, these gates may be operated in one of the following manners:

- Manually using a chain
- By an electric motor manually activated at the gate
- Remotely from another location (often in conjunction with a CCTV system so that the gate operator can remotely observe the gate area)
- Automatically using an electric motor triggered to raise the gates when activated by an electronic card reader verifying the vehicle occupant's card, a key pad, a radio control device, or a vehicle presence detector embedded in the roadway

One physical barrier used to protect openings for vehicles consists of rotating steel wedges installed in the ground across vehicle openings to a parking area. This barrier can be driven over safely when a vehicle is exiting a parking area, but will cause severe tire damage if a vehicle attempts to reverse direction or drive in through an exit. Another barrier, already addressed in the previous section (see Figure 5.5), is a crash-rated steel barricade that can be mounted in either a level driveway or on a ramp.

Within multilevel parking structures, steel shutter roll-down doors are used as fire barriers. Each door is equipped with a fusible link in the chain used to hold the door open. During a fire, the fusible link is designed to melt at

Figure 5.8 An open-grille roll-down gate leading to a subterranean parking garage. Photograph by Stephen Lo.

a predetermined temperature, causing the door to automatically descend, thereby limiting the spread of fire and restricting the movement of smoke.

Openings for Ventilation, Utilities, and Sewers

Openings for ventilation, utilities, and sewers may be protected by various methods using materials such as chain-link fabric, welded wire fabric, expanded metal, barbed wire, razor ribbon, metal grates, metal louvers, metal grilles, metal covers, steel bars, or steel rods. These openings, particularly outdoor air intakes and ducts for the HVAC systems and air handling units, should be constructed or modified[*] (or, if possible, their location changed so that access from the street level is denied) so that the introduction of materials—such as toxic chemical, biological, and radiological agents—is made extremely difficult, if not impossible.[†]

Building Floors, Ceilings, Interior Walls, and Interior Stairways

Floors and Ceilings

Modern high-rise buildings have floors that provide a substantial barrier to unauthorized physical access upward or downward through the floor or

[*]In addition, CCTV surveillance of these areas might be considered.
[†]For other protective measures, such as high-efficiency filters, ultraviolet light, and biological-agent detection devices, a biochemical expert or qualified HVAC professional should be consulted.

ceiling to an adjoining floor. Composite concrete floor slabs, resting on metal decks atop horizontal steel beams, constitute this barrier.

Suspended or Dropped Ceilings

Ceilings may be constructed of noncombustible acoustical ceiling tiles that are supported in a metal grid hung on metal hangers attached to the floor above. The concealed space created above the ceiling often extends throughout an entire floor area (apart from mandatory firewalls extending from a base floor slab to the floor slab of the floor above and in restrooms and corridors where fire-rated plasterboard ceilings are used for fire protection). It can provide a possible means of ingress to a tenant office. A person might remove the ceiling tiles on one side of a wall (i.e., a non–floor slab–to–floor slab wall), climb up into the ceiling space, crawl over the wall partition, and again remove ceiling tiles to drop down into the tenant office. There are two obvious physical countermeasures to prevent this from happening: use floor slab–to–floor slab partition walls for all sensitive areas or, if floor slab–to–floor slab partition walls surrounding these areas do not exist, install steel bars or rods above the partition walls to deter unauthorized entry. Furthermore, electronic security devices may be installed to detect any possible intrusion.

The concealed space could also be used to hide unauthorized listening or viewing devices such as microphones or cameras. The HVAC duct systems also provide a similar means for unauthorized listening and viewing. Countermeasures—steel bars or rods, electronic security devices, or providing a separate, stand-alone HVAC system for sensitive areas—are possible solutions to this potential security problem.

Interior Walls

Interior walls may be constructed of lath and plaster or prefabricated sheets of material such as fire-rated drywall, plasterboard, plywood, or wooden paneling attached to wooden or metal studs.

Interior Stairways

Interior stairways or staircases are sometimes found in high-rise buildings, often for access between floors of a multi-floor tenant. Depending on the security needs of the tenant, the free access that these stairways afford may need to be controlled.

Building Interior Doors

Doors to Offices and Interior Areas

Doors leading to offices and other interior areas can be single or double. Perimeter doors to tenant offices and inner office doors usually are constructed of solid-core materials (any fire doors must, by code, be of solid-core construction), although some inner office doors are made of glass (in particular, many conference rooms have glass doors and a glass wall that provide visibility and thereby reduces the chances of a person unintentionally interrupting a meeting).

Doors to sensitive areas, depending on the degree of physical security required, may have heavy-gauge sheet metal or steel plating.

Door hinge and frame construction requirements are the same as discussed earlier in the ‘‘Stairwell Exterior Fire Doors’’ section. These doors should be locked at all times, preferably with the locks being part of a master key system. Access control systems, CCTV systems, and intrusion detection systems also may be incorporated into the total security system protecting these interior offices and sensitive areas.

Some doors within high-rise buildings may be equipped with door viewers with a minimum 180-degree angle of vision. The specific application will vary depending on the security or safety reason for installing such a device. From a security standpoint, a door viewer allows one to see the person requesting entry before the access is granted or denied. For safety reasons, the person about to exit a door that swings out into a public corridor may use the door viewer. By doing so, the chance of the door swinging out and hitting a passerby is reduced. In addition, door viewers are installed on conference room doors to allow a person to see in to the room. This helps prevent unnecessary interruptions of meetings.

Within tenant areas there may be doors leading to individual offices, conference rooms, libraries, computer rooms, data centers, storage areas, and break rooms. These doors usually are of glass or solid-core construction.

Also, there may be various files, safes, and vaults used to store and protect papers, files, documents, computer software, cash, checks, bonds, precious metals, and other items of high value or sensitivity. The protection afforded may not only be against security threats such as burglary, but also against safety threats such as fire. It is important to realize that burglar-resistant containers are not necessarily fire-resistant, and vice versa. On some occasions, irreplaceable documents have been stored in safes that offer strong resistance to a would-be thief, only to have the items perish in a fire. Similarly, valuable items such as cash and precious metals have been stored in safes that were designed to resist the high temperatures of fire, but that offered no resistance to an enterprising burglar. The ideal solution may be a container that is burglar-resistant and built into a fire-resistant receptacle. The degree of protection depends largely on the value of the planned contents of the files, safes, and vaults.

Stairwell Doors

These single doors are of solid-core construction and made of wood, heavy-gauge sheet metal, or steel plating. They always swing in the direction of egress travel and are required to be equipped with self-closing and self-latching devices. Because these doors constitute openings in fire barriers, they are required to have a fire protection rating to limit the spread of fire and restrict the movement of smoke. A label indicating the rating is required on both the door and the door frame. These doors should be inspected after an area has been painted to ensure that the fire protection-rating label has not been obscured.

As for the stairwells to which these doors lead, details on their construction are found outlined in the laws, codes, and standards adopted by the authority having jurisdiction. These details include the following: the requirement that each floor in a high-rise has two or more stairwells, exit capacity, fire resistance rating of the walls (usually 2-hour), interior finish of walls and ceilings, width of stairwell, types of stairs, tread construction, types of guards and handrails, access to the roof and ground level, natural ventilation, mechanical ventilation, stairwell pressurization, lighting, signage, and so on. Figure 5.9 shows the inside of a typical emergency exit stairwell.

In some high-rise buildings, stairwells are occasionally interlocking- or scissor-type stairs (i.e., two stairways are located close together in the same stairshaft).

Won Doors

Won Doors are special accordion-style doors found in the elevator lobbies of some high-rise buildings. Normally, they are in a contracted or concealed position. On activation of a fire alarm, the Won Doors on the floor where the alarm is occurring will automatically expand by sliding across the opening to enclose and protect the elevator lobby. This compartmentation of the

Figure 5.9 Interior of a typical emergency exit stairwell in a modern high-rise building. Photograph by Stephen Lo.

elevator lobby assists in preventing the intrusion of products of combustion into the lobby.

Doors to Maintenance Spaces

Doors leading to maintenance spaces can be single or double, of solid-core construction. They usually are made of wood, heavy-gauge sheet metal, or steel plating. (For preferred hinge and frame construction, see the ''Stairwell Exterior Fire Doors'' section.) These doors should be locked at all times, with the locks preferably being part of a master-key system. They should be equipped with automatic door closers and self-latching mechanisms to prevent them being accidentally left open.

Restroom Doors

The single doors usually used as restroom doors are of solid-core construction and made of wood, heavy-gauge sheet metal, or steel plating. Doors to private restrooms situated in public access or common areas should be locked at all times. They should be equipped with automatic door closers and self-latching mechanisms to prevent them being accidentally left open. Keys to restrooms should not provide access to any other areas. The restrooms intended for public use should be located on the ground floor lobby or as close as possible to this location; they should be distinctly marked, in public view, and usually remain unlocked.

If advice is required about doors in commercial office buildings, a certified door consultant or an architectural hardware consultant should be contacted.

Elevators; Escalators; Moving Walks; Dumbwaiters; and Rubbish, Mail, and Laundry Chutes

The operation of elevators; escalators; moving walks; dumbwaiters*; and rubbish, mail, and laundry chutes varies from system to system and building to building. Because elevators usually provide access to all levels of a high-rise building, they are of particular security importance.

Elevators

Chapter 6 outlines the basic similarities of elevator features and controls in high-rise buildings.

In terms of tenant security, the access the elevator affords to tenant floors is of critical importance. The ability to ''lock out'' certain floors is an essential security tool. For example, for unoccupied floors or floors under construction,

*''A *dumbwaiter* is defined as a hoisting and lowering mechanism, used exclusively for carrying materials, with a limited size car that moves in guides in a substantially vertical direction'' (Donoghue, 1997, p. 8-57). This information is derived from ASME A17.1, *Safety Code for Elevators and Escalators*, ASME, Fairfield, NJ, 1996.

the ability to prevent elevators from accessing these floors will not only avoid the problem of unwanted visitors to an unsupervised area, but also the negative impression that an unoccupied floor may convey to building users such as tenants.

Many elevators are fitted with card access control systems that enable additional security controls to be implemented. The types of access control systems are discussed later in this chapter.

A word of caution here is that with today's telecommunications capabilities, one must be particularly careful when granting access to elevator programming functions. The following incident illustrates this point.

> For months, there were thefts of desktop computer systems from various tenants distributed throughout a 39-floor building. The modus operandi was always the same. The computers would disappear from locked tenant spaces after normal business hours. There were never any visible signs of unauthorized entry. Every conceivable pathway the thief might have taken to remove the items from the building was examined. It was determined that the only possible pathway for removal of the items was through the service/freight elevator. However, after normal business hours this particular elevator was always programmed to be ''on security.'' It was finally ascertained that the elevator was being taken ''off security'' for a period that coincided with the thefts. Further investigation revealed that a building engineer had dialed up to the elevator computer from a home computer and altered the elevator's security status. The engineer then went to the site and accessed the tenant floor by this elevator. The thefts were carried out using a building master key to gain access to the tenant space and the stolen items were then loaded into the elevator car and transported down to the loading dock, where there were no CCTV cameras to view the incident. The elevator was then later remotely placed back ''on security.''

Locks and Locking Systems

Pin Tumbler Locks*

The pin tumbler lock (or mortise cylinder lock) is the type of key-operated lock most widely used in architectural or builders (door) hardware (Figure 5.10). In high-rise office buildings, these locks may be found on various perimeter, stairwell, and maintenance areas, and on tenant doors. This type of lock is installed by hollowing out a portion of the door along the front or leading edge and inserting the mechanism into this cavity. The security afforded by the pin tumbler mechanism ranges from fair, in certain inexpensive cylinders with wide tolerances and a minimum of tumblers, to excellent in several makes of high-security cylinders. An irregularly shaped keyway and a key that is grooved on both sides characterize locks listed by Underwriters Laboratories as manipulation- and pick-resistant. Pin tumbler locks can be master keyed

*__Note__: The pin tumbler locks section is adapted from ''The use of locks in physical crime prevention'' by James M. Edgar and William D. McInerney, appearing in the *Handbook of Loss Prevention and Crime Prevention* by Lawrence J. Fennelly. Permission obtained from the National Crime Prevention Institute, School of Justice Administration, University of Louisville.

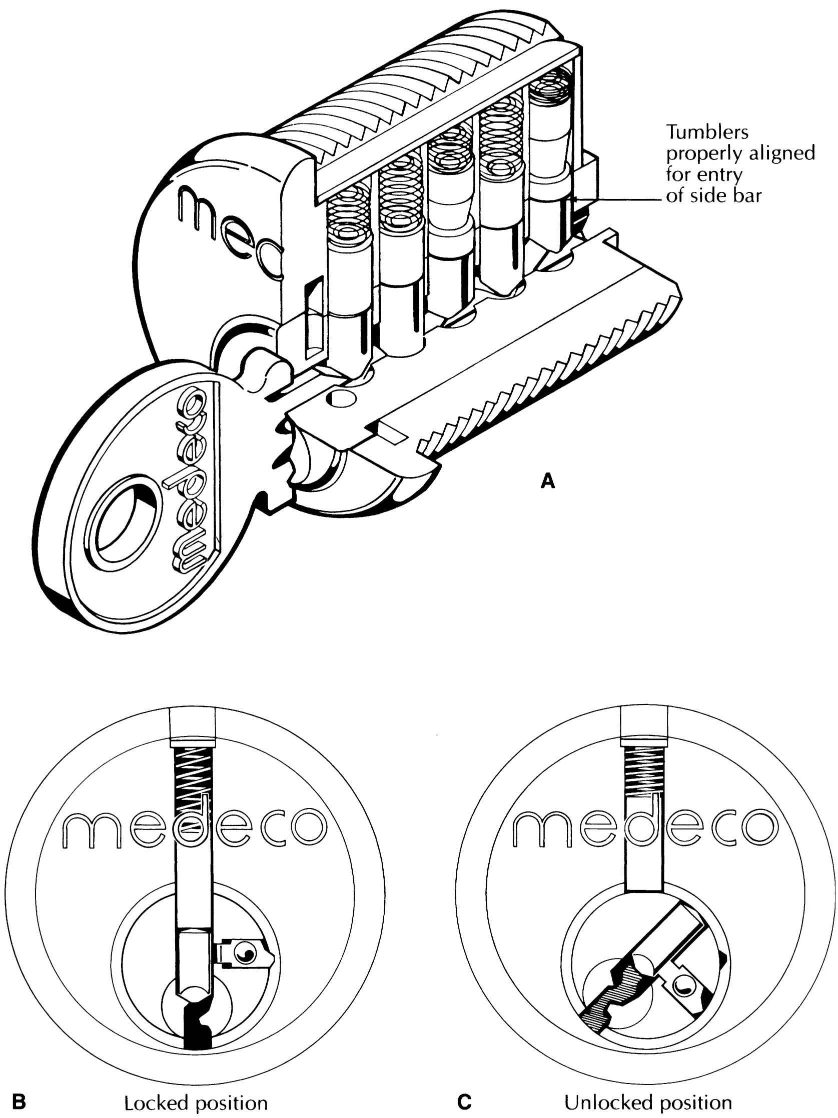


Figure 5.10 (A) A cutaway of a pin tumbler lock showing the springs and tumblers. (B) Locked position. (C) Unlocked position. Courtesy of Medeco Security Locks, Inc. Reprinted from Fischer, Robert J. and Gion Green, *Introduction to Security* (Butterworth–Heinemann, Boston, 1998), p. 221.

and are extremely useful in high-rise office buildings where large numbers of keys are required.

A tumbler mechanism is any lock mechanism having movable, variable elements (the tumblers) that depend on the proper key (or keys) to arrange them into a straight line, permitting the lock to operate (Figure 5.11). The pin tumbler is the lock barrier element that provides security against improper keys or manipulation. The specific key that operates the mechanism (which is

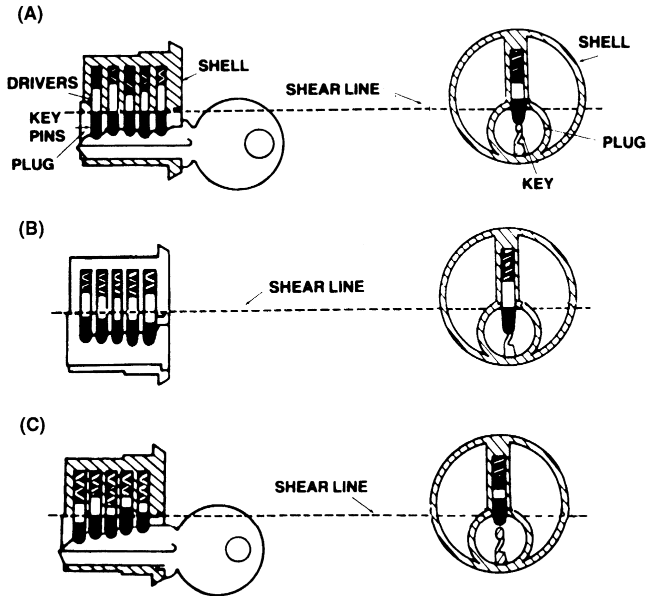


Figure 5.11 Operation of a pin tumbler cylinder mechanism. (A) When the correct key is inserted, the bittings in the key align the tops of the lower tumblers (key pins) with the top of the cylinder plug at the shear line. The plug may then be rotated in the shell to operate the lock. (B) When the key is withdrawn, the springs push the upper tumblers (drivers) into the cylinder plug. With the pins in this position, the plug obviously cannot be turned. (C) When an incorrect key is used, the bittings will not match the length of the key pins. The key will allow some of the drivers to extend into the plug, and some of the key pins will be pushed into the shell by high cuts. In either case, the plug cannot be rotated. With an improper key, some of the pins may align at the shear line, but only with the proper key will all five align so that the plug can turn. (From Edgar, James M., and William McInerney, ''The use of locks in physical crime prevention,'' in L. Fennelly, *The Handbook of Loss Prevention* [Butterworth–Heinemann, Boston, 1989], p. 230, with permission.)

called the change key) has a particular combination of cuts or bittings that match the arrangement of the tumblers in the lock. The combination of tumblers usually can be changed by inserting a new tumbler arrangement in the lock and cutting a new key to fit this changed combination. This capability provides additional security by protecting against lost or stolen keys. The different arrangements of the tumblers permitted in a lock series are its combinations. The total possible combinations available in a specific model or type of lock depends on the number of tumblers used and the number of depth intervals or steps possible for each tumbler. Master keying greatly reduces the number of useful combinations.

Pin tumbler mechanisms vary greatly in their resistance to manipulation. Poorly constructed inexpensive cylinders with wide tolerances, a minimum number of pins, and poor pin chamber alignment may be manipulated quickly by persons of limited ability. Precision-made cylinders with close tolerances, a maximum number of pins, and accurate pin chamber alignment may resist picking attempts even by experts for a considerable time. (Picking a lock involves the use of metal picks to align the tumblers in the same manner as an authorized key would do, thus making it possible for the lock to operate.)

There are a number of variations of the pin tumbler cylinder on the market. The removable core cylinder (Figure 5.12) often is used in high-rise buildings. The Best Universal Lock Company, whose initial patents have now expired, originally produced it. This type of cylinder uses a special key called the *control key* to remove the entire pin tumbler mechanism (called the core) from the shell. This makes it possible to quickly replace one core with another having a different combination and requiring a different key to operate it.

Removable core cylinders provide only moderate security. Most systems operate on a common control key, and possession of this key will allow entry through any lock in the system. It is not difficult to have an unauthorized duplicate of the control key made. If this is not possible, any lock of the series (particularly a padlock) may be borrowed and an unauthorized control key may be made. Once the core is removed from a lock, a screwdriver or other flat tool is all that is necessary to operate the mechanism. In addition, the added control pins increase the number of shear points in each chamber, thus increasing the mechanism's vulnerability to manipulation.

Bolts and Strikes

Before discussing the master keying of pin tumbler locks, it will be helpful to our understanding of locking systems to review two parts of locking mechanisms, namely bolts and strikes.

Bolts

There are two types of bolts used for most door applications: the latch bolt and the deadbolt (Figure 5.13). They are easily distinguished from each other.

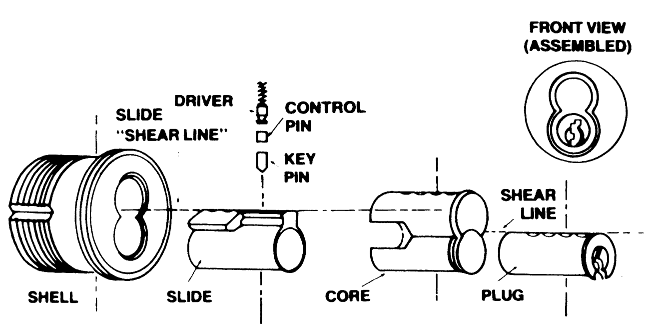


Figure 5.12 A removable-core pin-tumbler cylinder mechanism. (From Edgar, James M., and William McInerney, "The use of locks in physical crime prevention," in L. Fennelly, *The Handbook of Loss Prevention* [Butterworth–Heinemann, Boston, 1989], p. 231, with permission.)

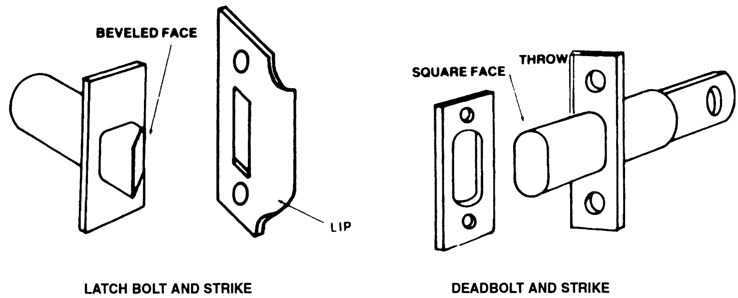


Figure 5.13 The basic types of bolts. (From Edgar, James M., and William McInerney, ''The use of locks in physical crime prevention,'' in L. Fennelly, *The Handbook of Loss Prevention* [Butterworth–Heinemann, Boston, 1989], p. 236, with permission.)

A latch bolt always has a beveled face, whereas the face on a standard deadbolt is square. (A latch is a device for holding a door closed. It may incorporate a bar falling or sliding into a hole, catch, or groove.)

A **latch bolt**—which sometimes is called a latch, a locking latch (to distinguish it from nonlocking latches), or a spring bolt—is always spring-loaded. When the door on which it is mounted is closing, the latch bolt retracts automatically when its beveled face contacts the lip of the strike. Once the door is fully closed, the latch springs back to extend into the hole of the strike, securing the door.

A latch bolt has the single advantage of convenience. A door equipped with a locking latch will automatically lock when it is closed. No additional effort with a key is required. It does not, however, provide very much security.

The throw on a latch bolt is usually 3⁄8 inch but seldom more than 5⁄8 inch (Throw is the maximum distance that the bolt can extend.) Because it must be able to retract into the door on contact with the lip of the strike, it is difficult to make the throw much longer. However, because there is always some space between the door and the frame, a latch projects into the strike no more than ¼ inch (often as little as 1⁄8 inch on poorly hung doors). Most door jambs can be spread at least ½ inch with little effort, permitting an intruder to circumvent the lock quickly.

Another undesirable feature of the latch bolt is that it can easily be forced back by any thin shim (such as a plastic credit card or thin knife) inserted between the face plate of the lock and the strike. Antishim devices have been added to the basic latch bolt to defeat this type of attack (Figure 5.14A). They are designed to prevent the latch bolt from being depressed once the door closes. These often are called *deadlocking latches*, a term that is mildly deceptive because these latches do not actually deadlock and are not nearly as resistant to jimmying as deadlocks. Often a thin screwdriver blade can be inserted between the faceplate and the strike and pressure applied to break the antishim mechanism and force the latch to retract.

An antifriction latch bolt (Figure 5.14B) reduces the closing pressure required to force the latch bolt to retract, which permits a heavier spring to be

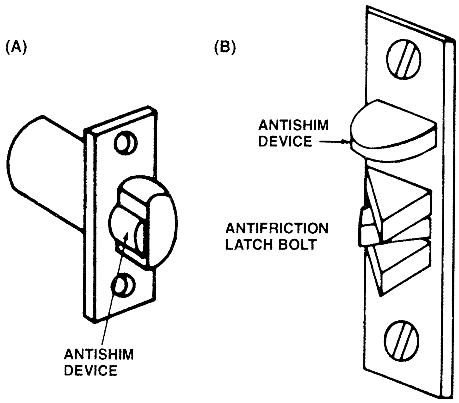


Figure 5.14 Modified latch bolts. (A) Latch bolt with antishim device. (B) Antifriction latch bolt with antishim device. (From Edgar, James M., and William McInerney, "The use of locks in physical crime prevention," in L. Fennelly, *The Handbook of Loss Prevention* [Butterworth–Heinemann, Boston, 1989], p. 237, with permission.)

used in the mechanism. Most modern antifriction latches also incorporate an antishim device. Without it, the antifriction latch is extremely simple to shim.

The **deadbolt** is a square-faced solid bolt that is not spring loaded and must be turned by hand into either the locked or unlocked position. When a deadbolt is incorporated into a locking mechanism, the result usually is known as deadlock. The throw on a standard deadbolt is also about ½ inch, which provides only minimal protection against jamb spreading. A long-throw deadbolt, however, has a throw of 1 inch or longer. One inch is considered the minimum for adequate protection. When properly installed in a good door using a secure strike, this bolt provides reasonably good protection against efforts to spread or peel the jamb.

The ordinary deadbolt is thrown horizontally. On some narrow-stile doors (stile refers to the vertical uprights forming the frame around the glass panels), such as aluminum-framed glass doors, the space provided for the lock is too narrow to permit a long horizontal throw. The pivoting deadbolt is used in this situation to get the needed longer throw (Figure 5.15). The pivoting movement of the bolt allows it to project deeply into the frame—at least the recommended minimum of 1 inch, and usually more. When used with a reinforced strike, this bolt can provide good protection against efforts to spread or peel the frame.

Strikes

Strikes are an often overlooked but essential part of a good lock. A deadbolt must engage a solid, correctly installed strike, or its effectiveness is reduced significantly (Figure 5.16).

Master Keying of Pin Tumbler Locks

Master keying is a variation of pin tumbler locks that has been in widespread use for many years. Almost any pin tumbler cylinder can easily be master keyed. Additional tumblers called master pins are inserted between the drivers and key pins. These master pins enable a second key, the master key, to operate the same lock (Figure 5.17).

Generally, an entire series of locks is combined and operated by the same master key. There may also be levels of master keys, including submasters that

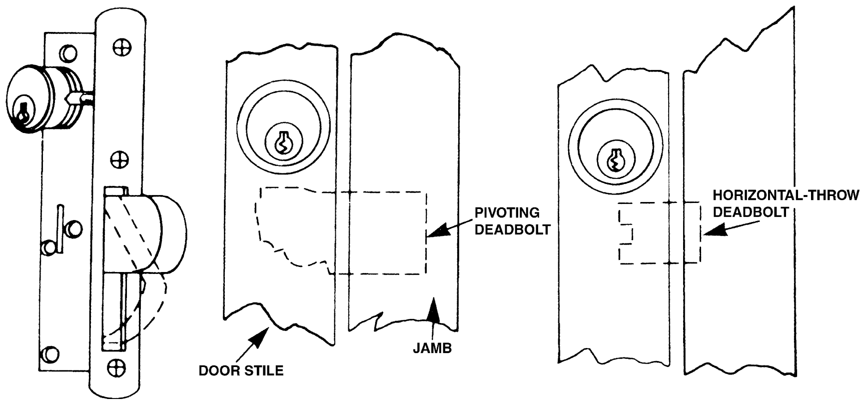


Figure 5.15 A modified deadbolt—the pivoting deadbolt. The deeper penetration into the door jamb afforded by the pivoting deadbolt increases protection against door jamb spreading. (From Edgar, James M., and William McInerney, "The use of locks in physical crime prevention," in L. Fennelly, *The Handbook of Loss Prevention* [Butterworth–Heinemann, Boston, 1989], p. 238, with permission.)

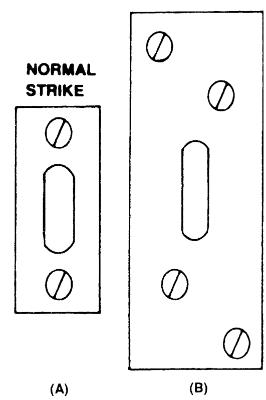


Figure 5.16 (A) A normal strike. (B) A security strike with offset screws. (From Edgar, James M., and William McInerney, "The use of locks in physical crime prevention," in L. Fennelly, *The Handbook of Loss Prevention* [Butterworth–Heinemann, Boston, 1989], p. 243, with permission.)

open a portion, but not all, of a series; master keys that open a larger part; and grand masters that open the entire series. In very involved installations, there may even be a fourth level (grand grand master key). A description of the various keys in a typical high-rise office building master key system follows:

1. The change key operates a single lock within the master key system. For example, individual occupants of a tenant space have a key that unlocks the door of their office but does not unlock perimeter doors leading to the tenant space.
2. The submaster key operates all locks within a particular area or group. For example, a tenant office manager has a key that unlocks all perimeter doors leading to his or her tenant space and all interior office doors within this space.
3. The floor master key operates one or more submaster systems. For example, a member of building management has a key that unlocks all perimeter doors leading to tenant spaces on a multiple-tenant floor, all interior office doors within these tenant spaces, and all maintenance spaces on that floor.

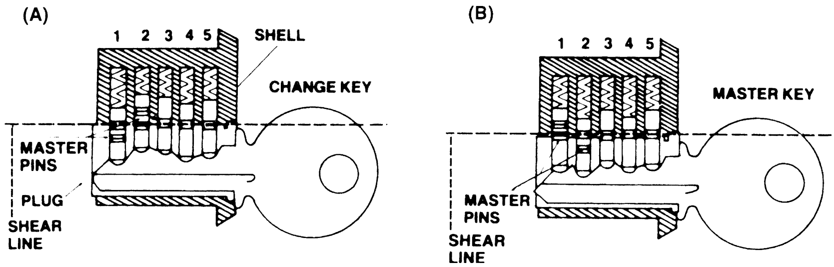


Figure 5.17 A master-keyed pin tumbler cylinder mechanism. (A) This is a simple master-keyed system using master pins in the first and second tumbler positions. When the change key is inserted, note that the top of the first master pin aligns with the top of the cylinder plug. The remaining positions show the key pins aligned with the top of the plug to turn. (B) With the master key inserted, the first position aligns the top of the key pin with the cylinder plug. The master pin is pushed further up the pin cylinder. The second position shows the master pin aligning at the top of the plug. The master pin has dropped further down the pinhole in the plug. The remaining three positions are unchanged. This arrangement also allows the plug to rotate. (From Edgar, James M., and William McInerney, ''The use of locks in physical crime prevention,'' in L. Fennelly, *The Handbook of Loss Prevention* [Butterworth–Heinemann, Boston, 1989], p. 232, with permission.)

4. The grand master key operates one or more master systems. For example, a member of building management has a key that unlocks all perimeter doors leading to tenant spaces, all interior office doors within tenant spaces, and all maintenance spaces within the building.
5. The grand grand master key operates one or more grand master systems. For example, in a high-rise project in which there are several high-rise buildings, a member of building management has a key that unlocks all perimeter doors leading to tenant spaces, all interior office doors within tenant spaces, and all maintenance spaces on all floors of all buildings.

An example of a master key arrangement is shown in Figure 5.18.

There are a number of security problems with master keys. The most obvious one is that an unauthorized master key will permit access through any lock of the series. Loss of a master key will compromise the whole system, necessitating an entire building to be re-keyed at a considerable cost. Finneran (1981) advises, ''If rekeying becomes necessary, it can be accomplished most economically by installing new locking devices in the most critical points of the locking system and moving the locks removed from these points to less sensitive areas. Of course, it will be necessary to eventually replace all the locks in the system, but by using the method just described the cost can be spread out over several budgeting periods.''

Another possible solution to mitigate the cost of rekeying is a high-security lock system developed in the 1980s. InstaKey™ is a unique system that allows locks to be rekeyed by simply inserting and turning a specially designed key (Figure 5.19). According to InstaKey, their lock permits up to fifteen changes to be loaded into the lock cylinder distributed in any combination between grand

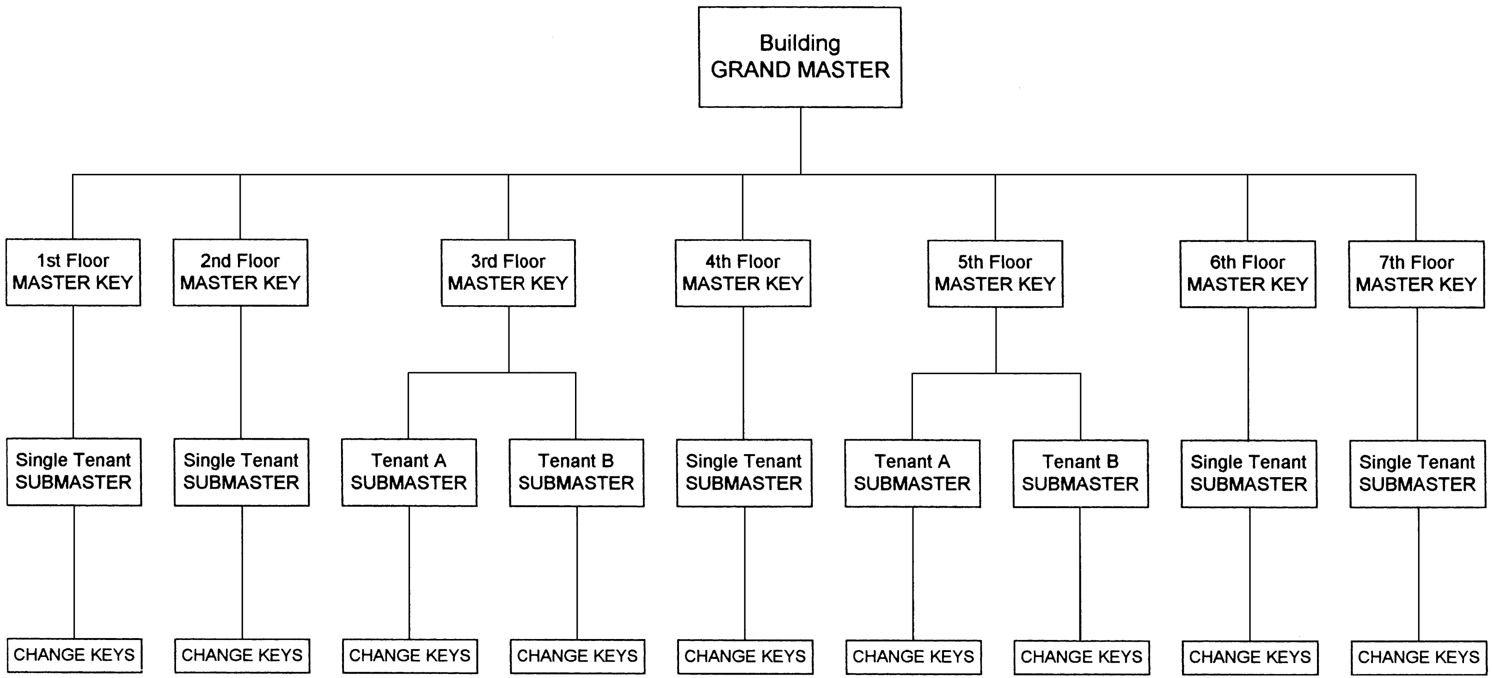


Figure 5.18 Diagram of a sample master key arrangement for a seven-story building.

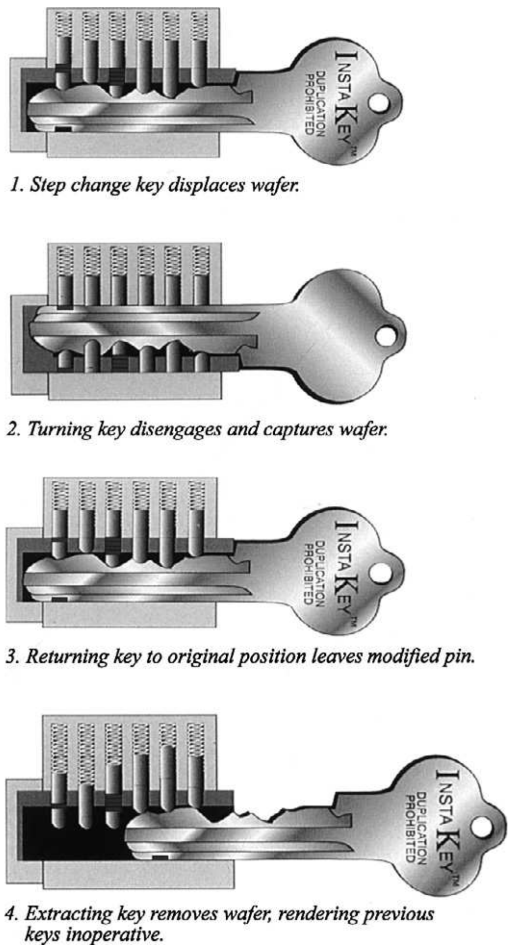


Figure 5.19 InstaKey™ four-step key change. Courtesy of InstaKey Lock Corporation.

master, master, and change key levels. It achieves this by a special key that removes wafers from different stacks within the lock cylinders. The lock also allows any level to be changed individually without affecting the operation or keying of any other level. Once all wafers have been removed, the cylinder can be reloaded and the cycle begun again.

An important feature of this system is that it allows locks to be changed immediately by the simple turn of a key. This is crucial from a security standpoint because a potential security breach can be addressed immediately. The expense of the lock change is restricted to the replacement keys for the affected level only. InstaKey is compatible with 90 percent of all locking systems, including Medeco, Corbin, and Falcon technologies. Converting locks to the InstaKey system is more expensive than a regular lock change. However, once the system is installed, subsequent lock changes are substantially cheaper and the system pays for itself within approximately three lock changes (InstaKey, 1995). Another locking system, the Winfield Lock, performs a similar function to InstaKey. Rather than removing wafers, this system operates using a mechanical adjustment.

A less obvious security problem with master key systems is the fact that master keying reduces the number of useful combinations because any combination used must not only be compatible with the change key, but also with the master key. If a submaster is used in the series, the number of combinations is reduced further to those compatible with all three keys. If four levels of master keys are used, the number of useful combinations becomes extremely small. If a large number of locks are involved, the number of locks may exceed the number of available combinations. When this occurs, it may be necessary to use the same combinations in several locks, which permits one change key to operate more than one lock (cross keying). This creates an additional security hazard.

One way of increasing the number of usable combinations and decreasing the risk of cross keying is to use a master sleeve or ring. This sleeve fits around the plug, providing an additional shear line similar to the slide shear line in a removable core system. Some of the keys can be cut to lift tumblers to the sleeve shear line, and some to the plug shear line. This system, however, requires the use of more master pins. Any increase in master pins raises the susceptibility of the lock to manipulation, because the master pins create more than one shear point in each pin chamber, increasing the facility with which the lock can be picked.

The basic pin tumbler mechanism has been modified extensively by a number of manufacturers to improve its security. High-security pin tumbler cylinder mechanisms used in high-rise buildings commonly are produced with extremely close tolerances and provide a high number of usable combinations. Additional security features include the use of very hard metals in their construction to frustrate attacks by drilling and punching.

Perimeter Locking Devices

To meet life safety codes, perimeter legal exit doors require approved panic hardware such as cross bars or push pads. This hardware is installed on building exterior doors normally located at the ground level, with the exception of stairwell exit doors. (According to National Fire Protection Association [NFPA[*]] codes, panic hardware[†] is used on doors that are not fire doors; approved fire exit hardware[‡] is required on fire doors.)

NFPA 101, *Life Safety Code,* Section 7.2.1.7.3, states, ''Required panic hardware and fire exit hardware shall not be equipped with any locking device, set screw, or other arrangement that prevents the release of the latch when pressure is applied to the releasing device. Devices that hold the latch in the retracted position shall be prohibited on fire exit hardware unless listed and approved for that purpose'' (NFPA 101, 2000).

---

[*]All NFPA material in this chapter is used with the permission of the National Fire Protection Association, Quincy, MA, 2000.

[†]*Panic hardware* is defined as ''a door-latching assembly incorporating a device that releases the latch upon the application of a force in the direction of egress travel'' (NFPA 101, 2000).

[‡]*Fire exit hardware* is defined as ''a door-latching assembly incorporating a device that releases the latch upon the application of a force in the direction of egress travel and provides fire protection where used as part of a fire door assembly'' (NFPA 101, 2000).

The different models of panic hardware and fire exit hardware include the following:

1. Latch at top and bottom of the door (called a vertical rod device): these can be surface-mounted (easier for installation) or concealed (aesthetically more pleasing)
2. Latch at one point in the door frame (referred to as a rim exit device)
3. Mortised exit device that also latches at a single point in the door frame

The push pad style has gained wide acceptance. One advantage to these push pads is that electric latching and electronic monitoring features can be added. Doors equipped with panic bars or pads may be locked on the exterior side, but at all times the inside of the door must be operable, providing uninhibited egress.

Panic hardware and fire exit hardware function well but provide only a low level of security. A reason for this is that some doors can be compromised easily from the outside (using, for example, a simple device such as a coat hanger to pull a bar down to release the door). When these devices are installed on aluminum doors, particularly on large front entrance doors, the installation must be done in such a way as to make the device somewhat secure. One way to do this is to use an electromagnetic lock, which meets life safety requirements.

Electromagnetic Locks

Electromagnetic locks are very useful in high-rise buildings. ''Devoid of moving parts—a characteristic that eliminates wear and binding—an electromagnetic lock possesses a holding power of from 1,500 to 2,700 lbs. and consumes six to nine watts of power at 24 volts'' (Geringer, 1991, p. 1).

Electromagnetic locks may be concealed (called shear electromagnetic locks) or exposed (called direct hold electromagnetic locks). They consist of an electromagnet, which is attached to the door frame header, and a metal armature or plate, which is mounted on the door itself (Figure 5.20). The *New Webster Dictionary* (1980 edition) defines an *electromagnet* as ''a bar of soft iron rendered temporarily magnetic by a current of electricity having been caused to pass through a wire coiled round it.'' When an electrical current is flowing through the electromagnet (usually at a low voltage of 12 or 24 volt DC), a magnetic field is created, and the armature is magnetically attracted to the magnet in the door frame, thereby holding the door closed.

Electromagnetic locks can be installed on perimeter legal exit doors and main entrance doors. Through use of a time clock, these doors can be locked automatically at the end of the day when the building closes. The times of opening and closing these perimeter doors can vary according to the building's needs. When the doors are secured, access from the outside of the building can be obtained by hooking up a card reader (normal egress is permitted using panic hardware or automatic unlocking devices such as motion detectors). Persons authorized to enter use their access card to open the door. In addition, the position of the door (whether it is open or closed) and its locking status (locked or unlocked) can be monitored at a remote location, such as the Security Command Center, via sensors included on the electromagnetic lock.

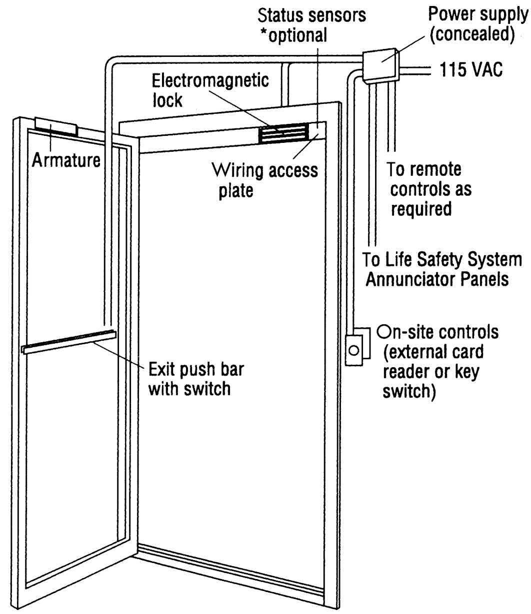


Figure 5.20 A typical installation of a direct hold electromagnetic lock for a single door with request to exit push bar. The electromagnet is attached to the door frame header, and a metal armature or plate is mounted on the door itself. Courtesy of Security Door Controls of Westlake Village, CA (for the Series 1500 EMLock).

Life safety codes mandate that the power source to all locks restricting occupants' means of egress must be supervised by the building's fire life safety system. In the event of an emergency, such as a power failure or activation of a fire alarm, electrical current to the electromagnet ceases and the doors unlock (i.e., fail-safe). Occupants can freely exit the building and responding emergency agencies, such as the fire department, can enter.

''The benefits of electromagnetic locks are that fire safety requirements can be easily met, security is attained and access is provided for select personnel. Electromagnetic locks take the place of illegal or other unapproved methods of security by eliminating the need for chains, padlocks, and other mechanical devices'' (Geringer, 1991, p. 1). Also, electromagnetic locks require minimal maintenance and are well adapted to poorly fitted or poorly hung doors; however, a good flat connection of the electromagnet and the armature or plate must still be made. The invention of the electromagnetic lock has been a great asset to high-rise building owners and managers in satisfying the demands of both fire life safety codes and security requirements.

Stairwell Locking Devices

Stairwell door security is a lot more complicated than perimeter door security. The stringent code requirements and specifications for stairwell locks and locking systems are essential because stairwells are a critical means of egress for occupants during building emergencies. During a fire, elevators generally are not considered a safe means of general population evacuation (although under special circumstances, when the fire department directs, they might be used for evacuation of the disabled). This leaves the stairwells as the primary means of egress.

Critical stairwell specifications of NFPA 101, *Life Safety Code* (which itself, or a modification thereof, has been adopted by many authorities having jurisdiction), are:

> Section 7.2.1.5.1 Doors shall be arranged to be opened readily from the egress side whenever the building is occupied. Locks, if provided, shall not require the use of a key, a tool, or special knowledge or effort for operation from the egress side.
> Section 7.2.1.5.2 Every door in a stair enclosure serving more than four stories shall allow re-entry from the stair enclosure to the interior of the building, or an automatic release shall be provided to unlock all stair enclosure doors to allow re-entry. Such automatic release shall be actuated with the initiation of the building fire alarm system. (NFPA 101, 2000)

The *Life Safety Code* allows for some exceptions to this, particularly in older high-rise buildings in which automatic release systems are not installed. These exceptions may allow selected doors on stair enclosures to be equipped with hardware that prevents re-entry into the interior of the building provided that, for example, the following conditions are met:

- There are at least two levels where it is possible to leave the stair enclosure.
- Not more than four floors intervene between floors where it is possible to leave the stair enclosure.
- Possible re-entry points exist on the top or next to top floor, permitting access to another exit.
- Doors allowing re-entry are identified as such on the stair side of the door.
- Doors not allowing re-entry have a sign on the stair side indicating the location of the nearest door, in each direction of travel, that allows re-entry or exit.

As Geringer (1991, p. 2) points out,

> The inherent problem is that building tenants may need to lock these exits on the stair side for obvious security concerns, such as transient pedestrian traffic. To ensure life safety [i.e., fire door integrity], all stairwell doors require a . . . mechanism that maintains a closed and latched door position, even when the door is unlocked, to prevent smoke and fire from entering the stairwell. . . . One solution is to install high-tower-function electrified mortise locksets on appropriate stairwell doors [Figure 5.21]. These locks are equipped with door-position sensors as well as locked/unlocked status sensors. When energized, only the stair side is secured. . . . . Generally, high-tower-function mortise locks are energized and locked at all times. Access control is accomplished by either a mechanical key, digital keypad, or a card reader. . . . The power source for these locks is controlled by the building life safety system so that in an emergency, doors immediately unlock yet remain closed and latched, protecting the stairwell from smoke and fire.
>
> The obvious benefits of this type of lock are that:
>
> - Life safety is provided.
> - Authorized personnel have controlled access.
> - Building tenants have supervised security.

Before leaving the discussion of stairwells, let us address the subject of fire exit hardware. Fire exit hardware is installed on fire doors within a high-rise building, including stairwell exit doors that normally exit at the ground level. These doors must remain closed and latched at all times for fire

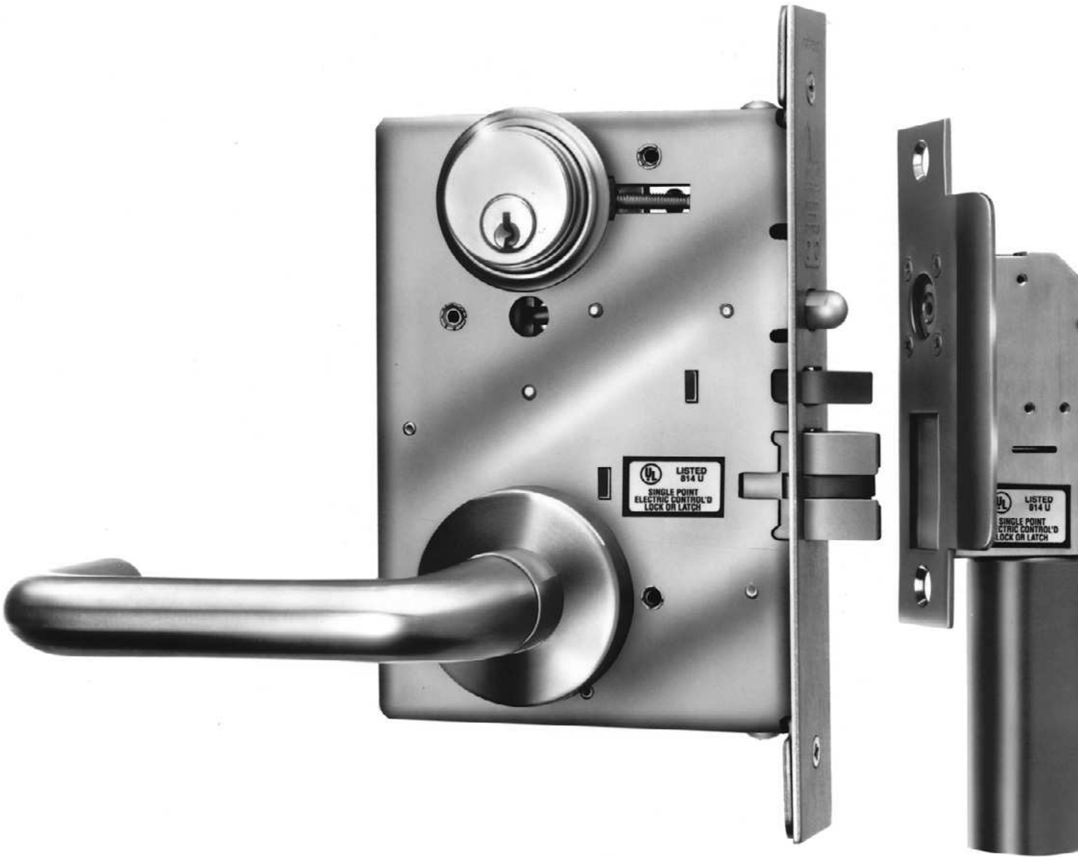


Figure 5.21 HiTower™ electrically controlled mortise lockset that installs in the stairwell door, with the electric controller that installs in the door frame. Courtesy of Security Door Controls of Westlake Village, CA.

compartmentation purposes. Fire exit hardware may consist of cross bars or push pads (see the previous section for the different models available).

Stairwell exit doors that normally exit at the ground level may be locked on the exterior side as long as, at all times, the inside of the door is operable, providing uninhibited egress. When an exiting occupant applies pressure to the fire exit hardware, the door will immediately unlock (although, as is discussed in the next section, under special circumstances a delayed egress lock may be incorporated into the emergency exit system). One way of doing this is to use a powerful electromagnetic lock to deter unauthorized entry from the outside of the building.

Delayed-Egress Locks

The fact that security and fire life safety are different disciplines, and that their priorities are sometimes in conflict with each other, is nowhere better demonstrated than at the stairwell exit. ''The conflict lies between the need to have immediate, unobstructed, one-step exit from a building that may be on fire and the need to prevent unauthorized ingress or egress'' (Atlas, 1993, p. 5).

As just discussed, stairwell exterior fire doors may be secured with an electromagnetic lock to deter unauthorized entry from the outside of the building. This maintains a high degree of security and has no impact on life safety. However, only under specific conditions can fire exit doors be locked from the inside of the stairwell at the point of exit from the building. NFPA 101, *Life Safety Code,* states:

> Section 7.2.1.5.1 Doors shall be arranged to be opened readily from the egress side whenever the building is occupied. Locks, if provided, shall not require the use of a key, a tool, or special knowledge or effort for operation from the egress side.
>
> Section 7.2.1.5.4 Doors shall be operable with not more than one releasing operation.
>
> Section 7.2.1.5.6 Devices shall not be installed in connection with any door on which panic hardware or fire exit hardware is required where such device prevents or is intended to prevent the free use of the door for purposes of egress. (NFPA 101, 2000)

These life safety requirements present a security problem—the need to maintain immediate, unobstructed, one-step exit from the stairwell at the ground level provides an opportunity for a person who has perpetrated a crime within the building to make a rapid exit. The NFPA addresses the need to maintain a degree of security on these emergency exit doors in NFPA 101, *Life Safety Code*.

> Section 7-2.1.6.1 Approved, listed, delayed-egress locks shall be permitted to be installed on doors serving low and ordinary hazard contents [i.e., those hazards most likely found in high-rise office buildings] in buildings protected throughout by an approved, supervised automatic fire detection system in accordance with Section 9.6 [Fire Detection, Alarm, and Communication Systems], or an approved, supervised automatic sprinkler system in accordance with Section 9.7 [Automatic Extinguishers and Other Extinguishing Equipment], and where permitted in Chapters 12 through 42, provided that the following criteria are met.
>
> a) The doors shall unlock upon actuation of an approved, supervised automatic sprinkler system in accordance with Section 9.7 or upon the actuation of any heat detector or activation of not more than two smoke detectors of an approved, supervised automatic fire detection system in accordance with Section 9.6.
>
> b) The doors shall unlock upon loss of power controlling the lock or locking mechanism.
>
> c) An irreversible process shall release the lock within 15 seconds upon application to the release device required in 7.2.1.5.4 that shall not be required to exceed 15 lbf (67 N) nor be required to be continuously applied for more than 3 seconds. The initiation of the release process shall activate an audible signal in the vicinity of the door. Once the door lock has been released by the application of force to the releasing device, relocking shall be by manual means only.
> *Exception:* Where approved by the authority having jurisdiction, a delay not exceeding 30 seconds shall be permitted.
>
> d) On the door adjacent to the release device, there shall be a readily visible, durable sign in letters not less than 1 in. (2.5 cm) high and not less than 1⁄8 in. (0.3 cm) in stroke width on a contrasting background that reads as follows:

PUSH UNTIL ALARM SOUNDS.
DOOR CAN BE OPENED IN 15 SECONDS.

As Atlas (1993, p. 5) points out, ''If the exit doors are designed as part of an integrated system, the time delay can be a substantial crime prevention tool'' (Figure 5.22).

Sequence of Events

If a person uses a stairwell to escape the building at the ground level after committing a crime on an upper floor, the following sequence of events could be designed to occur when he or she pushes on the emergency exit release bar:

- An alarm on the door will sound but the door will not immediately open.
- Activation of the door alarm will trigger an alarm signal at the Security Command Center to alert security staff to the situation. Building security using an intercom that communicates with this area could challenge the person, and staff members could be dispatched immediately to the location. If the suspect is attempting to flee the building, for example, security could go to the outside of the stairwell and possibly intercept him or her.
- A CCTV camera at the emergency exit door could be automatically activated to record the event.

Figure 5.22 Pair of emergency exit fire doors equipped with a delayed exit system. Note the rim-mounted push bar, the surface-mounted electromagnetic lock at the top of each door (close to the center divider), and the key switch that operates the electromagnetic lock immediately adjacent to the pair of doors on the right-hand side. (Each door is also equipped with surface-mounted automatic door-closing mechanisms.) Courtesy of Von Duprin, Incorporated, Indianapolis, IN.

Thus this 15-second (or 30-second, where permitted) egress delay may allow enough time for security staff to take action and to obtain a recorded image that may be helpful in identifying the individual and any property they may be carrying. The lock thus provides an opportunity to implement basic security measures without a substantial impact on life safety. Some delayed egress locking systems are even designed with features such as verbal exiting instructions and a lighted digital countdown display to indicate how many seconds remain before the door will release (Security Door Controls, 1995). Of course, the authority having jurisdiction must be consulted when installing such delayed-egress locks.

Tenant Locking Devices

Office doors within tenant space create a different type of problem. Those not leading to a legal exit, such as a perimeter or stairwell door, are permitted to use a variety of electric and combination locks (in addition to key-, card-, token-, and biometric system–operated locks), depending on their application.

Electric Locks

The three main types of electric locks are electromagnetic locks, electric strikes, and electric bolt locks. They are available in two operating modes: fail-safe—unlocked when deenergized, locked when energized, and fails into safe (unlocked) mode; and fail-secure—locked when deenergized, unlocked when energized, and fails into secure (locked) mode. The exception to this is the electromagnetic lock described before, which is fail-safe only.

The following description of electric strikes and electric bolt locks was obtained from *Electronic Locking Devices* by John L. Schum (1988, pp. 23–69).

- Electric strikes (also called electric door openers or electric releases) use either an electromagnet or a solenoid to control a movable keeper (Figure 5.23). The *New Webster Dictionary* (1980) defines a *solenoid* as: ''a coil of wire wound in the form of a helix, which, when traversed by an electric current, acts like a magnet.'' The keeper interfaces with the bolt of the lock device on the door. Electrical actuation of the strike allows the door to open even though the bolt of the lock device still is extended. Electric strikes usually are installed in the door frame in place of the conventional lock strike plate. They also are available for mounting on the door frame. They are used in conjunction with various door locksets to provide additional security features, including convenience and remote operation to lock or unlock doors electrically to control the egress and ingress of persons. Tenant receptionists often use these devices to open entrance doors without the inconvenience of physically going to the door itself.
- Electric bolt locks (or electric locks, electric deadbolts, or power bolts) consist of a spring-loaded bolt that is activated by an electric solenoid and moves into or out of a mounting strike. These generally are mounted in or on the door frame (Figure 5.24). They are not for use on doors used as points of egress. These devices can provide a range from low to high security and are used in traffic control situations, especially interlock systems. An interlock is a system of multiple doors with controlled interaction. Interlocks also are commonly

known as mantraps and sally ports. Security interlocks are popular in high-security areas such as tenant computer rooms. Unlike electric strikes, electric bolt locks require no other mechanical lock device to provide security.

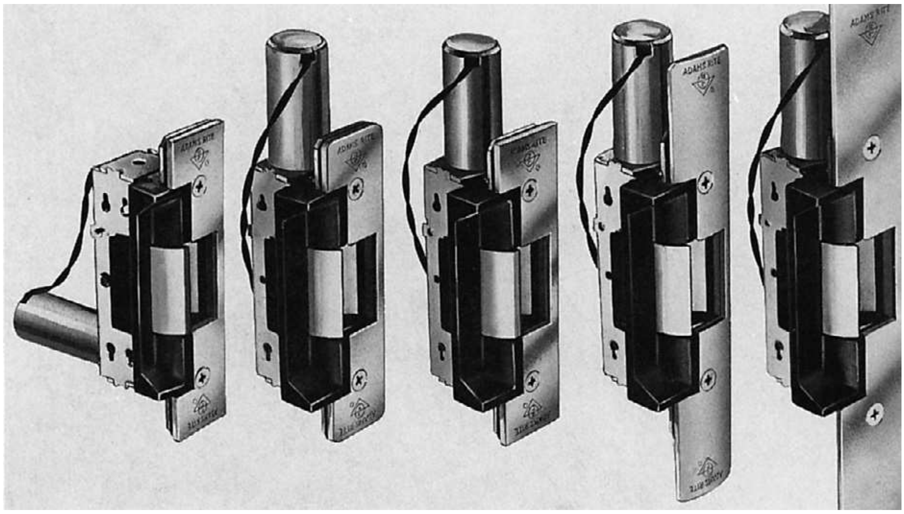


Figure 5.23 Electric strike releases for access control systems. Courtesy of Adams Rite Manufacturing Company. Reprinted from Cumming, Neil, *Security: A Guide to Security System Design and Equipment Selection and Installation* (1992), p. 231.

Figure 5.24 A mortise-mount right-angle electric bolt. Courtesy of Security Door Controls of Westlake Village, CA.

Combination Locks

Combination locks either operate mechanically or electrically (and are not to be confused with the dial-type combination locking mechanisms used on safes, etc.).

A mechanical push-button combination lock has an alphanumeric keypad that is part of the locking mechanism. The keypad is used to enter a series of letters or numbers in a particular predetermined sequence. If the correct sequence of letters or numbers is entered, the bolt in the lock is released mechanically. Some mechanical push-button combination locks are combined with a key that will only operate when the correct sequence of letters or numbers has been entered (Figure 5.25).

An electrical push-button combination lock is different in that the alphanumeric keypad assembly is remote to the locking mechanism. When the correct sequence of letters or numbers is entered, an electrical signal is generated to operate the lock.

Limitations of Combination Locks

A problem with combination locks is that denying access to a person who has the lock combination requires erasing the codes from the lock itself.

Also, someone can surreptitiously obtain the correct sequence of letters or numbers required for operating the lock by looking over the shoulder of a person as they enter the appropriate letters or numbers. A modern electronic numeric keypad manufactured by Hirsch Electronics Corporation has addressed

Figure 5.25 An example of a mechanical push-button lock. Courtesy of SimplexGrinnell, A Tyco Company.

Figure 5.26 Hirsch ScramblePad™ Secure Electronic Digital Keypad. The ScramblePad is also available with the dual technology of a hidden proximity card reader located behind the keypad; and for even higher security applications, a combination of biometrics (fingerprint) with a smart card (fingerprint storage) to activate the ScramblePad. Courtesy of Hirsch Electronics Corporation, Irvine, CA.

this problem. The Hirsch ScramblePad™ Secure Electronic Keypad (Figure 5.26) has a scrambler that automatically changes the position of the numbers on the keypad after each use, and can only be read by a person standing directly in front of the keypad. This makes it much more difficult for anyone other than the person using the device to observe the numbers being entered.

A safety feature incorporated into some combination locks is a duress alarm that is automatically initiated when a particular letter or number or sequence of letters or numbers is entered.

Push-button combination locks should never be installed on doors used as points of egress. Instead they are commonly installed within already-secured areas on doors leading to isolated areas such as a door leading to a computer room within a tenant suite. Electrical push-button combination locks should be equipped with standby power so that in the event of the loss of normal power the lock will continue to operate. If locks are not equipped with this feature, they often are designed, for security reasons, to fail-secure. Also, combinations on push-button locks always should be able to be changed rapidly and without difficulty.

Electromagnetic Hold-Open Devices

Before proceeding to card-operated locks, we will briefly discuss the use of electromagnetic hold-open devices on elevator lobby doors. Elevator lobby doors normally are held in an open position. On activation of the building fire life safety system, electrical current to the electromagnetic hold-open

Figure 5.27 Elevator lobby doors closing on activation of the building's fire life safety system. *Insert*, a close-up of an electromagnetic door holder, courtesy of Sentrol, Inc., Portland, OR.

device ceases and the device releases the lobby doors, which swing shut (Figure 5.27). This results in compartmentation of the elevator lobby and assists in preventing the intrusion of fire and products of combustion into the lobby.

Code Acceptance

The code acceptance of electromagnetic locks, delayed-egress locks, electric strikes, electric bolt locks, or combination locks always should be checked with the local authority having jurisdiction, a registered locksmith, a certified door consultant, or an architectural hardware consultant.[*]

Card-Operated Locks[†]

Card-operated locks are part of electronic access control systems commonly found in modern high-rise office buildings. In general, access control systems consist of the following basic components:

[*]**Note**: The preceding treatment of perimeter, stairwell, and tenant locking devices was developed using an article that appeared in *Access Control Magazine* (June 1991), ''High-Rises Look to Lock Out Problems,'' by Richard Geringer of Security Door Controls (SDC).

[†]A reference essential in compiling this section was *Access Control and Personal Identification Systems* (Bowers, 1988).

- The access control credential itself (whether it be a card, a tag, or a biological characteristic of the person requesting access)
- The access control credential reader (whether it be a card reader, a tag reader, or a biometric reader)
- The central processing unit (CPU) controlling the access control system
- The wiring or wireless communication system from the access control reader to the microprocessor
- The locking device or, in elevator installations, the elevator control system itself
- The closing mechanism of the door and the barrier itself or, in the case of elevator installations, the elevator operating system itself
- The Security Command Center, or similar location, where the microprocessor, keyboard, monitor display screen, and printer is located

According to Cumming (1992, p. 238),

> The various categories of the system all act under the same principle—that recognition of a binary [or, in large systems, hexadecimal] code generated electronically, activates a checking procedure within the system. If, after checking, the code is verified, a second signal activates a locking device [or, in elevator installations, the elevator control system itself], allowing entry. The choice of a particular access system is a matter of trying to match the product to the environment in which it will operate, the level of security required, and the needs of the users.

In the case of the card-operated lock, the unique card or credential of the building user is presented to a card reader at the location where access is being controlled. Within the card reader a sensor deduces information from the card. This information is translated into a binary code that is transmitted electronically to the CPU controlling the system. Access information of the cardholder has previously been programmed into the computer memory. This information, including the identification of the cardholder and the time period in which to grant access, is then compared by the CPU with the code number it has received from the reader. The CPU will then communicate back to the locking device to unlock and facilitate access, or remain locked and thereby deny access. The time the card was used and the identity of the cardholder will be recorded in the memory of the CPU and may also be printed out for future reference. If a communication failure occurs, modern systems are designed to perform, at the card reader location, limited functions of the CPU such as allowing or denying access.

Card-operated locks use various types of cards. Because the card is the key to the system, the system is only as secure as the security afforded to the card itself. The following sections describe cards used with card-operated locks.

Magnetic Slug Cards

Previously the magnetic slug card was widely used but has now been superseded by magnetic stripe cards and barium ferrite cards. The magnetic slug card consisted of magnetic bits embedded in an opaque plastic card in a particular row-and-column pattern. The presence or absence of a magnetic slug was then read by a row of magnetic-sensing heads to determine the appropriate code.

Magnetic Stripe Cards

The magnetic stripe, or mag-stripe (or strip), card is the most inexpensive and frequently used low-security access system card. It has the appearance of a standard credit card. It consists of a magnetic stripe fused onto the card's surface. Information, in the form of a binary code, is recorded on the magnetic stripe. Because the stripe is visible and accessible, and the technology involved is well known, the codes are susceptible to being duplicated, changed, or obliterated (low-strength magnetic fields may cause distortion of the coded information). To address this issue, some manufacturers have recorded on the magnetic stripe a unique code that cannot be changed or removed, and can be read only by using specialized equipment. The cards themselves are prone to normal wear and tear such as cracking and scratching. They are very reliable, producing few false readings, and have particular application where a large number of cards is required. Using a keypad in conjunction with the card reader raises the level of security of such card-operated locks.

Magnetic Sandwich or Barium Ferrite Cards

In these cards a sheet of magnetic material, usually barium ferrite, is laminated in sandwich fashion between two plastic layers. Spots in the magnetic material are magnetized in a particular row-and-column pattern. The presence or absence of a magnetic spot is then read by a row of magnetic-sensing heads to determine the appropriate code. These cards stand up to normal wear and tear very well with the recorded code being protected by the two outer layers of plastic material.

Wiegand Effect Cards

Wiegand cards, also known as embedded wire cards, are used for high-security applications where limited numbers of cards are required. The card has short lengths of special wire embedded within it. A magnetic field is generated within a card reader, causing the wires to carry electronic signals when the card is passed through the reader. These electronic signals determine whether or not a card user is authorized for access. These cards are relatively expensive but are difficult to reproduce and do stand up well to a considerable amount of wear and tear.

Insertion- and Swipe-Type Readers

Before examining other types of cards, it is appropriate to state that the aforementioned cards are usually read by one of the following types of card readers:

- The insertion-type, where the card is held by its end and inserted into a slot in the card reader (Figure 5.28). With this type, clips or chains attached to the card may interfere with the insertion of the card.
- The swipe-type, whereby magnetic stripe cards are held along the top edge of the card and are swiped through a slot in the card reader allowing the

Figure 5.28 Insertion-type electronic card reader. The access card is inserted into the horizontal slot and then removed. Photograph by Roger Flores.

magnetic stripe to be read (Figure 5.29). This reader is preferred to the insertion type because clips or chains attached to the card are not a problem, it has no moving parts requiring maintenance, and its design makes it less susceptible to jamming and the effects of the weather.

Proximity Cards

These low-security cards are usually of the standard credit type with three laminated layers, the center layer containing the coding information. They operate locks in a similar fashion to the aforementioned cards but are not required to come into contact with the card reader.

Proximity cards, when brought in proximity to the reader (Figure 5.30), can communicate with the sensor by electromagnetic, ultrasound, or optical transmissions. Because these user-friendly cards do not need to be inserted into or swiped through the reader, there is less wear and tear on the cards themselves. Because proximity card readers contain no moving parts, maintenance is seldom required. Also, persons carrying items such as books, manuals, a briefcase, a laptop computer, an umbrella, etc., can use proximity cards more conveniently than the previously mentioned insert- or swipe-type cards. Proximity cards are often more convenient for disabled persons to use. A feature of proximity readers is that they can be mounted behind glass or a digital keypad or otherwise made inaccessible to acts of vandalism.

Sometimes, access cards have dual technology. For example, a magnetic stripe card may be used for a building tenant to access a building garage, the building itself, and its elevators. In addition, the tenant may have a proximity card to access his or her office. By providing a dual technology card, a proximity card with a magnetic stripe on it, tenants only need to carry one card.

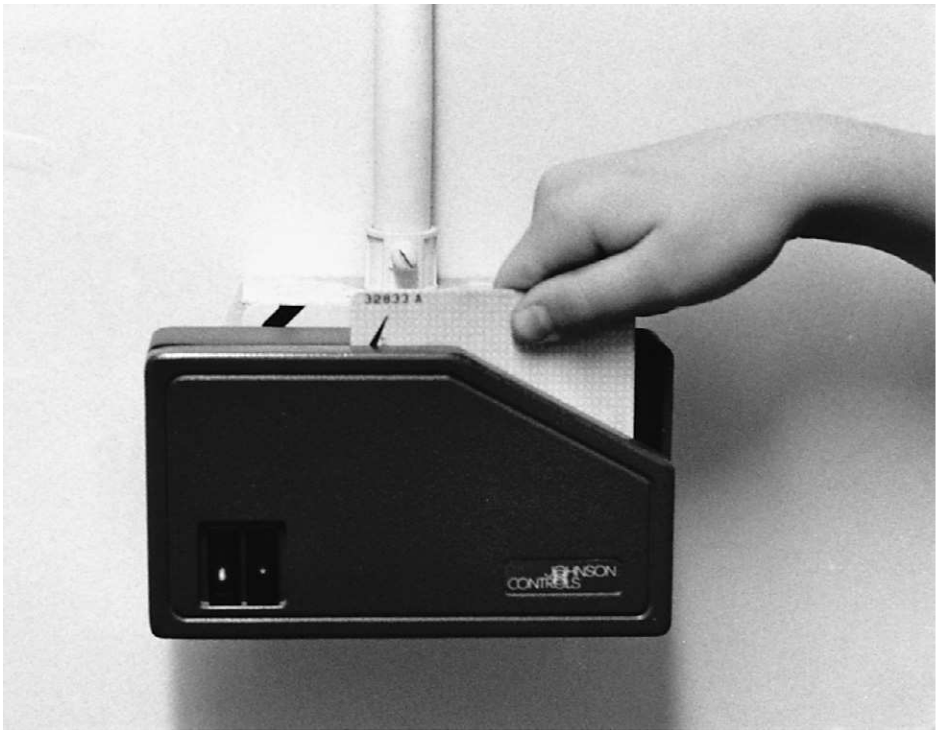


Figure 5.29 Swipe-type electronic card reader. An access card is ''swiped'' through the slot in the card reader. Photograph by Stephen Lo.

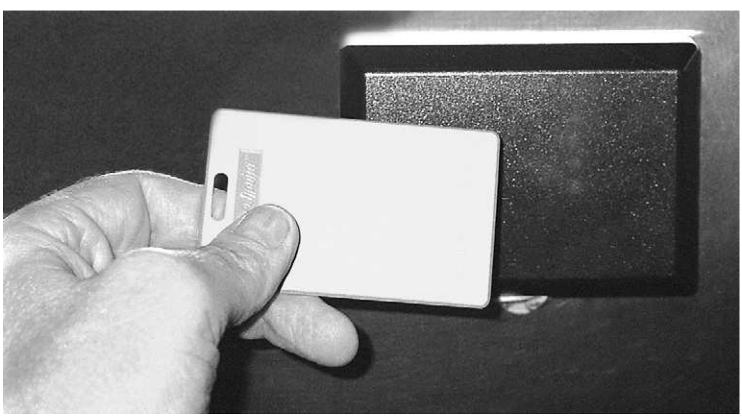


Figure 5.30 Proximity card reader. The access card does not come into direct contact with the reader.

In addition to these card access systems, one may find optical or barcode cards, where the code is embodied in infrared or ultraviolet light form; induction cards, where an electrical circuit contains the coded information; tuned circuit cards, where the code is sensed by radio-frequency waves emitted by the reader (because these cards do not have to come into contact with the reader, they are sometimes called proximity cards); and smart cards.

Smart Cards

Smart cards are similar to a credit card with information stored on a microprocessor-type integrated-circuit chip embedded in the plastic card itself. They can be used to store large amounts of information about the cardholder. There are two basic kinds of smart cards (Harwood, 1999, p. 44, 46),

> An ''intelligent'' smart card contains a central processing unit that actually has the ability to store and secure information, and ''make decisions,'' as required by the card issuer's specific applications needs. Because intelligent cards offer a ''read/write'' capability, new information can be added and processed. For example, monetary value can be added and deducted as a particular application might require.
>
> The second type of card is called a ''memory'' card. Memory cards are primarily information storage cards that contain stored value that the user can ''spend'' in a pay phone, retail, vending or related transaction.
>
> The intelligence of the integrated circuit chip in both types of cards allows them to protect the information being stored from damage or theft. For this reason, smart cards are much more secure than magnetic swipe cards, which carry information on the outside of the card and can be easily copied. Smart cards are an effective way of ensuring secure access to open interactive systems, such as encryption key mobility, secure single sign-ons and electronic digital signatures. . . . The smart card is ideal for IT security applications.

Smart cards are not used widely for access control in high-rise buildings. However, an ''emerging use of smart cards allows service providers such as newspaper delivery carriers and elevator repairmen to enter residential buildings to perform work or make deliveries. Cards can be programmed to allow certain people access to facilities at certain times'' (Gips, 1999, p. 106). This application could work well for particular people, such as couriers and delivery persons, who need to access multiple high-rise buildings at particular times.

> While other types of cards, such as proximity cards, can also be programmed for time-specific access, an advantage that smart cards have over other technologies is that a single chip can carry multiple codes for different kinds of systems, explains Bordes [of the Bordes Group, Orlando, Florida]. Also, the date and the access period are authenticated by a cryptographic algorithm contained in the smart card's chip—a feature not shared by mag stripe or other technologies. This setup eliminates the burden of carrying multiple mechanical keys for multiple buildings. It also authenticates the user and tracks his or her movement. Of course, all the buildings must have the appropriate technology installed for the system to work. (Gips, 1999, p. 106)

Presently, smart cards are generally used for high-security applications such as military and government installations.

Card Reader Applications

Card readers can be used for the various ingress and egress points to high-rise buildings (lobbies, loading docks, parking areas, stairwells, elevators, roofs, elevator machine rooms, fan rooms, central plant, mechanical and engineering facilities, and electrical closets) and tenant spaces. In some modern office buildings, the tenants use the same access card to enter the parking garage, the building itself, the elevator, and their tenant space (and in some facilities, to a building fitness center).

Anti-Passback Feature

Some card access systems that have both entry and exit card readers have an anti-passback feature. This prevents a card from being used again to authorize entry before the card has been used to exit a facility. The anti-passback feature often is used to control access to parking garages.

Piggybacking and Tailgating

As with all card readers, the designed level of security can be compromised when the card user permits tailgating or piggybacking. This occurs when a person who is authorized to enter at the location where access is being controlled permits, willingly or unconsciously, another individual to enter without being subject to the verification procedure. This phenomenon is particularly prevalent at card readers located at building and tenant entrance doors and in elevator cars. After the card has granted access, the authorized tenant holds the building or elevator door open so that the person immediately behind can gain access.

Identification Cards

Cards, in addition to facilitating access, may also be used as company identification cards. In this case, a photograph of the cardholder, a panel requiring the signature of the authorized cardholder, and possibly a company logo and text, can be added to the card itself. The first two features help ensure that the card is being used by the person authorized to do so. To enhance security, the badges may be numbered and issued in sequence. These permanent badges are either photographic-based laminated identification badges or the now prevalent, high-quality color photo ID cards produced quickly and easily using computer-based video imaging systems. As Goldfeld (1994, p. 22) says, the former

> are not capable of efficient badge verification or authentication, because photos and other ID information must be stored in hard copy form and are not readily retrievable. These types of systems also have no safeguards against fraudulent badge production. On the other hand, computer-based, video imaging systems store and retrieve all pertinent verification and authentication information

electronically, keep track of IDs that have been produced, as well as who produced them, and often have a number of security features to combat fraud.

The integration of photo ID badges with access control can be very useful in heightening the level of security for a particular area. ''The best benefit, and the one that increases both the security level and the system's usefulness, is that, in a truly integrated system, any access control system CRT [computer display] screen can display the person's original digital photo. The display can be initiated automatically by the presentation of an ID badge at a card reader or by operator manual selection via a keyboard, or [a] mouse. The operator can then visually compare the retrieved digital photo with the face, either directly or remotely via a CCTV image, of the cardholder'' (Aggleton, 1997, p. 7).

Biometric ID System–Operated Locks

In modern high-rise office buildings, biometric ID system–operated locks are part of electronic access control systems in very specialized areas (and in some major buildings, to control access to the building itself). Biometric ID system–operated locks work on the principle that people have certain biological characteristics unique to each individual. Such characteristics may include fingerprints, hand geometry, signatures, voice patterns, facial recognition, and iris and retina patterns. The biometric ID system works by checking such a physical characteristic. If, after checking, the specific characteristic is verified within the system, a second signal activates a locked device, allowing entry.

At present, biometric ID systems may be susceptible to errors such as rejecting a person authorized to have full access, and permitting access to a person whose access is not authorized. Part of the problem lies in the fact that over time human biological characteristics will change. These changes may be due to weight loss and gain, physical injuries, extended periods of prolonged usage, tiredness, and stress. A possible solution to overcoming this problem of changes may be the development of biometric ID systems that operate on more than one personal characteristic. Also, biometric ID systems are presently more expensive[*] than the conventional card access systems and do not have the ease of user operation that the simple presenting, inserting, or swiping of a card affords. Hence, card-operated locks and optical turnstiles are more attractive vehicles for electronic access control in high-rise buildings.

Rapid Entry Systems[†]

Before leaving the subject of locks and locking systems, it is important to discuss the availability of building and elevator keys for fire department use during an emergency situation. Having to force entry to locked buildings slows down emergency personnel response time, and doors may be unsecurable

[*]However, according to Wayman in Michael Gip's article (September 1999, p. 108), the cost of fingerprint technology (which allows, for example, fingerprint sensors to be built into doors and computer devices, such as the keyboard or a mouse) has dropped drastically.

[†]Much of the information in this section was provided by Knox, the major U.S. supplier of rapid entry systems (Knox System, 1991).

after the incident due to damage caused at entry. Essential building keys should therefore be readily available to a responding unit when arriving on site. If building staffs, such as security or engineering personnel, are not available to meet the responding agency, it is necessary to provide an alternative means to access the site and structure and move freely through it. One possible solution is for the fire department to be in possession of the essential keys for high-rise buildings to which they may be required to respond. For most city fire departments, however, it is virtually impossible to manage and control effectively the thousands of keys that could be involved.

In thousands of buildings across the United States this critical issue of key control is accomplished by way of a fire department rapid entry system, namely a Rapid Entry Key Vault or Fire Department Lock Box. Suppliers of Rapid Entry Vault Systems in the United States are the Knox Company of Irvine, California, and Supra Products, Inc., of Salem, Oregon. Selected building keys, access control cards, and, depending on the size of the selected container, the Building Emergency Procedures Manual, a list of key building personnel contacts, building floor plans, and Hazardous Material Safety Data Sheets may be stored in these specially designed, weatherproof, fixed steel encased boxes and vaults. They are usually installed in a conspicuous location on the exterior vertical wall of the building.

To help prevent tampering, the lock box usually will be situated more than 6 feet above the ground and securely mounted on the surface or recessed into the building wall. In some buildings, the rapid entry box or vault will be equipped with an alarm tamper switch connected to the building intrusion detection system. These UL-listed boxes and vaults are all fitted with the same specially designed master key, supplied free ahead of time to the local fire department. The key is secured to fire department primary response vehicles and ambulance or paramedic units and its use is strictly controlled. Such an arrangement can also reduce liability on the part of building owners and managers because building keys that are only needed during a fire are well secured and do not need to be left in the custody of building personnel.

Asset Tracking Systems*

Small asset tags—some being embedded into desktop and laptop computers at the time of manufacture—can be assigned to an asset that is permitted to leave a high-rise building. Integrated with a building's access control system, asset tracking can be utilized to control the movement of primary assets from the building. ''Prime assets tend to be IT [Information Technology] assets because

*According to *SECURITY*, ''The terms 'asset tracking' and 'asset management' are sometimes used interchangeably. But there is a difference. 'Asset management is a larger case statement that begins with pure asset control,' Small [president, Automated Identification Technologies, San Juan Capistrano, CA] says. 'Tracking assets means wanting to know where the asset is and with whom? Asset management really goes beyond that to what comes next in terms of how integrated that data is, and how you manage the database. It starts to be things like how old is the asset? When was it last inventoried? It provides a more rounded perspective than asset tracking' '' (''Asset management, tracking are access issues,'' July 2000, p. 27).

they tend to be portable and have intrinsic high value for themselves and for the information they contain'' (Small, 2000, p. 27).

The following describes an asset tracking/access control system in the lobby of a prominent 39-story Manhattan high-rise office building,

> An access card is assigned to tenants of the facility with normal access levels and work shifts. The card is encoded with the tenant or employee name and other information. Also assigned are small tags for assets permitted to be removed from the building. These asset tags are encoded with a serial number and the owner's name, department, and telephone number.
>
> Initially, all asset tags are assigned a zero access code, with no privilege for egress. When assigned, the tags are programmed into the system along with the cardholder or escort who is permitted to remove the asset from the facility. The loop [radio frequency (RF) signal] readers read card and tag at the same time, and the system checks to see if the two tags have been linked, records the movement and triggers an alarm at the security desk if the removal of property is unauthorized. The name of the person carrying the asset, the serial number of the asset and owner's name and extension appear on the PC screen at the security desk.
>
> All movements through the glass doors [in the main lobby] are recorded on the software system, by time and by employee and asset codes. The CCTV system keeps a visual record that is also date- and time-stamped.
>
> A security or facility manager can also keep track of assets throughout the building's interior. . . . By installing the loops at selected doors, assets can be tracked by department, user's name or asset serial number (''The glass shield,'' February 1998, p. 22).

Such a ''hands-free'' asset tagging and tracking proximity system ''allows free egress when authorized assets are removed, but prevents unauthorized removal of property. Without electronic tracking, assets can be removed by concealing them in a briefcase, package or gym bag'' (Macklowe, February 1998, pp. 21, 22). This system can also be adapted to screen assets being mailed out of a building through a central shipping area such as the loading dock.

Lighting

Lighting serves the purposes of security by acting as a psychological barrier against criminal attacks and, if such an attack should occur, making identification and potential apprehension by security and law enforcement personnel more likely. It likewise serves the purposes of safety by illuminating trip, slip, and fall hazards such as puddles of water, potholes, and difficult-to-see steps. It also serves to make areas more aesthetically pleasing. Security lighting can be used to complement and enhance other security measures such as physical barriers, stationary posts or mobile patrols, CCTV, and intrusion detection systems.

An unusual argument has been used in litigation regarding lighting providing people with a justifiable sense of security. It was brought before the Michigan Supreme Court and concerned the question of whether a property owner, by increasing lighting in a parking area and advertising this fact, was liable in an assault that later occurred in that area (Scott v. Harper Recreation, Inc., No. 92995, reported in the *National Law Journal*, 12/13/93). The assaulted patron sued on the basis that an owner increases the risk of harm by causing area users to be less anxious when property is made visibly safer. The Michigan Supreme Court denied the litigation (*The Merritt Company Bulletin*, 1994, pp. 3, 4).

Factors to Consider

The following factors need to be taken into consideration when selecting an appropriate lighting system:

1. The numbers and positions of light fixtures
2. The direction of light beams (often light will be directed toward walls, barriers, and the building itself)
3. The extent of illumination of particular areas (for example, security-risk locations such as parking areas will often require total rather than partial illumination)
4. The type of lighting sources—incandescent, mercury vapor, metal halide, fluorescent, and high- or low-pressure sodium vapor
5. The type of lighting equipment (continuous lighting is continuously applied to an outside area during periods of darkness; standby lighting is continuous lighting intended for reserve or for standby use, or to augment continuous lighting; portable lighting is movable and manually operated and can be used to augment continuous or standby lighting; and emergency lighting duplicates any or all of the previous three types and generally operates during power failures)
6. The method of activation of the light fixtures (manual, or automatic using a timer or photoelectric cell system)
7. The recommended minimum illumination levels for areas such as pedestrian walkways and building and vehicle entrances as may be required by local ordinances, standards, and practices

For exterior lighting, consideration also must be given to protecting the light fixture from weather and vandalism. When making recommendations regarding lighting, a qualified lighting engineer should be consulted.

General Types of Lighting

The descriptions of the general types of lighting sources that follow were adapted from a chapter, "Security Lighting," in the *Handbook of Loss Prevention and Crime* (Girard, 1989, pp. 281–283).

Incandescent

Incandescent lamps, common, relatively inexpensive, glass light bulbs, become luminous (i.e., emit light) through the action of an electric current on a material called a filament. They produce very good to excellent color rendition (color rendition affects one's ability to discriminate, grade, or select colors and determines whether colors will appear natural), providing warm, white light. They are relatively short in rated life (500–4000 hours) and low in lamp efficiency as compared with other lighting sources. These lights are generally for interior use and have largely been replaced by fluorescent lights in high-rise office buildings.

Mercury Vapor

Mercury vapor lamps emit a purplish-white color because of the action of an electric current passing through a tube of conducting and luminous gas. They are considered more efficient than incandescent lamps of similar wattage, have widespread application for exterior lighting, and produce good color rendition. They are used in approximately 75 percent of street lighting and are commonly used as security lighting in parking lots. They have a long life (more than 24,000 hours) and are used where long burning hours are required. The time needed to light these lamps once they are switched on is considerable. However, once illuminated they can tolerate substantial dips in electrical power.

Metal Halide

Metal halide lamps are similar in physical appearance to mercury vapor but provide a light source of higher luminous efficiency and better color rendition. Therefore, fewer fixtures are required to light the same area as mercury vapor lamps. The rated life (6000 hours) is short when compared with that of mercury vapor lamps. They are used where the burning hours per year are low and color rendition is of utmost importance. As with mercury vapor, the time to light these lamps once they are switched on is considerable. However, once illuminated they can tolerate substantial dips in electrical power.

Fluorescent

Fluorescent lamps, large, elongated bulbs, have a long rated life (9000–17,000 hours), have a high lamp efficiency, and produce good color rendition. They cannot project light over large areas and may have a decreased efficiency at low ambient temperatures. Because of the latter, they have limited value in colder climates for outdoor use. Compared with incandescent lamps, their initial cost is higher, but they have a lower operating cost because they require less electrical power to emit an equivalent amount of light. Fluorescent lights provide ample illumination for safe working conditions. They are commonly used as interior lights in modern high-rise buildings.

High-Pressure Sodium Vapor

High-pressure sodium vapor lamps are discharge lamps that are similar in construction to mercury vapor lamps but emit a golden-white to light pink color. The cost of the light fixture is high, but the cost of operation is low. They have a long life (up to 24,000 hours), produce relatively good color rendition, and are used for the exterior lighting of parking areas, roadways, and buildings.

Low-Pressure Sodium Vapor

Low-pressure sodium vapor lamps are discharge lamps that are similar in operation to mercury vapor lamps but produce very poor color rendition. They emit a light yellow color, and their maintenance of light output is good throughout their rated life. Their expected life is good (up to 20,000 hours), and they operate at a low cost. The cost of the light fixture is equivalent to that of high-pressure sodium vapor lamps. Previously, they were widely used in urban centers. They are now most common on major highways.

Atlas (1993) emphasizes, ''The important thing to remember is to make the light selected best fit the need or purpose. . . . If a parking lot is very large, and many fixtures are required, the priority should be a long lasting bulb with good maintenance (higher mean time between failures) and low replacement costs'' (pp. 6, 7). Also, if the light is to be used for CCTV cameras, the lower the available minimum ambient lighting level is, the more expensive will be the camera required to produce images of reasonable clarity and definition. The extra cost invested in the lighting system can result in an overall reduction of costs because a less expensive camera may be able to be used.

Communication Systems

There are various forms of verbal communication systems available for use in high-rise office buildings and tenant spaces, as described in the following sections.

Telephones

Telephones (fixed position and portable) are an essential communication tool within a high-rise complex. Telephones located in the Security Command Center should be sufficient to handle daily operations plus the extra demands placed on them when building emergencies occur. Important telephone numbers, particularly those of emergency services (fire department, police department, emergency medical services such as paramedics, etc.), may be programmed into many telephone systems for speed dialing. In selecting a telephone system, it is important to consider whether the system can operate in the event of an electrical power failure.

Portable telephones (cellular or mobile) have application in large high-rise complexes because they afford mobility to the user. However, losing telephone connections in under-building parking garages and elevators is a problem. ''Studies show that 51 percent of wireless users experienced dead spots on a regular basis when in commercial office buildings'' (Totum Research, April 2002).

As with most systems, telephones are subject to misuse. The primary misuse is unauthorized calls, including those to pay-per-minute services. Arrangements can be made with the telephone company to screen out and block certain numbers so they cannot be dialed without an authorized code.

Portable Two-Way Radio Systems

Portable two-way radios (sometimes called handheld radios or walkie-talkies) are another essential communication tool within a high-rise complex. All two-way radios have two major components: the transmitter that converts sound waves into inaudible RF energy that is broadcast over the air, and the receiver that converts the inaudible RF energy into sound that can be detected by the human ear. The following information was obtained from the American Protective Services *Tools for Security* training course (1980, p. 1) and Motorola (Worldwide Learning Services, 1994, p. 2).

Transmitter and Receiver

For transmitter control, most radios have a ''Mic Key,'' or ''Press-To-Talk Switch,'' used to turn off the receiver and activate the transmitter. Receiver controls are more diverse. A ''Volume Knob'' is used to adjust the level of sound that is heard but has no effect on the loudness of transmissions. The ''Squelch Knob'' is used to adjust the sensitivity of the receiver to incoming signals and acts like a filter. A common way of adjusting it is to turn it down until a rushing noise is audible and then to turn it up just until the noise stops. The ''PL,'' or ''Private Line Switch,'' is used to limit a signal received to only that from radios that have the same crystal. The ''Channel Selector'' is used to select the frequency the radio will use to transmit and receive the radio frequency energy. In some high-rise buildings, radios with multiple channels are provided—one for the exclusive use of security staff, one for engineering staff, one for janitorial staff, one for parking staff, and one channel designated for use during emergencies only.

Base Station

A base station, located in the Security Command Center or the Building Management Office, should be able to broadcast to all frequencies. The specific controls and their location on the radio will vary from manufacturer to manufacturer, and model to model.

Use of a Repeater

Because of the large amounts of concrete in high-rise structures, it is vital that the radio communication system selected has adequate power and quality to facilitate audible and clear communication to all normally occupied areas of a building. Usually in high-rise buildings, a device called a repeater is added to the radio system to enhance radio coverage. A repeater receives radio transmissions and then retransmits them so that communication is maintained. The repeater consists of several basic components—a receiver, a transmitter, circuitry linking the transmitter and receiver, and either one antenna or two antennas and a duplexer (a duplexer permits a single antenna to transmit and receive at the same time). An antenna is a conductor used for transmitting or receiving electromagnetic radio waves. The repeater usually will have its antenna located on the roof of a high-rise building and will permit inexpensive, low-powered radios to communicate with each other over greater distances.

Pagers

A pager or beeper is a pocket-size electronic device useful for notifying the person carrying it of a telephone message. Notification is by way of a high-pitched audible signal or by vibration. Particularly useful are those pagers that display alphanumeric text messages.

Paging systems can be very effectively integrated with security and fire life safety systems. For example, the access control system at a facility can be set up so that, ''when an alarm comes in, it can be simultaneously sent over pagers carried by security personnel'' (Garbera, 1997, p. 29).

Paging of groups of people can be a very effective means of communication when many individuals need to be simultaneously informed of an event, particularly of an emergency situation.

Personal Data Assistants

Personal data assistants (PDAs) provide a compact, portable means of maintaining and organizing information. The PDA is also becoming a mobile means for monitoring security systems.

Public Address Systems

A public address (PA) system is a one-way system providing a means of communication from the Fire Command Center to the occupants of the building. It should have adequate power and speaker quality so that, in all normally occupied areas of the building (including elevator cars), voice messages can be clearly and distinctly heard. Each PA system is different, depending on the manufacturer and system models. Usually, the system will function with the operator manually selecting the required zones (ordinarily separate paging zones will be designated for each floor and for stairways and elevators) and speaking loudly and clearly into a microphone that connects to these areas. The capability for communication to individual floors or the whole building at once is usually provided.

Megaphones or Bullhorns

Megaphones or bullhorns can be important communication tools, particularly if the public communication system in a high-rise building fails to operate. They can also be of great value in communicating with large groups of people inside, or congregated together outside, the building.

Intercom Systems

An intercom is a two-way communication device enabling communication from the Security Command Center, or other constantly monitored area, to specified locations throughout a building. These locations may include elevators, stairwells (for the use of occupants who are inside the stairwell and need assistance), on the roof at the entrance to stairwells, passenger elevator lobbies, at certain card access points, and various outside locations and parking structures. Intercoms in parking structures are primarily to assist lost persons and those requesting emergency assistance.

Intercoms usually are mounted on walls, columns, or bollards and may be operated by the occupant simply pressing a button and speaking while the button is depressed, or speaking hands-free after the button has been pressed to activate communication. This action will initiate a signal at the monitoring location and should identify the station from which the call originated. If the button is pressed and no answer is received from the originating station, many security operations require staff to be dispatched immediately to that location. The intercoms should be clearly visible, particularly those in parking areas, and should have their number and location distinctly marked on them, along with written instructions as to how to operate them.

Many facilities include phrases such as ''SECURITY ASSISTANCE,'' ''EMERGENCY INTERCOM,'' or ''EMERGENCY CALL STATION'' printed in bold letters on signs at each intercom location. For safety and identification purposes, some intercom systems have distinctive flashing lights that activate at the station that is in use. Others are integrated with the CCTV system so that, on activation of an intercom station, the appropriate camera will be automatically called up for the operator who is monitoring the system.

Speakers and Microphones

A two-way voice communication system from the Security Command Center to speakers and microphones located at sensitive areas, such as stairwells, can be a valuable tool for security. If there is a problem in a remote area, it can be handled by security staff immediately communicating to that location. Used in conjunction with CCTV, speakers and microphones* can become an effective part of the total security system. If, for example, security staff observes a crime in progress while monitoring camera images, they can use the speaker system to communicate to that area and possibly thwart the crime. This combination of CCTV and speaker systems has been very effective in exterior parking areas where potential car thieves have been successfully warned off before they have had the opportunity to carry out their intentions.

In addition to these communication systems, there may be fire department voice communication systems.

It is of critical importance that all essential communication systems are provided with backup power to ensure their continued operation during an electrical power failure.

Closed-Circuit Television Systems

CCTV, sometimes called closed-circuit video, involves the transmission of scenes or moving pictures by conversion of light rays to electronic signals,

*The use of microphones and listening devices is prohibited in some jurisdictions.

which are transmitted via coaxial cable, fiberoptic cable, twisted pair wire (hence the terminology ''closed-circuit''), or infrared beams, microwave, radio waves, satellite, and/or a host of other methods to specific receiving equipment such as a video display monitor, or a video-recording device.

CCTV recording systems are used extensively for surveillance in high-rise buildings. The primary purpose of a CCTV system is to enhance existing security measures and amplify the range of observation of security staff. To improve security, it may be useful to interface the CCTV system with intercoms and intrusion detection devices such as magnetic door contacts, motion detectors, or video motion detectors. The primary purpose of the video-recording system is to record the picture from a camera and provide a permanent record for possible later review. As with other security systems and equipment, such as physical barriers, locking systems, and lighting and intrusion detection systems, CCTV is part of the basic security measures that make up the total security program.

In addressing CCTV systems, it is important to realize that presently there are two types of CCTV—analog and digital—that are available. Analog (the older video format) is rapidly being replaced by digital (the new video format). This section will touch upon both these technologies, but is not intended to be an in-depth treatise.

Area Observed and Ambient Lighting Levels

Illumination is a critical factor in the quality of the CCTV picture. For exterior- and interior-mounted cameras, it is essential that adequate levels of useful light be available (whether it be sunlight, moonlight, starlight, or an artificial source of illumination such as mercury, fluorescent, sodium, metal-arc, tungsten, or other lamps). For nighttime viewing, infrared lighting may be more cost effective than traditional security lighting. For all cameras it is essential that not only adequate levels of useful light be available, but also that the light be compatible with the type of image sensor contained in the camera.

Camera and Lens

The camera is the device that facilitates the conversion of the image, produced by the lens, to an electronic signal for transmission via coaxial cable, fiber optic cable, or other means to the remote video monitor and/or video recording device. The functions of the lens are to collect the light from the area being observed and to form an image of the scene on the imager contained within the camera (i.e., the lens focuses light onto a chip or tube within the camera). Lenses come in different sizes that allow choices for the area view. Each lens has a specified focal length (FL). FL is ''the distance from the lens center, or second principal plane to a location (plane) in space where the image of a distant scene or object is focused. FL is expressed in millimeters or inches'' (Kruegle, 1995, p. 435). For use in remote control applications, fixed FL lenses are usually obtainable in an auto or motorized iris form. By varying the diameter of the aperture, the iris controls the amount of light reaching the image sensor.

Types of Lenses

The various types of lenses available are as follows:

1. Standard, wide-angle, and telephoto lenses are lenses with a fixed focal length. A standard lens produces an image that is the same as what the eye sees at the same distance; a wide-angle lens is designed to view a wide area up close; and a telephoto lens is designed to view distant areas and produce images larger than what the naked eye sees.
2. A zoom lens has a variable focal length. It can be manually operated or motorized and can be used as a standard, wide-angle, or telephoto lens. ''A motorized zoom lens (in the CCTV industry) is distinguished by it's full ratio of zoom from wide angle to telephoto . . . usually in a 10 to 1 (10:1) or higher format. Additionally, the zoom and focus functions are physically connected so that a zoom lens may be focused in the full telephoto mode and then 'zoomed out' to the wide-angle view while maintaining perfect focus'' (Pierce, April 2002).
3. ''A vari-focal lens is a form of limited zoom lens. Usually in a manual format, the vari-focal lens has a limited zoom ratio of usually less than 2:1 . . . i.e. 8.5 mm – 12.5 mm. Additionally, the vari-focal lens has no physical attachment between the zoom and focus functions and so requires refocusing each time the scene perspective is changed'' (Pierce, April 2002).
4. A split lens or bifocal lens is a system consisting of two separate lenses that view two scenes with identical or different magnifications and then combines them on the camera imager.
5. A pinhole lens and a right angle lens can be used for covert surveillance purposes. The pinhole lens can be used with the camera mounted behind a wall and the lens viewing through a small hole in the wall. The lens is designed to produce an image with a wide-angle field of view (i.e., the angle of view encompasses the width and height of the scene being monitored). The right angle lens can be used with the camera mounted inside a thin wall or above the ceiling.

An essential key in properly designing any CCTV system is to select the most appropriate lens for the application at hand. Doing so maximizes the value of the resultant video images.

Analog and Digital Cameras

Analog systems use chip cameras—also called charge-coupled device (CCD) cameras—that were introduced in the early 1980s and caused tube cameras to become effectively obsolete for security applications (POA, 2000, pp. 38-1A, 38-14) by the late 1990s. CCD cameras ''are integrated circuit devices that utilize an array of solid state, light sensitive elements (picture elements or pixels) arranged on a silicon chip to sense light passed from the scene through the lens. The pixels, the smallest sensing elements in the sensor, are arrayed in horizontal rows and vertical columns of varying size'' (POA, 2000, p. 38-14). As Pierce (1989, pp. 71, 72) writes,

> The strongest advantages of chip cameras are that they require less energy and take up less space (because of the lack of high-voltage image tubes), require less maintenance (average image chip life expectancy is five years, compared to the

> average image tube life of one to two years), and are more flexible, coming with more standard features than tube cameras ... Vidicon [tube] cameras have a high propensity to burn or retain images, meaning the pickup tube shows the scene it has been staring at even after the lens is capped. ... Chip cameras, on the other hand, cannot burn or retain images, and are even warranted against such problems.

Digital systems use CCD and complementary metal oxide semiconductor (CMOS) cameras. CCD cameras require a digital signal processor to change the signal from analog to digital, whereas CMOS cameras always transmit digital signals (Gips, April 2001, pp. 78, 79). ''For now, CCD is the camera of choice in digital systems. But some engineers and consultants predict that CCDs will be challenged by CMOS technology, in part because it is much cheaper to manufacture than CCD cameras'' (Gips, April 2001, p. 79).

Monochrome (black and white) cameras have been largely replaced by color cameras, except for a few specialist applications* (POA, 2000, p. 38-1A). ''Color offers valuable additional information on the objects being monitored. More importantly, the human eye captures color information quicker than the fine details of an object. The drawback is not so good performance in low light levels'' (Damjanvoski, 2000, p. 21). As buildings upgrade their camera systems, color is increasingly becoming the camera of choice.

Camera Mounting and Housing

A camera can be mounted in several ways: on a support bracket; recessed into a ceiling or wall; or housed in a dome, a box, or a custom-shaped protective container made of metal or strong plastic material (housings can be high-impact and vandal-resistant, and even ballistic-rated). In interior locations such as reception areas, the camera housing needs to be inconspicuous and fit in with the décor of the facility. Some housing can even be designed to look like track lighting.

The electrical power supply to a camera should not be a simple plug-in, as is often the case, but should have the greater degree of security afforded by hard wiring extending from the camera into conduit,† plastic channels, or directly into the wall. The camera should be mounted so that it is out of the normal reach of people and cannot be approached without the person doing so being in the field of view of the camera. If it is not mounted at a sufficient height, the camera may be sabotaged by a person who reaches the camera and either pulls the plug or cuts the power supply or covers the camera lens with an object to obstruct its view.

---

*''While the performance of color cameras for outdoor applications in artificial light is still inferior to monochrome, most indoor applications, particularly when identification and recognition of people are the primary purpose, benefit considerably from the use of color'' (POA Publishing, 2000, p. 38-15).

†''All conduit should be securely fastened to walls or ceilings with no openings or compartments between the two ends. If a separate connection or junction box needs to be added, then security measures should be taken to prevent access to that box. One method would be to use nonconventional screw heads that require special tools to remove. All conduit used for security wiring should be dedicated only to security. No other type of wiring should be allowed to run through the same tubing'' (Beaudry and Brandt, 1998, p. 75).

Exterior-mounted cameras, in particular, need to be protected with a heavy-duty housing against weather, vandalism, and intentional interference with a camera to make it inoperative. An environmental housing can provide protection against wind, snow, rain, moisture, dirt, or, in some cases, explosions. Sometimes, the housing is equipped with a windshield wiper and heater.

Dummy Cameras

In the past, some buildings, particularly in areas such as parking garages and lots, used dummy cameras. A dummy camera looked like a camera but was not one. It consisted of an opaque camera housing with an apparent power supply connected to it. It may have contained a camera but was not hooked up to any monitor or did not contain a camera at all. The use of such devices can provide people with a ''false sense of security'' because they believe they are in an area monitored by personnel or recorded by a CCTV system. In the case of a security-related incident, such as robbery or assault, the presence of such devices can result in liability exposure for the owner or manager of the facility.

Camera Pan, Tilt, and Zoom Capabilities

Pan or pan/tilt mechanisms are peripheral devices that allow the camera or the housing to move along a horizontal plane (pan) or vertical plane (tilt). Pan moves the camera mounted to it from side to side. Pan/tilt moves the camera mounted to it from side to side and up and down. These mechanisms can be designed to operate automatically or manually. A controller is a device that controls the pan, pan/tilt, and/or automatic lens functions. Controller types include a zoom lens controller; a pan or pan/tilt controller; or an operations controller, which is a combination of the first two in a single unit.

Most pan, tilt, and zoom (PTZ) cameras are now housed in domes. As Damjanoviski (2000, pp. 281, 283) writes,

> They are usually enclosed in a transparent or semitransparent dome, so they make an acceptable appearance in aesthetically demanding interiors or exterior. . . . Transparent domes usually have an inner mask, with an optical slot in front of the lens, while the rest of the mask is a non-transparent black plastic. By keeping the interior dark (black zoom lenses and camera bodies), they offer a very discrete and concealed surveillance. Very often it is impossible to judge where the camera is pointing, which is one of the very important features of dome cameras. Tinted domes usually have no mask and so the whole dome is transparent but tinted. . . . Almost all PTZ domes of the newer design have preset positioning.

Preset positioning causes a camera to automatically turn in a particular direction, zooming in and focusing on a particular area. For example, a particularly sensitive door can be equipped with a magnetic contact. When the door is opened ''we can force the camera to automatically turn in that direction, zooming and focusing on the previously stored view of the door'' (Damjanoviski, 2000, pp. 282, 283).

Closed-Circuit Transmission

The most common systems for transmission of the closed-circuit video signal, whether from a digital or analog camera, are coaxial cable or fiber optic (also called optical fiber) cable. The CCTV camera manufacturer generally specifies the maximum distance between the camera and the monitor over which the CCTV will perform efficiently. Coaxial cable remains the typical method for transmission over distances up to 2500 feet, without the need for amplification of the video signal (Pierce, April 2002). ''The actual distance depends on the type of coaxial cable used'' (POA, 2000, p. 38-30). It is ordinarily reliable and often the up-front lowest-cost method.

If there are difficulties with the installation of coaxial cable, the video signal can be transmitted via several other different transmission means: fiber-optic, two-wire, wireless, infrared, microwave, radio frequency, and satellite. ''Fiber-optic cable is gaining acceptance because of its better picture quality (particularly with color) and lower risk factor with respect to ground loops and electrical interference'' (Kruegle, 1995, p. 183).

Remote Transmission

There is a growing demand for remote monitoring and playback capability of CCTV cameras. For example, a security director responsible for multiple buildings may be notified of a serious incident that is occurring, or has occurred, at one of the facilities. The ability to use a home or office computer or wireless technology (such as a cellular telephone or PDA) to remotely access the building's CCTV system to view live video or a recording of the incident would be very useful. The means of video transmission will largely determine the quality of the video. Such means may include a local area network (LAN), a wide area network (WAN), the Internet, or wireless methods.

Video Monitor

The video monitor displays the image obtained from the camera. The image can be shown in black and white (B/W) or color depending on the camera and monitor equipment. As mentioned previously, color has become increasingly popular, particularly where enhanced imaging is vital to the scene being viewed. In certain applications, particularly identification, it is far better to have the camera image displayed in color. For example, a camera may be located in a dark-colored floor area that is being viewed to monitor property removal. If a person carrying property close to her or his body is wearing dark-colored clothing and walks across the area, the property itself may not be discernible on a B/W monitor. However, the same image displayed in color may clearly display the property being removed.

Before proceeding, it is appropriate to address a common belief—that CCTV video monitors are nothing more than overpriced television sets. ''The video monitor is designed to work with the industrial closed-circuit video system, and will outlast—and out-perform—the consumer television at a lower overall cost, provided that it is installed in a proper environment''

(Pierce, 1993, pp. 29–32). Pierce further elaborates, ''The average television is designed to operate eight hours a day for five years. The monitor is designed to run continuously for 24 hours per day for five years.'' In other words, the actual life of the CCTV video monitor is three times that of the consumer television. Pierce (1993, pp. 29–32) also states that the life of the monitor is reduced if the environment includes the following:

1. Dust levels are high (dust gets inside the monitor and leads to heat buildup and premature breakdown of the solid state electronics).
2. Papers are stacked on top of and around the monitor (not permitting proper dissipation of heat and thereby resulting in premature failure of the cathode ray tube).
3. Brightness and contrast controls are turned to the maximum.

Controls

The controls on the monitor are similar to domestic television sets, with power on and off, contrast, brightness, horizontal, and vertical hold (and color controls, if the monitor is color).

Size

Video monitors can be procured with diagonal screen size of 5, 7, 9, 14, 17, 19, 21, or 23 inches, with the most common being 9 inches. Kruegle (1995, p. 189) gives several reasons for the popularity of the 9-inch screen:

> 1. The 9-inch diagonal screen provides the highest resolution from the monitor.
> 2. Using a 9-inch monitor, the optimum viewing distance of the operator from the monitor is approximately 3 feet, a convenient distance in many security console rooms.
> 3. The 9-inch monitor size is such that two 9-inch monitors fit side-by-side in the standard EIA [Electronic Industries Association] rack configuration. This is an important consideration, since space is generally at a premium in the security console room and optimum integration and placement of the monitors is important.

On-Screen Displays

Several types of displays and on-screen character generation can be used to assist the performance of an operator viewing a monitor. Displays using graphic floor plans and maps with flashing, colored icons symbolizing event locations and definitive text can be used to decrease the operator's response time and increase adherence to, for example, established procedures for responding to alarms.

On-screen character generation varies from camera system to camera system. It may show the camera number, camera title (brief description of camera location), date, and time. Also, if alarms are part of the CCTV system, it may show the alarm status of each camera being displayed at that time. The date and time information is generated either by an exterior unit or the camera microprocessor unit. The unit producing this information should have battery backup to accommodate limited power failures.

Mounting

Monitors may be tabletop or rack mounted depending on the number being viewed. "There have been several studies of operator effectiveness regarding the most effective angle of the monitors to the operator. Design the console or viewing area in such a way that the monitors that will be viewed by the operator will be aimed straight at wherever the operator is sitting" (Pierce, 1993, pp. 29–32). Figure 5.31 displays a two-guard security console configuration.

Rack mounting, particularly where large numbers of monitors are involved, permits the monitors to be mounted in a functional way that takes into account the camera scenes that are being monitored. For example, if there are a series of cameras in a corridor, the monitors displaying those images should be programmed together in a horizontal or vertical pattern where one monitored scene leads immediately to the adjacent monitored scene. Other examples in the high-rise setting may be a series of cameras monitoring the loading dock area, various levels of the parking structure, building lobbies, elevator cars, or ground floor exits from building stairwells. Rack mounting also saves space and the clutter that ensues when multiple monitors are mounted on a tabletop.

Operator Viewing Effectiveness

Before proceeding, it is appropriate to mention a problem that occurs with monitoring large numbers of cameras. There does come a point when the person cannot keep pace with the demands of the viewing operation. "There have been several studies of operator effectiveness regarding the number of monitors an operator can watch. Effectively the average person cannot watch more than four pictures simultaneously with any comprehension of what is happening" (Pierce, 1993, pp. 29–32). The operator will view multiple monitors by repeatedly scanning back and forth across them. To monitor effectively, additional operators may need to be added. However, because of the financial impact such a move would have, this issue is often not addressed. As a result,

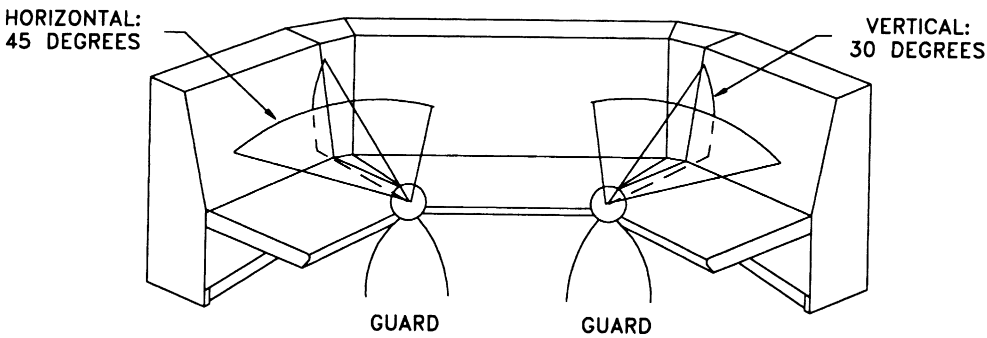


Figure 5.31 A two-operator security console configuration. Courtesy of Herman Kruegle, *CCTV Surveillance: Video Practices and Technology* (Butterworth–Heinemann, Boston, 1995), p. 188.

the effectiveness of the security operation suffers and the operators themselves are subjected to stress and fatigue. ''To combat this problem, CCTV systems should be designed to be as ''hands free'' or automated as possible. This provides the operator the ability to respond to the situation versus watching the screen and concentrating on the controls'' (Pierce, April 2002).

Video switching (see next section) amplifies a person's ability to view multiple video cameras. Using a split screen arrangement, 2, 4, 9, 16, or 32 scenes can be simultaneously displayed on a single monitor. The problem with this technique is that the resolution of the scenes is decreased proportionately and it becomes more difficult for the operator to distinguish what is being viewed.

Another possible solution to monitoring large CCTV installations is to continuously display a few cameras that have security importance, continuously record all cameras, and automatically call up cameras on alarm (using alarm devices such as a magnetic door contact, a motion detector, or video motion detection).

An important factor in the monitoring of CCTV systems is the total time an operator is able to stay alert and work effectively while viewing single or multiple monitors. The studies mentioned earlier have addressed this vital, but often neglected, factor. ''After approximately one hour (less time for people of below average intelligence) the average operator's mind has mentally shut off the monitor to the point that an object or objects of identifiable size can be moved into and consequently through the scene at a rate of six inches per minute'' (Pierce, 1993, pp. 29–32). One obvious solution to this problem is to rotate the video operators. However, in many high-rise building operations, training multiple operators and frequently rotating them may not be a viable option because of the limited size of the staff. Where little change is occurring, providing color monitors and alarm interfacing can assist to break the monotony of monochrome images. The more that is happening, the more likely it is that the operator will stay active and alert and be more effective in monitoring the CCTV system.

Video Switchers

The simplest CCTV system involves a single camera with its image displayed on a single video monitor. Larger high-rises often have an extensive camera system covering multiple locations within the building, with camera images being displayed on multiple monitors. A person viewing the monitors is restricted because he or she can comfortably view only a certain number of monitors at any given time.

Video switchers are devices that allow multiple cameras to be monitored on a single monitor or multiple monitors, either in sequence or one at a time. ''Video switchers enhance a video system, allowing it to save costs while remaining effective through multiple camera monitoring through a single source of view'' (Pierce, 1995, p. 1.4). There are various types of manually and automatically operated video switchers. ''Manual switchers, sequential switchers, and alarming switchers have been replaced by various multiplexers, matrix switchers, and the newer digital control/manipulation systems. They are still in use but are of no consequence to modern design'' (Pierce, April 2002).

Matrix Switcher

Large high-rise buildings may contain vast numbers of CCTV cameras and large numbers of monitors that require monitoring (this is also true in multi-building complexes where multiple security systems are being monitored in a centralized location). As POA (2000, p. 38-56) puts it,

> Matrix switching uses microcomputer control circuits and permits the display of any camera view on any monitor. Available systems can include hundreds of cameras and scores of monitors. The camera views are inputs to the central processor that can match camera view to monitor manually via an operator keyboard, automatically through video motion detection* or alarm activation [by a magnetic door contact or a motion detector], or in accordance with programmed sequence patterns via the keyboard and CPU [central processing unit] or developed off-line and loaded into the CPU.

Multiplexer

A multiplexer is a powerful, high-speed video switcher that has largely replaced the aforementioned switchers (Pierce, 2002). It is a device that can input the video signals from monochrome or color cameras (up to 16 cameras), and produce two kinds of video outputs: one for displaying on a video monitor and one for recording on a video recorder. ''The multiplexer operates by selecting a frame from each camera in sequence, digitizing it, and displaying it in a predefined location on the [video monitor] screen'' (POA, 2000, p. 38-57) and/or sending it to the recorder.

Multiplex Video Recording

A problem in reviewing VHS tape recordings was when multiple camera images were sequentially displayed on a single monitor and then recorded on the VCR. When the video was played back, the images from all the cameras were sequentially displayed. The frequent image switching made it very difficult for the reviewer to follow clearly what was occurring on any one particular camera. The situation was chaotic when up to 16 camera images were being viewed. This difficulty has been removed by multiplex video recording. As explained by POA (2000, pp. 38-66, 38-67),

> A major advance in video recording has been the development of multiplex recording which digitizes the camera input, processes or enhances the signal in various ways and then records it in real-time or time lapse. Multiplexing allows multiple cameras (up to 16 at present) to be recorded on a single recorder (DVRs, typically have built-in multiplexers). Instead of switching from camera to camera to select the image, the multiplexer merely selects or ''grabs'' a frame from each

*Video motion detection allows a CCTV camera to be used as an alarm device. ''A video motion detector (VMD) is a device that analyzes the video signal at its input and determines whether its contents have changed and consequently, produces an alarm output'' (Damjanoviski, 2000, p. 190). ''For each camera involved, a detection pattern is selected and stored in the processor. The detection pattern may be all or some of the camera image. Video Motion Detection is only used with fixed position and fixed focus cameras'' (POA Publishing, 2000, p. 38-61).

> camera in series, processes or enhances the signal and passes it to the recorder, until all cameras have been selected. It then starts the cycle over again. . . . When grabbing frames the multiplexer electronically identifies each with its source camera. When the tape is played back, utilizing the multiplex unit as a playback control, only the successive images from the selected camera are displayed. The net effect is as though the tape was made from a single camera.

Because there is a small time lapse between camera images, when the tape is played back motion may appear slightly ''jumpy.'' Despite this, the quality of the tape is acceptable for most applications in the high-rise setting.

Video Recording and Storage

A video-recording device records camera images. These images can be used to examine past incidents, for investigations, as evidence in civil litigation or criminal actions (although the admissibility of digital recordings in judicial proceedings has still to be determined), and to defend against insurance claims.

Video recording can be in either real time or time lapse mode. (Real time means that all images the camera captures are recorded; time lapse means that the images are recorded intermittently.) ''The prime reason for including time-lapse capability in the CCTV recorder is to conserve the storage medium'' (POA, 2000, p. 38-63).

Previously in the security field, reel-to-reel videotape recorders were the standard type of recorder, followed by videocassette recorders (VCRs) and then digital video recorders (DVRs). VCRs generally use ½-inch VHS tape cassettes; DVRs can use digital videotape, DAT (digital audiotape), compact discs (CDs), or hard drive disks as the storage medium.

Digital Video Recorders

Digital video recorders (DVRs) offer a number of advantages over VCRs. For an existing analog system, DVRs can provide digital recording and playback capabilities. DVRs have ''the ability to record and play back video from the same storage space at the same time . . . DVRs differ in terms of disk space, resolution, compression, frame rates, motion detection, archiving ability, searchability/retrieval, playback, image authentication, and operating systems. Advances are being made in all these areas'' (Gips, 2001, p. 82). As stated by CCTV expert Herman Kruegle (''DVRS still the talk of the town,'' 2001, p. 32),

> Both magnetic and optical disk systems have an advantage over VCRs with respect to storage and retrieval time of a particular video frame, which leads to the advantages of using a digital recording system. The biggest return on investment is the amount of time saved while investigating a particular event. The other benefits include:
>
> - Fast retrieval, transport and enhancement of images
> - Storage capacity

- Able to record multiple times without image degradation

To increase storage capacity, hard drives are often used simultaneously. For long-term storage, images are archived and stored on a removable memory device.

With regard to the amount of time saved while investigating a particular event, rather than manually winding and rewinding through endless videotape, ''to review recorded images, users simply type into a PC keyboard the time and date the images were recorded; the computer calls them up instantly'' (Partington, 1999, p. 21). Also, when required, digital images of a particular image can be easily printed out.

In large high-rise complexes deploying huge numbers of cameras, digital video recording means that the archiving and storage of vast numbers of videotapes is now no longer a necessity.

Rapid Technological Change

In the past decade, an incredibly rapid change in the technology that supports CCTV systems has occurred. CCTV specialists, consultants, manufacturers, dealers, and suppliers can be an invaluable source of information for determining what state-of-the-art systems and equipment are available in this ever-changing field. However, one needs to be aware that advice may be given with the specific intention of promoting one particular product or system. Charlie Pierce, a leading authority on CCTV, advises to, ''Design the application first and fit the equipment to it'' (Gips, 2001, p. 82).

Camera Applications

CCTV can enhance the security provided of the building perimeter, the building, public access or common areas, maintenance spaces, and tenant areas. Entrances, exits, corridors, elevators and elevator lobbies, parking garages, and other sensitive areas can be monitored and kept under surveillance. CCTV cameras are recommended for the following locations in a high-rise office facility:

- *Access points where occupants enter on foot.* All building entrances, particularly when an entrance door is remotely controlled. With the latter application, it is vital that persons be viewed on camera to determine whether they are to be granted access. If the door is equipped with an electronic card reader, a camera is useful to view when tailgating or piggybacking occurs.
- *Crucial entry and exit points within the building.* These include cross-over floors between elevator banks (for example, cross-over floors between the passenger elevators that serve the building tower and the passenger elevators that serve an under-building parking garage, or between low- and mid-rise elevator banks, or between the mid- and high-rise elevator banks), strategic locations on mechanical floors or floors that have restricted access, and critical reception areas.

- *Access points for vehicles to parking garages.* If a vehicle gate or traffic arm is remotely controlled, it is vital that vehicles, and possibly drivers, be viewed on camera to determine if they are to be given access. Many high-rise parking structures—particularly under-building garages—have cameras installed at all ingress/egress points that, in conjunction with a video-recording device, record the license plates of all vehicles entering and exiting the property, as well as close-up images of the drivers.
- *Crucial egress points such as ground floor exits from building stairwells.* A camera in conjunction with a video motion detector can, when movement is detected in the stairwell, draw the operator's attention and trip a video-recorder to record the images in real time. This can be an invaluable tool for detecting unauthorized removal of property from a building via the stairwell. The provision of a two-way voice communications system with a speaker and microphone (prohibited in some jurisdictions) at the camera location can be effective for communications between the Security Command Center and these areas.
- *Sensitive areas.* These include the building perimeter; neighboring streets; parking garages; passenger and service/freight elevator lobbies; stairwell exits to the building roof; dumpster and trash compactor areas; openings to outdoor air intakes and ducts for HVAC systems and air handling units; entrances to main utility areas such as the power transformer room and central plant; and high-value item storage areas, including safe and vault areas. Again, use of video motion detection can be used to warn the operator of movement within a certain area.
- *Inside passenger and service/freight elevator cars.* Cameras within elevator cars can be an effective deterrent to threats against persons (such as lewd behavior, assault, robbery) and threats against property (such as vandalism of the elevator car). With vandalism, particularly graffiti, if no action is taken against this type of activity, it tends to escalate. A possible solution for deterring or identifying the persons responsible for graffiti is to install a CCTV camera, either openly or covertly, in the affected elevator car.
- *Locations where covert surveillance is required.* A concealed camera can be a tremendously important tool for observing activities, particularly illegal ones such as theft. A hidden camera can be used to observe events where it would be impossible to conceal a person. Modern technology has led to a reduction in the size of surveillance equipment and to aids such as pinhole devices. Cameras are available that can be ingeniously concealed in emergency lighting systems, in emergency exit signs, behind clocks, behind works of art, behind one-way mirrors, in ceiling-mounted sprinkler heads, in portable radios, in air fresheners, in hollowed-out books, and in other items openly displayed in the office setting. In conjunction with a video-recording device, concealed cameras can be used to view areas for extended periods and provide a permanent record of the taped events. In some applications, the portable unit of CCTV and VCR/DVR may need to be equipped with a self-contained power source—for example, on top of elevator cars where the camera, equipped with a pinhole lens, and the VCR/DVR may be installed as a self-contained unit. Note that such installations must always be carried out in conjunction with a certified elevator technician.

Of course, not all public access or common areas may be monitored by any CCTV system, covert or not. Usage is not permitted in restrooms and locker rooms, or in any other areas where users have a reasonable expectation of privacy. The question of whether employers can use CCTV cameras and other surveillance equipment for security purposes continues to be the subject of legislation.

The actual design, configuration, and location of any CCTV system in a high-rise building will depend largely on the security and life safety needs of the building or the specific areas being monitored.

Intrusion Detection Systems

There are various types of intrusion detection systems (IDSs) available to enhance the quality of security provided for the building perimeter, public access or common areas, maintenance spaces, and tenant areas.

The purpose of an intrusion detection system is to detect when an unauthorized intrusion has occurred in an area and to transmit an alarm signal. (A signal may also be sent when the person setting an alarm system fails to do so correctly or inputs a predetermined code that indicates he or she is under duress and needs assistance.) The signal may be transmitted to sound a local alarm—a bell, horn, siren, whooper, etc.—at or near the protected area. It may be transmitted to an on-site monitoring location staffed with operators trained to carry out a predetermined alarm response procedure, or to an off-site central station likewise staffed with personnel trained to notify the appropriate agencies.

On-Site Monitoring

In the high-rise building, the on-site monitoring location may be the local annunciator and control panels built into an open-style desk arrangement, or the more complex and sophisticated Security Command Center, both of which usually will be located in the main lobby. In the case of on-site monitoring, when an intrusion alarm is activated, security staff will either investigate the reason for the alarm themselves or notify the appropriate law enforcement agencies. If the intrusion alarm involves a tenant space, a prearranged tenant notification procedure should be carried out.

Off-Site Monitoring

In the case of off-site monitoring, once the central station staff are notified of an intrusion alarm, they will either notify security staff at the building, dispatch a responding agent such as a patrol officer, or notify the appropriate law enforcement agency and request a response to investigate the reason for the alarm. In addition, the central station staff may also directly notify building management or a tenant representative if the incident involves a tenant area. The specific response procedures will be preplanned and should be in writing or stored on a computer.

Intrusion Detection Components

An intrusion detection system consists of three basic components: a sensor, a control unit, and an annunciation device.*

Sensors

Sensors are installed in the area being protected and are designed to detect intrusion. The types of sensors that may be found in high-rise buildings are described in the following sections.

Pressure Mat or Pad Detector
Pressure mat or pad detectors are, in effect, simple switches that either react to pressure when it is applied to them, or react when normally applied pressure is released. They may be in the form of a strip or a mat. In some locations—for example, inside tenant offices—they may be secreted under carpeting with the associated electrical wiring concealed from view.

Magnetic Contact Switch
Magnetic contact switches are reliable, simple devices that consist of a permanent magnet attached to a door (and in some applications, to a window), and a magnetically operated switch attached to the frame. The magnet may be surface-mounted and visible, or flush-mounted and concealed. The switch operates by means of a magnetic field generated when the door is closed. If the door is opened, the magnetic field is interrupted and an alarm is initiated. Magnetic contact switches are effective devices but bridging or jumping the circuit can defeat surface-mounted ones. These switches are commonly used in high-rise buildings for exterior doors (particularly stairwell exterior fire doors), interior doors (particularly stairwell doors and doors leading to maintenance spaces), and interior doors leading to offices and sensitive areas within tenant spaces. These devices are useful for monitoring intrusions into building stairwells.

Electrical Switch
Electrical switches are installed in a similar fashion to magnetic contact switches. However, in this case, they consist of electrical contacts. They operate on the principle that an electrical circuit is completed when the door is closed and the contacts come together. If the door is opened, the electrical current is interrupted and an alarm is initiated. As with magnetic contacts, electrical switches can be defeated by bridging or jumping the circuit.

Break-Wire System
Very fine, electrically conductive wire configured in the form of a screen or a crisscross arrangement across an opening can be used to detect intrusion. When the wire is broken, the electrical circuit is severed and an alarm is initiated. Such an arrangement can be useful in protecting building exterior openings such as those leading to HVAC air intakes. The wiring system also

*The information in the following sections was compiled with the assistance of ''Intrusion Alarms: Sensing Principles'' (Purpura, 1991).

can be modified, using magnetic contact switches to detect movement of the wiring assembly without the wire actually breaking. Accordingly, an alarm will be initiated to notify security personnel of the intrusion.

Vibration Detector

A vibration detector uses microphones to detect audio noise. The sensitivity of the detector can be adjusted to initiate an alarm when it detects vibrations such as those resulting from forced entry. It can be installed on surfaces—walls, ceilings, floors, and doors—and objects such as works of art, files, safes, cabinets, and vaults. Although vibrations of the building and equipment contained within it can lead to false alarms, by adjusting the sensitivity of the vibration detector system these false alarms can be reduced.

Capacitance Detector

Capacitance detectors operate using an electromagnetic ''barrier.'' On application of a small electrical charge to a metal object, an invisible electromagnetic field is set up around the object such as a file, safe, cabinet, or vault. If something intrudes into the field, an alarm will be initiated. When this device is in use, it is vital to properly ground the object being protected.

Passive Infrared Detector

Instead of emitting a signal or field that can be disturbed by an intruder, passive infrared (PIR) devices are passive or inert and operate on the principle that human beings emit heat, in the form of infrared radiation, from their bodies. When an intruder moves within the range of the detector, an alarm is triggered by the very small, but detectable, variations in heat caused by the intruder's presence.

The proper location of the passive infrared detector is critical because false alarms can be caused by sunlight and HVAC systems. In high-rise buildings, PIR detectors are also commonly used as automatic door openers, particularly in heavily traveled public access or common areas such as building lobbies.

Ultrasonic Motion Detector

Ultrasonic motion detectors operate on the principle that a space can be filled with inaudible sound waves. Using a transmitter, the device both sends and receives ultrasonic waves. If an intruder enters the protected space, the standing-wave pattern is disturbed and an alarm is initiated. Ultrasonic motion detectors can false alarm because HVAC systems discharge air into the protected space. In addition, noises (such as telephones ringing) within or outside the protected area can cause false alarms by disturbing the wave patterns.

Microwave Motion Detector

Microwave motion detectors have an operating principle similar to ultrasonic motion detectors, with the exception that high-frequency electromagnetic microwaves are transmitted into an area. If an intruder enters the protected space, the standing-wave pattern is disturbed and an alarm is initiated. Because microwaves can penetrate building walls they may be used to detect movement outside of areas where the device is operating, but this feature can also lead to movements being detected that are not of consequence to the space being protected. Some tuning devices can circumvent these problems by restricting the area covered by the detector. Electric motors, fluorescent lights, or other devices that interfere with the detector by emitting electromagnetic waves can cause false alarms.

Video Motion Detector

Video motion detection allows a CCTV camera to be used as an alarm device. The underlying principle of operation is that the contrast change in a specific area of the image causes an alarm output. If motion occurs and the particular scene changes, the sensing device will initiate an alarm to draw the viewer's attention to this fact, or will switch on a video-recording device to record the activity. ''A video motion detector (VMD) is a device that analyzes the video signal at its input and determines whether its contents have changed and consequently, produces an alarm output'' (Damjanovoski, 2000, p. 190).

Acoustic Detector

Acoustic detectors use a very sensitive and accurate hi-fi microphone to detect noise created by an intruder attempting to gain entry to a particular area or moving within the protected space. Their use is usually restricted to vaults and other high-security applications.

Photoelectric Detector

When an invisible beam of light projected from the transmitter of a photoelectric detector to its receiver is interrupted, an alarm is initiated. Various patterns of the photoelectric beam can be devised, and mirrors can be used to deflect the beam around corners. An obvious method an intruder can use to circumvent the system is to climb over the beam or crawl under it. Photoelectric detectors tend to be more commonly used in outdoor applications.

Control Unit

The sensors are linked, usually electrically, to the control unit. The control unit normally will consist of circuitry installed in a metal enclosure. The cover of the unit often contains a key-operated switch that permits one to alter the signal(s) sent to the annunciation device and deactivate the sensor, thus permitting access to the protected area without an alarm signal being activated. A standby battery source normally will be provided to furnish power in case the primary electrical power source fails. Also, a tamper switch usually will be provided so that if the unit is interfered with, a signal is sent to the annunciation device.

Annunciation Device

On activation of a sensor, a signal will be sent to the control unit, which in turn will transmit a signal to sound a local, audible alarm (such as a bell, horn, or siren) at or near the protected area; transmit a signal to an on-site monitoring location; or transmit to an off-site central station. A combination of these signals is also possible.

Often in high-rise office buildings, tenants will have their own intrusion detection systems, separate from the building's systems. Usually off-site central stations monitor tenant systems. Sometimes, building owners and managers are approached to monitor tenant alarm systems within the building. This is not recommended. It can lead to many operational problems associated with the alarm response itself and can result in substantial liability exposure for the building.

Duress Alarm Switches and Kick Bars

Duress alarm switches and kick bars are simple, electrical switches manually operated by people to summon assistance. They may be mounted underneath or on the side of a desk or counter, or on the floor. The assistance may be requested for security reasons such as when the person feels threatened, is under attack, or has just been attacked or for safety reasons such as a medical emergency. The switches operate through an electric current continuously running through a circuit. When the duress alarm (or sometimes called *panic alarm*) switch is activated, the current stops, resulting in the initiation of an alarm at a remote location. The remote location may be another area within the facility, the Security Command Center, an off-site central station, or some other location that is constantly monitored when the switch is operational.

In the security application, it is generally considered safer to transmit a signal that does not sound a local alarm (such as a bell, horn, or whooper) at or near the protected area. Sudden noise around a person committing a robbery, for example, may lead that individual to react violently.

As with all security systems and equipment, the operation of duress alarms should be regularly tested and this activity documented. Duress alarms are particularly important because their activation usually indicates an emergency situation. It is critical that they operate as designed. Their construction should always include protective guards or other design features to avoid accidental activation.

Security Mirrors

Although not security equipment, per se, a convex mirror is a reflecting device commonly found in parking garages and other areas where there are ''blind corners.'' Such a device extends the range of observation of a person looking into the mirror so that they can see around a corner and observe oncoming people or vehicles.

Metal Detectors and X-Ray Systems

Metal detectors and x-ray systems, although not commonly used in high-rise office buildings, are deployed in sensitive facilities such as high profile building complexes, signature buildings, courts and other government facilities, and for special events requiring screening, mainly for weapons. ‘‘Metal detectors [or magnetometers] work by generating an electromagnetic field and then measuring changes in that field caused by the presence of metal objects. Newer metal detectors can direct operators to the area of the body where a gun or knife might be hidden’’ (Alonso-Zaldivar, 2002, p. A20). (Since the September 11, 2001, terrorist attacks on the New York World Trade Center, these devices have received considerable attention as a screening measure for guns, knives, and explosives concealed on people and contained in parcels, packages, carried possessions, and in vehicles.[*])

The type of tenancy and pattern of use of the building will largely determine whether such security measures are appropriate. For example, the 25-story high New York Municipal Building in Manhattan houses 5000 employees, including prominent city officials and city agencies. Due to the threat of violence,

> Visitors entering the main lobby of the building must pass through a Metorex walk-through metal detector that incorporates LEDs [light-emitting devices on the side of the device or on a separate panel] that indicate an area of a person’s body that may conceal a weapon. ‘‘The use of the walk-through has minimized the use of metal detecting wands because they can pinpoint an area in question. Now, wands are used only to confirm the presence of metal,’’ says director of security, James J. Darmos. Items carried by visitors are put through Heimann Systems High Scan x-ray equipment. X-ray machines are also used in the mailroom. The machines can zoom in on an object within a package and exhibit densities in black-and-white and color.’’ (Garbera, 1999, p. 26)

An added layer of protection is to combine a metal detector with an access control system. According to Scott Dennison, director of CEIA USA, ‘‘This allows for metal detection and hands free access control in a single unit, enabling the user to have an extremely high flow rate while dealing with the threat of workplace violence,’’ (‘‘Metal detectors meet multiple need,’’ December 2000, p. 27). ‘‘We’ve developed a technology that will read an access control card as the person is walking through the metal detector,’’ he says, ‘‘It verifies that not only does the person not have a weapon, but they are also authorized to be in that facility’’ (‘‘Metal detectors add shapes, sizes, features and functions,’’ August 1998, p. 26).

In planning the installation of metal detectors and x-ray machines it is important to analyze traffic patterns and select equipment that can accommodate the expected traffic and avoid compromising the security objectives or creating traffic jams. According to Scott Dennison (1998, p. 38),

> Security should begin by calculating the number of persons expected to enter during each half-hour increment and reviewing the type of personal articles that entrants will bring with them. Then, security should determine how many metal detectors and x-ray machines will be required to handle this traffic flow, factoring in a cushion of about 25 percent. (The processing rate of a single-lane, walk-through metal detector and x-ray machine ranges from 300 to 600 persons per hour.)

[*] *MobileSearch*™ is a noninvasive inspection system that involves the use of an x-ray source mounted in a truck. It can be used to x-ray vehicles, including large trucks. Such a device can be very effective in screening for explosives and weapons prior to a vehicle being permitted entry to an under-building parking garage.

> The number of metal detectors and x-ray machines should be based on the estimated flow rate of entrants and the established acceptable waiting time.
>
> The correct number of security screening personnel required to operate the equipment can be ascertained at this point. [A walk-through metal detector and x-ray machine requires four-persons: one for the metal detector, one for the x-ray machine, one to carry out inspections with a hand-held wand, and one to carry out physical bag inspections, when required.] It is also important to develop a floor plan that accommodates entrants who will need a place to line up for processing.

Training and periodic checks of the efficiency of the screening personnel in detecting certain objects are critical. ''Detection equipment is only as good as the employees who operate it. Personnel must be trained properly, and equipment stations must be staffed with sufficient personnel. Poor training or understaffing will undermine the effectiveness of the screening process'' (Dennison, 1998, p. 43).

Security Monitoring Center

The focal point for an entire building's security operations may be local annunciator and control panels built into an open-style desk arrangement or a complex and sophisticated Security Command Center. In either case, their design should configure the security systems and equipment in a user-friendly manner that takes into consideration the operator's intelligence and educational level. The systems should be readily accessible to the operator and positioned in such a way that monitoring does not contribute to operator stress and fatigue. The design should bear in mind the comfort of the operators who will be spending considerable time performing routine and, at times, monotonous tasks within its confines. It is essential that adequate ventilation, heating, and air conditioning be provided for the area.

The organization and appearance of the open-style desk arrangement or the Security Command Center often will reflect the building's commitment to security. If the area is attractive and well laid out; if equipment is up-to-date, well maintained, and sufficient for the needs of the security staff to carry out their duties and responsibilities; and if the work surface of the operators is clean and free of clutter, then there is a fair indication that building security is taken seriously and that the program is being professionally managed.

If the Security Command Center is located in a separate room, it should be of adequate size to accommodate the operation and future expansion needs. It should be highly secure, with access doors to it kept locked at all times. Interior windows should be constructed using burglar-resistant (and possibly bullet-resistant) glass, and windows facing the exterior of the building should be kept to a minimum. Other security elements to be considered include providing dip trays, if a window that is accessible to the public exists. A dip tray is a small opening at the base of a window through which keys, access cards and other small items can be passed. Also, high-security doors should have peepholes and possibly mantraps. Some buildings, for security purposes, prefer to house the Security Command Center in a windowless room so that an outsider is not even aware of its presence.

Summary

The security systems and equipment of high-rise buildings vary according to the specific needs of each facility. An individual building will utilize a combination of barriers, locks, asset tracking, lighting, communication, closed-circuit television, intrusion detection systems, and other security devices integrated into a total security system designed to meet the protection requirements of that particular site.

References

Aggleton, David G., ''Integrating access control systems with badging,'' *Protection of Assets Manual.* Timothy L. Williams, Editor (POA Publishing, LLC, Los Angeles, February 1997), Bulletin.

Alonso-Zaldivar, Ricardo, ''Metal detectors will take center stage in new era'' (*The Times Mirror Company,* Los Angeles, June 14, 2002).

''Asset management, tracking are access issues'' (*SECURITY,* Highlands Ranch, CO, July 2000).

Atlas, Randall I., ''Security design: designing fire exits,'' Bulletin, *Protection of Assets Manual,* 9th printing. Timothy L. Williams, editor (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, July 1993).

Atlas, Randall I., ''Security design: lighting for security,'' *Protection of Assets Manual,* 9th printing. Timothy L. Williams, editor (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, October 1993).

Beaudry, Mark H., and H. Skip Brandt, ''Suite security'' (*Security Management,* Arlington, VA, January 1998).

Bowers, Dan M., *Access Control and Personal Identification Systems* (Butterworths, Stoneham, MA, 1988).

Cumming, Neil, *Security: A Guide to Security System Design and Equipment Selection and Installation,* 2nd ed. (Butterworth–Heinemann, Stoneham, MA, 1992).

Damjanovoski, Vlado, *CCTV* (Butterworth–Heinemann, Woburn, MA, 2000).

Delta Scientific Corporation, Delta TW Barricades and ''A discussion of the background, operation, selection and installation of a vehicle arrest system,'' (Delta Scientific Corporation; Valencia, CA; Lorton, VA, available at http://www.deltascientific.com, 2002).

Dennison, Scott, ''Developing the right sensitivity to weapons'' (*Security Management,* Arlington, VA, August 1998).

Donoghue, Edward A., ''Building transportation systems,'' *Fire Protection Handbook,* 18th ed. Arthur E. Cote, Editor-in-Chief (National Fire Protection Association, Quincy, MA, 1997).

''DVRS still the talk of the town'' (*SECURITY*, Highlands Ranch, CO, May 2001). Text adapted from *CCTV Surveillance: Video Practices and Technology* by Herman Kruegle (Butterworth–Heinemann, Boston, MA, 1995).

Edgar, James M., and William D. McInerney, ''The use of locks in physical crime prevention,'' *Handbook of Loss Prevention and Crime Prevention,* 2nd ed. Lawrence J. Fennelly, editor (Butterworth–Heinemann, Stoneham, MA, 1989).

Finneran, Eugene D., *Security Supervision: A Handbook for Supervisors and Managers* (Butterworths, Stoneham, MA, 1981).

Fischer, Robert J., and Gion Green, *Introduction to Security* (Butterworth–Heinemann, Boston, 1998).
Garbera, Don, ''Critical security operation at inner-city hospital doesn't skip a beat,'' comments by John Nicoletti, North Central Bronx Hospital, director of security (November 1997), ''New York City's Municipal Building secures against clear and imminent danger'' (*Access Control & Security Systems* magazine, Atlanta, June 1999).
Geringer, Richard G., ''High-rises look to lock out problems,'' (*Access Control* magazine, Atlanta, June 1991).
Gigliotti, Richard, and Ronald Jason, ''Physical barriers,'' *Handbook of Loss Prevention and Crime Prevention,* 2nd ed. Lawrence J. Fennelly, Editor (Butterworth–Heinemann, Stoneham, MA, 1989). Adapted from Gigliotti, Richard, Ronald Jason, *Security Design for Maximum Protection* (Butterworths, Stoneham, MA, 1984).
Gips, Michael A., ''Let's get digital'' (*Security Management,* Arlington, VA, April 2001).
Gips, Michael A., ''The name's the game'' (*Security Management,* Arlington, VA, September 1999).
Girard, Charles M., ''Security lighting,'' *Handbook of Loss Prevention and Crime Prevention,* 2nd ed. Lawrence J. Fennelly, editor (Butterworth–Heinemann, Stoneham, MA, 1989). Adapted in part from *An Introduction to the Principles and Practices of Crime Prevention* by Koepsell Girard and Associates, Inc., and *Principles and Practices of Crime Prevention for Police Officers* (Texas Crime Prevention Institute, San Marcos, TX).
''The glass shield'' (*Access Control & Security Systems* magazine, Atlanta, February 1998).
Goldfeld, Doron, ''Badging technology offering new options,'' (*Access Control* magazine, Atlanta, December 1994).
Harwood, Emily M., ''The smart card: it's not just for physical security,'' (*Security Technology & Design*, Cumming, GA, February 1999).
Hinman, Eve E., ''Lessons from ground zero,'' (*Security Management,* Arlington, VA, October 1995, copyright 1995 Failure Analysis Associates, Inc.).
InstaKey: *Re-Key Your Own Lock in Seconds* and conversations with Scott Serani and Harvey Hlista (Englewood, CO, 1995).
Knox System, *A Guide to Professional Rapid Entry* (The Knox Company, Newport Beach, CA, 1991).
Kruegle, Herman, *CCTV Surveillance: Video Practices and Technology* (Butterworth–Heinemann, Boston, 1995)
Macklowe, Harry, comments in ''The glass shield'' (*Access Control & Security Systems* magazine, Atlanta, February 1998).
''Metal detectors add shapes, sizes, features and functions'' (*SECURITY,* Highlands Ranch, CO, August 1998). Comments by Scott Dennison, director, Ceia USA, Twinsburg, Ohio.
''Metal detectors meet multiple need'' (*Access Control & Security Systems* magazine, Atlanta, GA, December 2000). Comments by Scott Dennison, director, Ceia USA, Twinsburg, Ohio.
MobileSearch™ (Information obtained at a demonstration of the American Science and Engineering [AS&E] MobileSearch system, Billerica, MA, www.as-e.com, June 2002).
National Crime Prevention Institute, *Understanding Crime Prevention* (Butterworth-Heinemann, Stoneham, MA, 1986), as quoted in Ed San Luis, Louis Tyska, and Lawrence J. Fennelly, *Office and Office Building Security,* 2nd ed. (Butterworth–Heinemann, Boston, 1994, p. 30).
New Webster Encyclopedic Dictionary of the English Language, 1980 Edition, Virginia S. Thatcher, Editor-in-Chief (Consolidated Book Publishers, Chicago, 1980).
NFPA 101, *Life Safety Code* (National Fire Protection Association, Quincy, MA, copyright 2000).

O'Leary, Tim, ''Security gates, turnstiles & portals'' (*Security Technology & Design,* Cumming, GA, February 1998).
O'Mara, Deborah L., ''A cure for terrorism blues,'' (*SECURITY,* Highlands Ranch, CO, October 2000).
Partington, George, ''Digital video system eases the burdens of surveillance,'' (*Access Control & Security Systems* magazine, Atlanta, July 1999).
Pierce, Charlie R., ''CCTV: kiss and choose'' (Copyright LTC Training Center, *Security Management,* Arlington, VA, November 1989).
Pierce, Charlie R.,''CCTV: monitor overview'' (*Access Control* magazine Atlanta, June 1993).
Pierce, Charlie R., ''CCTV: video theory.'' Paper presented to the International Security Conference (ISC), Anaheim, CA (LTC Training Center, Davenport, IA, February 1995).
Pierce, Charlie R., comments made in review of section, ''Closed-circuit television systems'' (April 2002).
POA, ''Television in security,'' *Protection of Assets Manual,* Vol. IV. Timothy L. Williams, editor (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887, copyright 2000).
Post, Richard S., and Arthur A. Kingsbury, ''What is security?'' *Security Administration: An Introduction to the Protective Services,* 4th ed. (Butterworth–Heinemann, Boston, 1991).
Purpura, P. P., *Security and Loss Prevention,* 2nd ed. (Butterworth–Heinemann, Boston, 1991), ''Intrusion Alarms: Sensing Principles'' as it appeared in *Encyclopedia of Security Management* by John Fay (Butterworth–Heinemann, Stoneham, MA, 1993), pp. 432–433.
Reese, Shelly, ''Decisions, decisions,'' comments by Don Belles, a consulting fire protection engineer with Koffel Associates, Inc. (*NFPA Journal,* National Fire Protection Association, Quincy, MA, November/December 1998).
Schum, John L., ''The load,'' *Electronic Locking Devices* (Butterworths, Stoneham, MA, 1988).
Security Door Controls, *SDC Exit Check* (Security Door Controls, Westlake Village, CA, 1995).
Small, Don, president, Automated Identification Technologies, San Juan Capistrano, CA, commenting in ''Asset management, tracking are access issues'' (*SECURITY,* Highlands Ranch, CO, July 2000).
Smith, Darrel L., ''Window film: the most cost-effective means to protect existing windows,'' (*Security Technology & Design,* Cumming, GA, June 1999).
Tawa, Renee, ''Barricades cover their muscle with warmth, style'' (*Los Angeles Times,* The Times Mirror Company, Los Angeles, November 8, 2001).
The Merritt Company, ''Added lighting does not increase liability,'' Bulletin, *Protection of Assets Manual* (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, February 1994).
Tools for Security: Two-Way Portable Radios (American Protective Services, Inc., Oakland, CA, 1980).
Totum Research, as reported in ''Tired of cell phone dead zones? Consider in-building wireless systems'' (BOMA.org, Washington. D.C., April 2002).
True, Tim, ''Raising the ramparts,'' (*Security Management,* Arlington, VA, October 1996).
''Window film protects Wells Fargo Center during 2000 DNC'' (*SECURITY,* Highlands Ranch, CO, December 2000).
Worldwide Learning Services, *Motorola Radius GR300 and GR500 Reference Guide* (Motorola, Schaumburg, IL, 1994).

Additional Reading

Damjanovoski, Vlado, *CCTV* (Butterworth–Heinemann, Woburn, MA, 2000).
Dennison, Scott, ''Developing the right sensitivity to weapons'' (*Security Management,* Arlington, VA, August 1998). Guidelines for selecting and installing metal detectors and x-ray machines.
Garcia, Mary Lynn, *The Design and Evaluation of Physical Protection Systems* (Butterworth-Heinemann, Woburn, MA, 2001).
''The glass shield'' (*Access Control & Security Systems* magazine, Atlanta, February 1998). Description of an asset tracking/access control system installation.
Gips, Michael A., ''Let's get digital'' (*Security Management,* Arlington, VA, April 2001).
Kruegle, Herman, *CCTV Surveillance: Video Practices and Technology* (Butterworth–Heinemann, Boston, 1995).
O'Leary, Tim, ''Security gates, turnstiles and portals,'' (*Security Technology & Design,* Cumming, GA, February 1998). Article on security revolving doors and turnstiles.
Pierce, Charlie R., *Interactive CCTV Training System* (LTC Training Center, Davenport, IA, http://www.ltctrainingcntr.com).
Pierce, Charlie R., *Professionals Guide to CCTV* (LTC Training Center, Davenport, IA).
POA, ''Television in security,'' *Protection of Assets Manual,* vol. IV (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Copyright 2000).
True, Tim, ''Raising the ramparts,'' (*Security Management,* Arlington, VA, October 1996). A comprehensive review of security barriers.

Additional Resources

Access Control & Security Systems Buyers Guide (*Access Control & Security Systems* Technology magazine, Atlanta, available at http://www.securitysolutions.com.
ASIS International Glossary of Terms (ASIS International O.P. Norton Information Resources Center, available at http://www.asisonline.org/irc.html).
ASIS *Security Industry Buyers Guide* (American Society for Industrial Security, 1625 Prince Street, Alexandria, VA 22314, available at http://www.securityindustrybuyersguide.com).
SECURITY For Buyers of Products, Systems and Services Buyer's Guide (*SECURITY,* Highlands Ranch, CO, available at http://www.securitymagazine.com).

This Page Intentionally Left Blank

6 *Fire Life Safety Systems and Equipment*

In high-rise office buildings, there are many types of fire life safety systems and equipment that can be deployed as potential solutions to specific vulnerabilities. Their primary purpose is to help ensure that a building is safe to use, that occupants are able to escape safely and quickly in the event of a fire or other emergency, and that appropriate control measures are rapidly initiated.

This chapter outlines the systems and equipment that may be found in a typical modern high-rise office building. This outline is generic in nature. Because of the number of different model codes and standards, it does not focus on the statutory requirements of any one code or standard; however, extensive reference is made to National Fire Protection Association (NFPA*) National Fire Codes®. To determine what is actually required at a specific site, one must review the laws, codes, and standards that have been specifically adopted by the authority having jurisdiction.

Monitoring of Fire Life Safety Systems

The focal point for the fire life safety operations and communications network of an entire building may be either a simple local annunciator and control panel, or a more complex and sophisticated *Fire Command Center,* both of which may be located in the main floor lobby. The latter may be called the Fire Control Room, the Central Control Station, the Command Center, the Control Center, the Fire Command Station, or the Fire Control Center (Figure 6.1). In the event of a fire, the fire department will usually designate this area as its command post. If the Fire Command Center is located in a separate room, it should be identified as such by a conspicuous sign on its door. (Some authorities discourage this for security reasons—in that case, the local fire department must be consulted and a nonpublic identifier established.) The door should be kept locked at all times. The Fire Command Center (or the local annunciator and control panel) will usually be located near or adjacent to the main entrance to the building; the fire authority that has jurisdiction will oversee its actual location and accessibility.

*All NFPA information in this chapter is used with permission from the National Fire Protection Association, Quincy, MA, Copyright 1997.

Figure 6.1 Example of a Fire Control Center. Photograph by Roger Flores.

The Fire Command Center is separated from the remainder of the building by fire-resistive construction, with all openings protected by assemblies with a fire-resistive rating specified by the local authority having jurisdiction. The Fire Command Center should not be used for any other purpose than that for which it is designed. It usually will contain the following as a minimum:

- Voice communication and building public address (PA) system
- Fire department voice communication systems
- Public telephone for fire department use
- Stairwell intercom systems
- Fire detection and alarm system annunciator and control panels
- Sprinkler control valve, water-flow detector, and fire pump status panels
- Other fire protection equipment and system annunciator or status indicators
- Air-handling system controls and status indicators
- Elevator status panel displaying elevator operations
- Emergency and standby power systems status indicators
- Controls for simultaneously unlocking stairwell doors locked from stairwell side

- Building and elevator keys
- A copy of the Building Emergency Procedures Manual (as described in Chapter 11)
- A computer terminal and printer, which are often provided for the fire life safety systems

All fire life safety systems should be Underwriters Laboratories, Inc. (UL), FM Global,* Wernock Hersey International (WHI), or Electronic Testing Labs (ETL) listed as having met minimum standards.

Voice Communication and Building Public Address System

The voice communication and building PA system is a one-way system providing a means of communication from the Fire Command Center to the occupants of the building. It should have adequate power and speaker quality so that audio messages can be clearly and distinctly heard in all normally occupied areas of the building (including elevator cars and stairwells).

Each system is different depending on the manufacturer and system models. Usually, the operator manually selects the required zones (ordinarily separate paging zones will be designated for each floor and for stairwells and elevators) and speaks loudly and clearly into a microphone that connects to those areas (Figure 6.2).

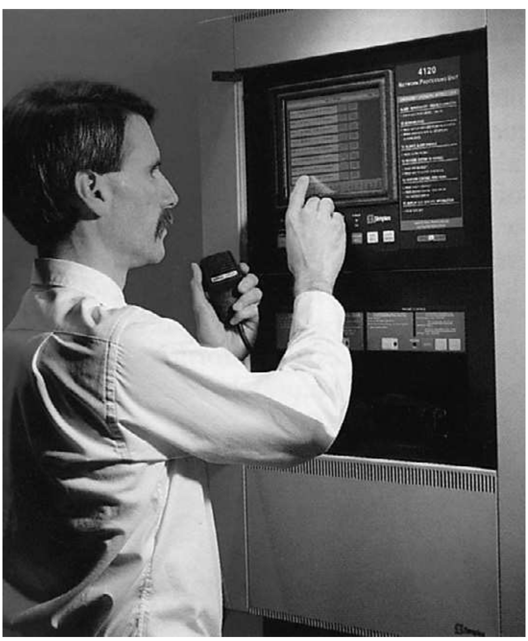


Figure 6.2 A Building Fire Safety Director identifies the type of fire detection device in alarm and its location before making a public address announcement to the occupants of a modern high-rise building. Courtesy of SimplexGrinnell, A Tyco Company.

*Formerly called Factory Mutual.

The system almost always allows communication to individual floors or the whole building at once. (This feature has sometimes led to problems in buildings. By mistake, operators have activated the ''ALL CALL'' feature of the panel, thereby causing the audible fire signal to sound on all floors. To reduce the chance of accidentally activating this feature, some buildings, with the approval of the local fire authority having jurisdiction, install a molded polycarbonate cover over the ALL CALL button or switch. This cover is hinged to the panel, and if the ALL CALL feature needs to be used, the operator swings the cover open to access the appropriate button or switch.) Systems usually are designed so that the sounding of a fire alarm signal in any particular area or floor will not prevent voice communication to other floors or areas; also, when the voice communication system is selected for a zone in which a fire alarm is already sounding, the audible alarm will automatically discontinue when the microphone is activated for the operator to speak.

Fire Department Voice Communication Systems

This emergency communication system is provided for fire department use. It enables two-way telephone communication between the Fire Command Center and specified locations throughout the building where telephone jacks (Figure 6.3) or handsets are installed. These locations include entries to stairwells on each floor, standby and emergency electrical power rooms,

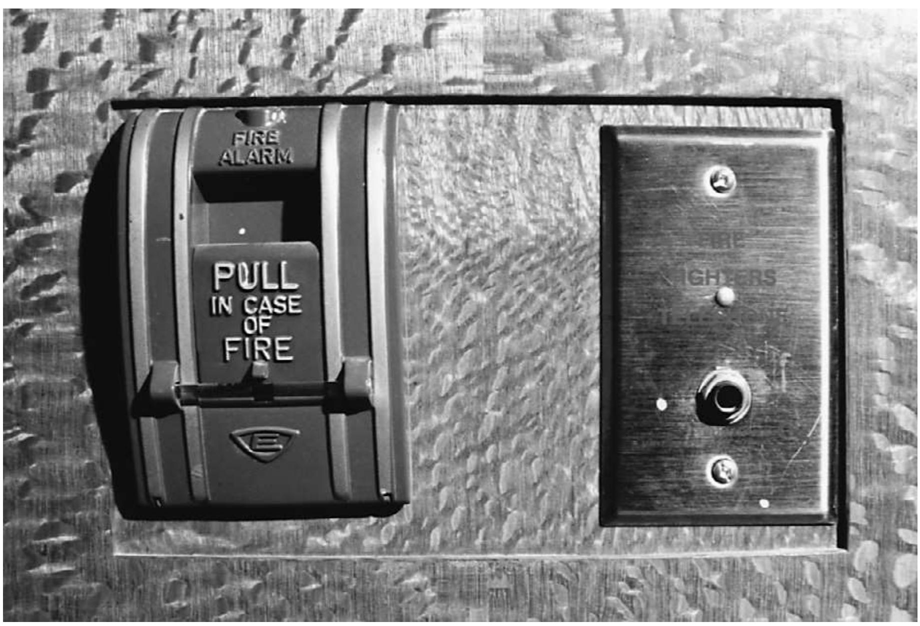


Figure 6.3 Example of a manual fire alarm station on the left-hand side and a fire department voice communication system jack on the right-hand side. Photograph by Roger Flores.

elevator cars, elevator machine rooms, and passenger and service/freight elevator lobbies. In Los Angeles, for example, the systems permit simultaneous voice communication between six locations. If telephone jacks rather than fixed handsets are installed, the handheld telephone sets normally will be kept in the Fire Command Center, one being permanently installed with a cord of sufficient length to reach all areas of the Fire Command Center. Some authorities having jurisdiction permit the use of an approved fire department radio communication system operable to all locations within the structure.

Public Telephone for Fire Department Use

A public telephone designated for fire department use allows controlled access to the public telephone system. Its call back number should be clearly marked on the handset. Often this telephone is red to indicate that it is to be used for emergency purposes only.

Stairwell Intercom Systems

An intercom is a two-way device enabling communication between the Fire Command Center, or other constantly monitored location, and other specified locations throughout the building. From a life safety standpoint, intercoms are often installed in stairwells for the use of occupants who are inside the stairwell and need assistance. They are usually mounted on the wall just inside the stairwell entrance and operated by pressing a button and speaking while the button is depressed.

The intercom should have its floor number and location marked on it, along with written instructions on how to operate it. Some jurisdictions require that older high-rise buildings that do not have stairwell door automatic unlocking systems that activate (i.e., unlock the stairwell doors) when a fire alarm occurs provide two-way intercoms inside the stairwells at every fifth floor. This is to ensure that any occupant trapped inside the stairwell would have a means of communicating with building staff to notify them of their situation. Someone could then come and open a stairwell door near the location, thus eliminating the need for the occupant to walk all the way down the stairwell to exit the building.

Fire Detection and Alarm System Annunciator and Control Panels

Annunciator and control panels monitor and control the fire detection and fire alarm system devices located throughout the building. According to Wilson* (1997, p. 5-5),

*This quote has been slightly modified. The original reads ''a secondary, or standby, power supply.'' Also, ''sirens and whoopers'' has been added.

> Fire alarm systems are classified according to the functions they are expected to perform . . . . The basic features of each system are:
>
> 1. A system control unit.
> 2. A primary, or main, power supply.
> 3. A secondary power supply.
> 4. One or more initiating device circuits or signaling line circuits to which manual fire alarm boxes, sprinkler waterflow alarm initiating devices, automatic fire detectors, and other fire alarm initiating devices are connected.
> 5. One or more fire alarm notification appliance circuits to which audible and visible fire alarm notification appliances, such as bells, horns, [sirens and whoopers,] stroboscopic lamps, and speakers, are connected.
> 6. Many systems also have an off-premises connection to a central station, proprietary supervising station, remote supervising station, or public fire service communication center by means of an auxiliary fire alarm system.

The secondary supply is an emergency power system from which power is automatically transferred. Examples of emergency power supplies include a storage battery or group of batteries, a generator driven by a fuel-supplied prime mover, or an *uninterruptible power supply* (UPS); also, there may be other means authorized by the authority having jurisdiction. (Emergency power systems will be discussed later in this chapter.) The secondary power supply may also energize trouble signals in the fire detection and fire alarm system. A trouble signal initiated by the system will occur due to either a problem with the fire protective signaling system equipment itself (such as a device or the wiring associated with the system) or the failure of the system's primary power supply.

According to Bryan (1982, p. 320), ''The primary purpose of a fire detection system is to respond to a fire, and to transform this response into a visual-audible signal which should alert the building's occupants and the fire department that a fire has been initiated. The fire detection system is intended to respond to the initial signs, signals, or stimuli which indicates that a fire has begun.'' When a fire detection device is activated, a signal immediately will be sent to the Fire Command Center. The signal may also be sent to the Security Command Center, depending on the on-site monitoring arrangements, or to an off-site central station.

In some modern high-rises, alarm signals are graphically displayed on a video monitor with operator input using touchscreen, mouse, or keyboard commands. (One state-of-the-art fire detection system has a display screen located on the fire annunciator panel itself.) Screen information, such as floor plans and graphic maps with flashing icons symbolizing event locations, fire safety symbols, and programmable step-by-step emergency instructions, can be customized for a specific building. Using graphic systems can help train operators quickly and thoroughly, decrease an operator's response time, and increase adherence to established alarm response procedures.

The annunciator and control panels that monitor and control the fire protection systems will take various forms depending on the designer and manufacturer of the equipment, and on the requirements of the authority having jurisdiction.

Manual Fire Alarm Stations

Manual fire alarm stations (i.e., manually activated fire alarm stations) are sometimes called *manual fire alarm boxes, manual pull stations*, or *manual pull alarms*. According to the NFPA 101, *Life Safety Code* (2000), this manual fire alarm box

> shall be provided in the natural exit access path near each required exit from an area, unless modified by another section of this *Code* [9.6.2.3] .... Additional manual fire alarm boxes shall be located so that, from any part of the building, no horizontal distance on the same floor exceeding 200 feet (60 m.) shall be traversed to reach a manual fire alarm box [9.6.2.4] .... Each manual fire alarm box on a system shall be accessible, unobstructed, and visible [9.6.2.6].

However, according to Bill Webb, Chief Engineer of Rolf Jensen and Associates, some authorities discourage or prohibit the use of manual fire alarm stations (Webb, 1994).

In a typical modern high-rise, manual fire alarm stations [see Figure 6.3] will be mounted on walls located in the common area corridors adjacent to the stairwells, in passenger and service/freight elevator lobbies, and at the roof adjacent to the exterior door of each stairwell.

Sequence of Operations

A manual fire alarm station may be activated by depressing, lifting, or pulling a lever or switch or by breaking a thin glass plate and pulling a lever or switch. In modern high-rise buildings, this usually will cause the following sequence of operations:

- An audible and (as recently required by the Americans with Disabilities Act for new or modified construction) a visual signal—usually a strobe (flashing lights)—on the floor on which it is initiated (in some high-rises a signal will simultaneously occur on the floor where the alarm initiated, on one or two floors above this floor, and on one or two floors below this floor) (Figure 6.4)
- An audible and visual signal at an off-site central monitoring station
- A live voice or prerecorded evacuation or relocation message to the occupants (some fire departments do not allow an automatically activated prerecorded message, as it may not be appropriate for every alarm situation)
- Shutdown of the air-handling—heating, ventilating, and air-conditioning (HVAC)—system on the floor in alarm, and in other areas as designated by the system
- Activation of the smoke control system on the floor in alarm
- Activation of building stairwell and elevator shaft pressurization fans

Figure 6.4 Example of an audiovisual signaling strobe to notify occupants of an alarm condition on their floor. Courtesy of System Sensor, St. Charles, IL.

- Release of hold-open devices for doors (usually elevator lobby doors) on the floor in alarm
- Release of all stairwell door locks in the building

Municipal Fire Alarm Box

Some municipalities provide a means for an alarm to be manually sent directly to the local public fire service from a municipal fire alarm box (street box) housed in an enclosure in the street outside of the building. Many city fire departments eliminated these boxes due to persons transmitting alarms when no fire conditions existed. The need for these public reporting stations has been largely eliminated throughout the United States by the widespread use of ''911'' emergency telephone services.

Automatic Detection Systems

As Bryan states, ''The automatic fire detector is designed to respond and transmit a signal via a pneumatic, electric, hydraulic, or mechanical communications system. The automatic fire detector is programmed to respond when the appropriate physical-chemical condition exceeds certain response thresholds'' (Bryan, 1982, p. 320). A variety of detectors exist to sense the presence of smoke, heat, flame, and gas. The selection of the appropriate detector will depend on factors such as the type of combustion or gaseous build-up that may be anticipated, intended location and purpose of the detector, architectural configuration, and the presence of air currents caused by the HVAC systems.

The selection, installation, and maintenance of the appropriate detector are all critical factors in avoiding false alarms. A *false alarm* occurs when a detector indicates that there is a fire but in reality there is none. Causes of false alarms include a lack of detector maintenance, short-term electrical interference in the communications systems sending the signal back to the Fire Command Center (such interference typically can be addressed by initiating an alarm verification feature), and—to a much lesser degree—faults in the detector itself. A false alarm also may be caused by conditions that appear to indicate a fire but actually are caused by the occupants themselves, such as an occupant smoking a pipe, cigar, or cigarette and blowing the smoke toward a smoke detector. Very closely aligned in meaning to a false alarm is a nuisance alarm. A *nuisance alarm* is ''any alarm caused by mechanical failure, malfunction, improper installation, or lack of proper maintenance, or any alarm activated by a cause that cannot be determined'' (NFPA *Glossary of Terms*, 2001).

Smoke Detectors

Smoke is often the first sign that a fire is occurring; therefore, an automatic detection system based on smoke detectors is a valuable tool in the early detection of fire. ''Smoke is defined here as the total airborne effluent from heating or burning a material'' (Clarke, 1997, p. 4-8). Smoke detectors are commonly classified by their mode of operation.

Ionization Smoke Detector

Ionization smoke detectors (Figure 6.5) use a radioactive material to convert the air contained within an ionization chamber into positive and negative charges. This allows the air to conduct a certain amount of electrical current. When

Figure 6.5 An ionization smoke detector. Courtesy of System Sensor.

smoke particles are present in the chamber, they attach themselves to the ions and cause the air to become less conductive. The detector initiates an alarm when the conductivity of the air falls below a certain predetermined level (Figure 6.6).

Photoelectric Smoke Detector

Photoelectric smoke detectors (Figure 6.7) use light to detect visible smoke particles produced by burning material. They are designed to detect smoke when it either obscures a light beam (thereby reducing the amount of light received by a photosensitive device) (Figure 6.8) or it scatters a light beam (thereby causing the light to fall on a photosensitive device that would not receive light when smoke was not present) (Figure 6.9). When this occurs, the detector initiates an alarm.

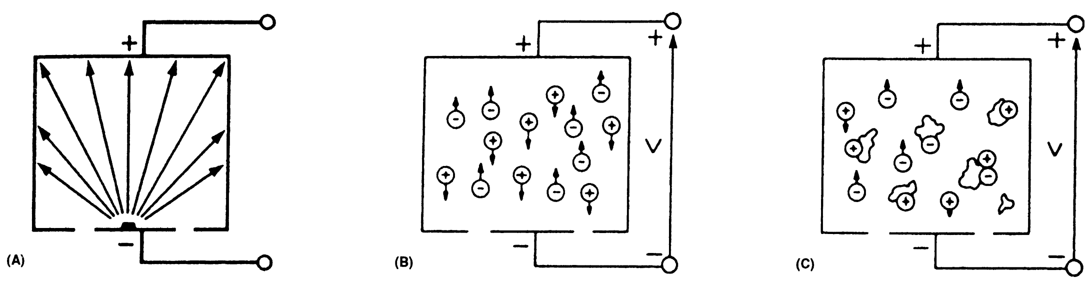


Figure 6.6 Diagrams of how an ionization smoke detector works. (A) Particle radiation pattern. (B) Ion distribution. (C) Ion and smoke distribution. Courtesy of System Sensor: *Guide for Proper Use of System Smoke Detectors.*

Figure 6.7 A photoelectric smoke detector. Courtesy of System Sensor.

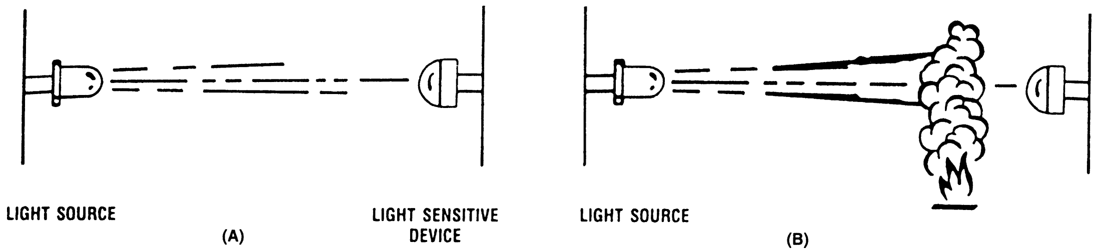


Figure 6.8 Diagrams of how a photoelectric light obscuration smoke detector works. (A) Light obscuration detector. (B) Light obscuration detector with smoke. Courtesy of System Sensor: *Guide for Proper Use of System Smoke Detectors.*

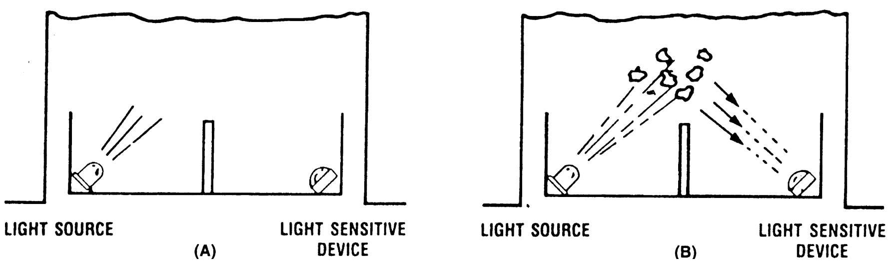


Figure 6.9 Diagrams of how a photoelectric light scattering smoke detector works. (A) Light scattering device. (B) Light scattering detector with smoke. Courtesy of System Sensor: *Guide for Proper Use of System Smoke Detectors.*

According to Moore (1997, p. 5-15),

> As a class, smoke detectors using the ionization principle provide somewhat faster response to high-energy (open-flaming) fires, since these fires produce large numbers of smaller smoke particles. As a class, smoke detectors operating on the photoelectric principle respond faster to the smoke generated by low-energy (smoldering) fires, as these fires generally produce more of the larger smoke particles.

Placement of Smoke Detectors

Smoke detectors generally are located in open areas, spaces above suspended ceilings, spaces under raised floors (particularly in computer rooms and data centers), cafeteria areas, air duct systems, passenger and service/freight elevator lobbies, elevator shafts, elevator machine rooms, enclosed stairways, dumbwaiter shafts, chutes, and electrical and mechanical equipment rooms. The specific locations and spacing of smoke detectors are determined by an assessment of local laws, codes, and standards and engineering issues. Factors include "ceiling shape and surface, ceiling height, configuration of contents in the area to be protected, burning characteristics of the combustible materials present, ventilation, and the ambient environment'' (NFPA 72, 1999, 2-3.4.1.1). For example, in reviewing ventilation, it must be taken into account that at times, particularly after normal business hours, the HVAC systems in the building may be shut down. Hence, duct smoke detectors must not be used as an alternative to area smoke detectors because during the times the HVAC system is shut down, smoke may not be drawn from open areas to the duct detectors. Also, dilution of the smoke makes them inappropriate for area detection. ''In spaces served by air-handling systems, detectors shall not be located where airflow prevents operation of the detectors'' (NFPA 72, 1999, 2-3.5.1).

Of course, all locations chosen for the installation of smoke detectors must be accessible for periodic device testing and maintenance. If the detectors are located in areas where they may be subject to mechanical damage, they should be adequately protected; for example, some smoke detectors may have a protective wire-frame covering.

Addressable System

The use of multiple smoke detectors in high-rise buildings has been made possible by the development of the *addressable* system. When an alarm occurs, an addressable system can determine which particular device and its address or location that is causing an alarm. This permits new systems to be zoned by device, rather than by floor and adds flexibility to their operation. For instance, if an elevator lobby smoke detector is activated, all elevators are recalled in the manner described under ''Controls in Elevator Lobbies'' later in this chapter. The sequence of smoke detector operation in a typical modern high-rise building is detailed in Table 6.1.

Heat Detectors

Heat detectors are automatic fire detection devices that initiate an alarm when a certain temperature or rapid change in temperature causes a variance in the physical nature or electrical conductivity of a sensing material. Heat detectors are classified by their mode of operation:

- *Fixed-temperature detectors* initiate an alarm when a detecting metal or metals, heat-sensitive cable, or expanding liquid attains a predetermined temperature. The metal may be a fusible alloy, such as that commonly used in automatic sprinklers.
- *Rate compensation detectors* initiate an alarm when the air surrounding the detector attains a predetermined temperature, irrespective of the rate at which the temperature rose.
- *Rate-of-rise detectors* initiate an alarm when the rate of increase in temperature exceeds a predetermined amount.

In addition, there are combination detectors that, for example, combine the features of both fixed-temperature and rate-of-rise devices. The fixed-temperature element will sense a slow developing fire when a predetermined temperature has been attained; the rate-of-rise element will sense a rapidly

Table 6.1 Sequence of Operation of Fire Life Safety Systems in a Typical High-Rise Building

	MANUAL FIRE ALARM STATION	AREA SMOKE DETECTOR	DUCT SMOKE DETECTOR	ELEVATOR LOBBY SMOKE DETECTORS	ELEVATOR SHAFT SMOKE DETECTOR	HEAT DETECTOR	SPRINKLER WATER-FLOW DEVICE	SPRINKLER VALVE TAMPER DEVICE	SPECIAL EXTINGUISHING AGENTS
AUDIBLE AND VISUAL SIGNAL AT BUILDING CONTROL STATION	YES	YES	YES	YES	YES	YES	YES	YES	DEPENDS ON THE SYSTEM
SIGNAL AT OFF-SITE MONITORING STATION	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM	DEPENDS ON THE SYSTEM
AUDIBLE (AND POSSIBLY VISUAL) SIGNAL ON FLOOR IN ALARM	YES	YES	YES	YES	NO	YES	YES	NO	DEPENDS ON THE SYSTEM
SHUTDOWN AIR-HANDLING SYSTEMS ON FLOOR IN ALARM	YES	YES	YES	YES	NO	YES	YES	NO	DEPENDS ON THE SYSTEM
ACTIVATE MECHANICAL SMOKE REMOVAL SYSTEMS ON FLOOR IN ALARM	YES	YES	YES	YES	NO	YES	YES	NO	DEPENDS ON THE SYSTEM
ACTIVATE PRESSURIZATION FANS IN BUILDING STAIRWELLS	YES	YES	YES	YES	NO	YES	YES	NO	DEPENDS ON THE SYSTEM
RELEASE HOLD-OPEN DEVICES ON FLOOR IN ALARM	YES	YES	YES	YES	NO	YES	YES	NO	DEPENDS ON THE SYSTEM
RELEASE STAIRWELL DOOR LOCKS IN BUILDING	YES	YES	YES	YES	NO	YES	YES	NO	DEPENDS ON THE SYSTEM
RECALL ALL ELEVATORS SERVING FLOOR IN ALARM	NO	NO	NO	YES	NO	NO	NO	NO	DEPENDS ON THE SYSTEM

developing fire. (See Figure 6.10 for an example of a fixed-temperature/rate-of-rise thermal sensor.)

The selection of an automatic fire detection device, such as a heat detector, is important if it is to be effective in detecting the type of fires expected in the area concerned and not be subject to frequent false alarms.

> Although [heat detectors] have the lowest false alarm rate of all automatic fire detector devices, they also are the slowest in detecting fires. A heat detector is best suited for fire detection in a small confined space where rapidly building high-heat-output fires are expected, in areas where ambient conditions would not allow the use of other fire protection devices, or where speed of detection is not a prime consideration. (Moore 1997, p. 5-12)

The sequence of heat detector system operation in a typical modern high-rise building is detailed in Table 6.1.

Figure 6.10 A fixed temperature/rate-of-rise thermal sensor. Courtesy of System Sensor.

Gas Detectors

Gas detectors are automatic detection devices that monitor low-level concentrations of combustible gases such as methane, ethane, natural gas, and propane. When concentrations reach a predetermined level, an alarm will be triggered to advise building occupants of the possible hazard. Various Los Angeles high-rise structures, for example, use this type of device. Methane gas seeps up out of the ground in some areas; as a result, methane gas detection systems have been installed as part of some high-rise life safety systems. If a certain concentration of methane gas is detected, an initial automatic alarm will notify security and engineering staff that further investigation is required. If the concentration continues to increase and reaches a predetermined level, the system automatically initiates another alarm indicating that the fire department and building occupants should be notified immediately of the potential hazard.

Automatic Sprinkler Systems

''In 1872, Philip Pratt of Massachusetts is credited with developing the first automatic sprinkler system in the United States . . . the first practical sprinkler was patented by Henry Parmelee of Connecticut in 1874. Parmelee improved on his device in 1875 and 1878 and it became the first sprinkler used extensively'' (Hoover, 1991, pp. 24, 25).*

An automatic sprinkler is ''a device for automatically distributing water on a fire in sufficient quantity either to extinguish it entirely or to prevent its spread in the event that the initial fire is out of range, or is a type of fire that cannot be extinguished by water'' (Abbott, 1994, p. 2-1). As explained by Robert E. Solomon (1997, p. 6-140),

> A *sprinkler system* is defined as a combination of underground and overhead piping that is installed throughout the building. The piping within the building is used to carry the water supply throughout the structure. The sprinklers are then connected to this part of the system. Sprinklers are usually activated by heat from the fire, and only those devices in the immediate vicinity of the fire will operate.

Automatic sprinklers not only are required in new high-rise office buildings, but in many cities it is mandated by code that existing high-rises be retrofitted with automatic sprinkler systems.

The prime motivational factor for the installation of sprinkler systems is that in the time that they have been in existence, they have proven to be an effective means of controlling fires. There is a substantial reduction of the chances of death or extensive property damage in a fully sprinklered building. ''The NFPA has no record of a fire killing more than two people in a fully sprinklered public assembly, educational, institutional, or residential building in which the sprinkler system was operating properly, except in the case of explosions and flash fires† and in instances in which fire brigade members or employees were killed during fire suppression operations'' (Hall, 1993, p. 47). In a later report, Dr. Hall, NFPA's assistant vice president for Fire Analysis and Research, states that, ''When sprinklers are present, the chances of dying in a fire and property loss per fire are cut by one-to two-thirds, compared to fires reported to fire departments where sprinklers are not present'' (Hall, 1997, p. 1-14).

Sprinkler Control Valve, Water-Flow Detector, and Fire Pump Status Panels

These annunciator panels monitor the sprinkler control valves and water-flow detection devices located throughout the building and the status of the fire

---

*The need to develop a consensus standard for sprinkler system installation led to a committee that helped in forming the National Fire Protection Association and in the writing of its first standard, *Standard for the Installation of Sprinkler Systems*, in 1896 (Hoover, 1991, p. 29).

†Although it might be argued that the catastrophic loss of life in the September 11, 2001, destruction of the New York World Trade Center was caused by fire.

pumps. NFPA 101, *Life Safety Code*, requires that, ''High rise buildings shall be protected throughout by an approved, supervised automatic sprinkler system installed in accordance with Section 9.7 [Automatic Sprinklers and other Extinguishing Equipment]. A sprinkler control valve and a waterflow device shall be provided for each floor'' (2000, 11.8.2.1).

The following description of automatic sprinkler systems was compiled using NFPA 13, *Standard for the Installation of Sprinkler Systems* (1999), and the *Fire Protection Handbook* (Solomon, 1997, pp. 5-136–5-164; and Martin, 1997, 6-165–6-174) as references.

Water Supply for Sprinklers

For automatic sprinklers to operate, there must be a supply of water to the sprinkler that opens to extinguish or control fire and prevent it from spreading. This water may come from a variety of sources such as public water systems (usually considered the principal or primary water supply) and storage tanks of three types.

Gravity tanks are tower- or roof-mounted water reservoirs that are not likely to be used for modern high-rise buildings. *Pressure tanks* are pressurized water reservoirs used to supply a limited amount of water for building sprinkler systems. Each tank is located above the highest sprinkler heads. When the public water pressure is too low to supply water to sprinklers on upper high-rise floors, the pressure tanks are used until water can be pumped into the sprinkler system through fire department connections (these connections are explained later). *Suction tanks*, equipped with automatically operated fire pump(s), are increasingly used as a secondary water supply and sometimes, where the authority having jurisdiction permits, as a principal water supply. These tanks are normally constructed of concrete, steel, or fiberglass and may be located directly beneath the fire pumps.

The selection and location of these tanks and automatic fire pumps are based on the size and height of the building, its type of tenancy, and pattern of use.

Fire Pump

A *fire pump*[*] is a mechanical device for improving the water supply pressure from public water systems and storage tanks. In modern high-rise buildings, centrifugal force is primarily responsible for developing fire pump pressure. The pumps are driven by electric motors (Figure 6.11), or by internal combustion engines fueled by diesel oil. Fire pumps usually are housed in areas protected from the possible effects of fires, freezing temperatures, explosions, and natural disasters such as floods and earthquakes.

Fire pumps usually are designed to start automatically when water pressure in the fire protection system drops to a predetermined level and are shut down manually when their services are no longer needed.

[*]''Some [fire pumps] are called booster pumps because they 'boost' the pressure of the public supply'' (Hoover, 1991, p. 186).

Figure 6.11 Two electric fire pumps located alongside each other in the fire pump room of a high-rise building. Photograph by Roger Flores.

In addition to automatic fire pumps, there are pressure maintenance *jockey pumps*. These very small pumps automatically maintain the operating pressure in the fire protection system. To avoid starting the fire pump engine when there are small fluctuations in pressure, the jockey pump automatically starts, boosts the pressure to the correct level, and then shuts itself down.

Fire Department Connections

In addition to the aforementioned water sources, on the exterior of the building there are fire department connections that can be accessed by the fire department to pump water into the sprinkler system. These connections are required by NFPA 13, *Standard for the Installation of Sprinkler Systems* (1999). They are used when the building water supply system is unable to provide water at sufficient pressure for the sprinkler system to discharge and disperse water effectively.

These fire department connections are easily accessed, usually being situated on the street side of the building, and are conspicuously marked with signs. Examples of the signs are ''AUTOSPKR.,'' ''OPENSPKR.,'' or ''AUTOSPKR. and STAND-PIPE.'' The connections often are fitted with protective caps that can be easily removed by the fire department to attach their hoses (Figure 6.12).

The fire department obtains water for these connections from water hydrants using fire department pumpers. Fire hydrants generally are located close to intersections and along the street to meet the needs of adjoining structures. Today there are two basic types of fire hydrants in use. The dry barrel, base valve, or ''frost-proof'' hydrant is the one most common and is found in areas where temperatures sometimes go below freezing. The wet barrel or ''California'' hydrant is used in areas where temperatures do not go below freezing (Figure 6.13).

In the typical modern high-rise, water is vertically transported upward in the building through a sprinkler system riser or vertical pipe located in each stairwell. A system of overhead piping on each floor horizontally connects the riser to the sprinklers that are located at regular intervals along the pipes. The horizontal pipes are commonly located in the concealed space throughout the whole floor area. They are attached to the floor above using hangers and clamps (Figure 6.14).

In high-rise office buildings, sprinklers usually are the standard spray types. These sprinklers often visibly protrude through the ceiling (Figure 6.15) or are flush with it and hidden from view by a metal cap or disk (Figure 6.16). In the latter case, when a predetermined temperature is attained,

Figure 6.12 Fire department connections serving high, mid, and low zones of a modern high-rise building. Photograph by Roger Flores.

Figure 6.13 ''California'' wet barrel fire hydrant. Photograph by Roger Flores.

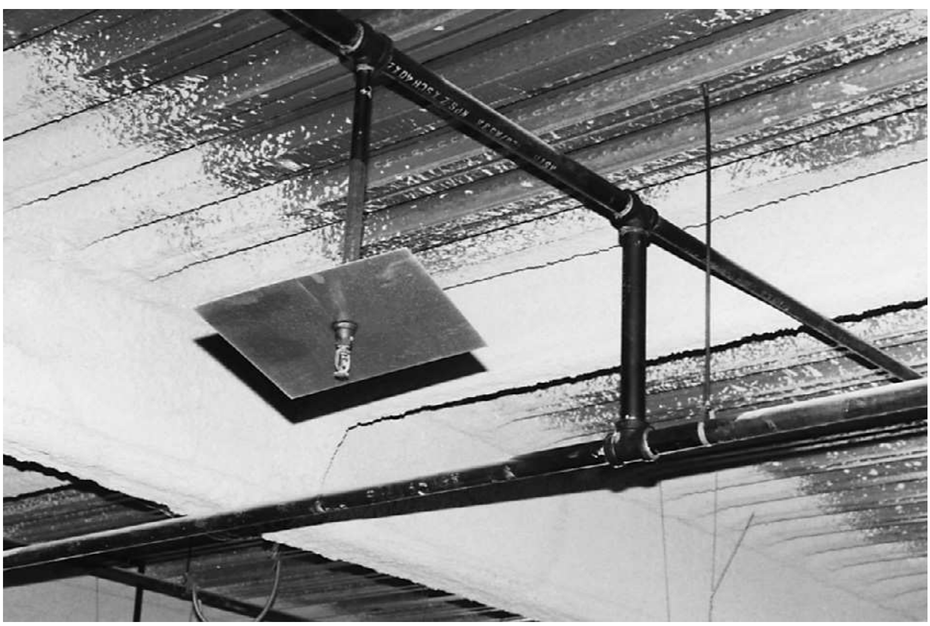


Figure 6.14 Sprinkler pipes and sprinkler before the suspended ceiling is installed. Photograph by Roger Flores.

Figure 6.15 A recessed sprinkler protruding through the ceiling. Courtesy of Viking Corporation, Hastings, MI.

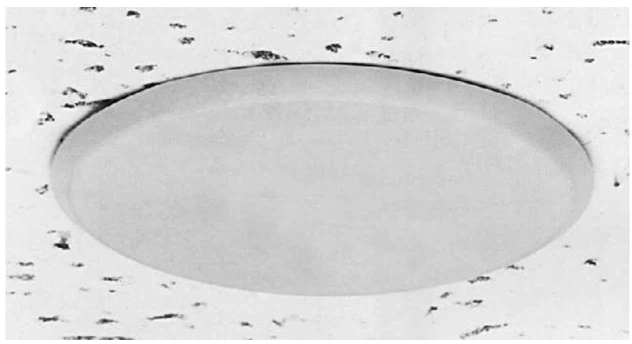


Figure 6.16 Cover plate for a concealed sprinkler. Courtesy of Viking Corporation.

the cap or disk drops away, leaving the sprinkler exposed. The cap is marked ''Do Not Paint'' to help prevent the problem of the cap being painted over and thereby possibly adhering to the ceiling.

Sometimes sidewall sprinklers are used in high-rise buildings. They have the same parts as a standard sprinkler with the exception of a special deflector that discharges water toward one side.

How Automatic Sprinklers Work

An automatic sprinkler is ''a device consisting of a threaded orifice, a cap, supporting arms, a fusible element, and a deflector, which when attached to a sprinkler system branch line discharges water in a specific pattern onto a fire'' (Hoover, 1991, pp. 347, 348). Sprinklers commonly contain a fusible metal that melts rapidly at a certain temperature and fuses, thereby permitting a cover over an opening in the sprinkler to drop away, water to flow, and a water-flow indicator to initiate a fire alarm. ''Initiation of the alarm signal shall occur within 90 seconds of waterflow at the alarm-initiating device when flow occurs that is equal to or greater than that from a single sprinkler of the smallest orifice size installed in the system. Movement of water due to waste, surges, or variable pressure shall not be indicated'' (NFPA 72, 1999, 2-6.2). The reason for the 90-second delay is to avoid false alarms by allowing sufficient time to ensure that a stable water flow has been achieved. The fire alarm is automatically transmitted to the Fire Command Center and possibly to an off-site central monitoring station, sounds on the floor where the sprinkler water flow has occurred (and possibly on one or two floors above and below the alarm floor), and sounds a sprinkler fire-alarm bell located on the exterior of the building near ground level.

Types of Automatic Sprinkler Systems

There are three types of sprinkler systems found in high-rise office buildings: wet pipe, dry pipe, and pre-action.

Wet-Pipe System

The wet-pipe system is the most common sprinkler system used in high-rise buildings. In the event of a fire, if the temperature exceeds a predetermined point, the fusible link in the sprinkler fuses, the sprinkler opens, and *water contained in the pipe* (which is connected to the water supply) is immediately discharged on the fire. A prerequisite of this system is that the area in which it is installed must be kept at temperatures above freezing.

Dry-Pipe System

In a dry-pipe system, in the event of a fire, if the temperature exceeds a predetermined point, the fusible link in the sprinkler head fuses, the sprinkler head opens, and *pressurized air* (or *nitrogen* for a small dry system) *contained in the pipe* escapes, permitting a dry-pipe valve to open; water then enters the sprinkler piping and flows out of the open sprinkler.

This type of system is used in unheated areas. If water were contained in a sprinkler pipe at low temperatures, it could freeze, thereby rendering the system ineffective. Because most commercial high-rise buildings are temperature-controlled, few of these more expensive dry-pipe systems are used in them, except possibly in garage or loading dock areas.

Pre-action System

The pre-action system works on the principal that, in the event of a fire, an automatic fire detection device (such as a smoke or heat detector) located near the sprinkler will be activated. This in turn will allow water to enter the piping *before* the sprinkler is activated. Then, when the sprinkler opens at a predetermined high temperature, water can immediately flow out of it.

This system is used in areas such as tenant computer rooms and data centers where there is great concern for the accidental discharge of water, which could damage, disable, or destroy computers or other valuable electronic equipment.

Supervision and Manual Operation of the Automatic Sprinkler System

A sprinkler control valve is provided on each floor in the stairwell(s) so that the automatic sprinkler system can be manually shut down for that floor. A *looped* sprinkler system means that the piping is continuous throughout a floor and a sprinkler control valve is located in each stairwell. To manually shut down the looped sprinkler system for a floor, the control valve in *each* stairwell must be shut down. Under normal conditions, the sprinkler control valve remains in the *open* position. (To avoid malicious tampering with the sprinkler control valve, it is generally recommended that the valve be maintained in the open position using a chain and padlock. An authorized person needing to shut the control valve can access it by unlocking the padlock. If this cannot be done in a timely manner, the chain can be cut.)

The sprinkler control valve is fitted with a supervisory signal-initiating device. Whenever the valve is moved from or back to its normal position, separate and distinct signals are initiated and immediately sent to the Fire Command Center.

The supervisory signal-initiating device that monitors a sprinkler control valve, the water-flow switch, and the hose connection and valve for a combined sprinkler and standpipe riser are shown in Figure 6.17.

Standpipe and Hose Systems

Before proceeding further, it is appropriate to discuss standpipe and hose systems. A *standpipe* system in a high-rise building is a pipe structure designed to vertically transfer water to upper floors of the building so that the water can be used to fight fires manually with fire hoses (Figure 6.18). The standpipe system is another tool that can be used by trained building personnel or members of the fire department to combat fires. ''Even in buildings that are protected by automatic sprinklers, standpipe systems play an essential role in building fire safety by serving as a backup for, and complement to, sprinklers'' (Shapiro, 1997, p. 6-249).

Standpipe systems are subdivided into ''classes'' and ''types.''

Classes of Standpipe Systems

''Standpipe classes delineate the intended use of a system, i.e. fire department use or occupant use'' (Shapiro, 1997, p. 6-250). There are three classes* of standpipe systems classified according to the service for which they are designed.

*The descriptions of these classes, and the ensuing description of the types of standpipe systems, were compiled using NFPA 14, *Standard for the Installation of Standpipe, Private Hydrant, and Hose Systems* and the *Fire Protection Handbook* (Shapiro, 1997, pp. 6-249–6-263).

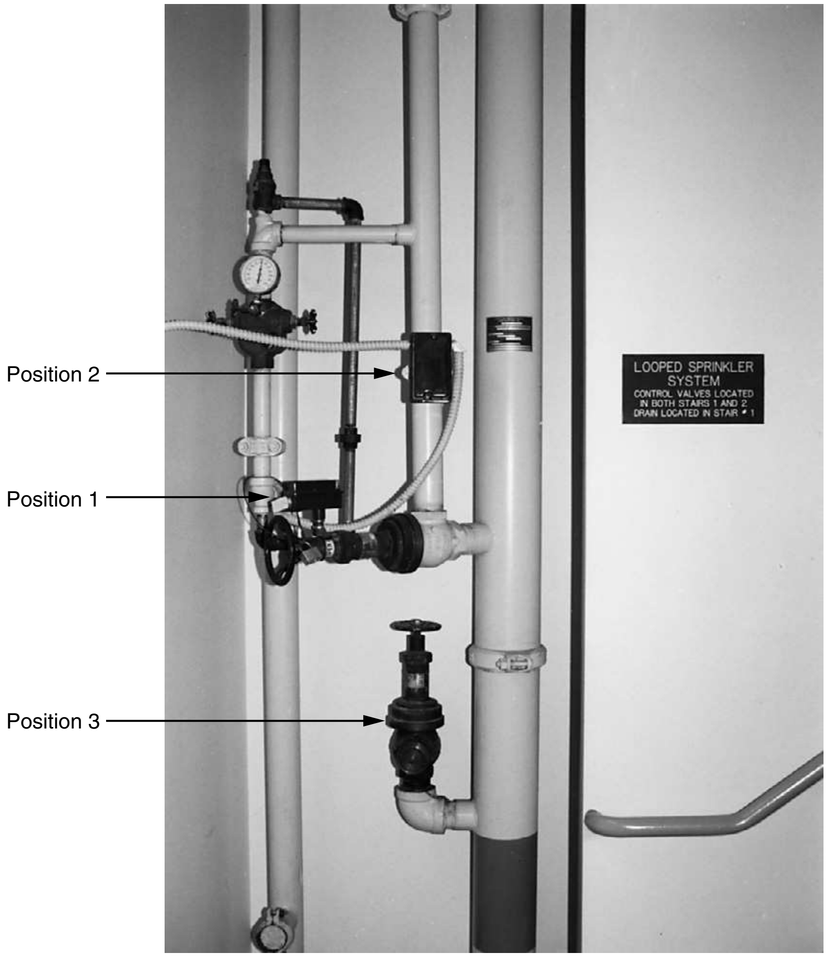


Figure 6.17 A looped wet-pipe sprinkler riser located in a stairwell. (The vertical pipe on the left-hand side is a drain and test pipe.) The supervisory signal-initiating device that monitors the open position of the OS & Y (outside screw & yoke) sprinkler control valve is located at position 1 and a water-flow switch is mounted at position 2. At position 3 is a hose connection and valve. (**Note**: The system displayed here is a combined sprinkler and standpipe riser.) Photograph by Roger Flores.

Class I Systems

Class I systems provide 2½-inch (63.5-mm) hose connections from a standpipe or combined riser for use by fire departments and those trained in handling heavy streams of water. (A *hose connection* is the point where the fire hose connects to the standpipe system. A *combined riser* is a vertical pipe that serves outlets for fire department use and provides water for automatic sprinklers.)

Use of a Class I system reduces the time and number of fire department personnel needed to attack a fire because hoses can be run within the building

Figure 6.18 A fire hose cabinet. (This cabinet is located on the roof of a high-rise building in Los Angeles, where such installations are required by code.) Photograph by Roger Flores.

close to the fire rather than running extensive lines from exterior locations. Therefore, Class I systems are generally required in both sprinklered and non-sprinklered high-rise buildings.

Class II Systems

Class II systems provide 1½-inch (38.1-mm) hose connections from a standpipe, combined riser, or sprinkler system for use by trained building staff, occasionally by the fire department on arrival, and perhaps by building occupants before the fire department arrives. Typically each hose connection has a hose, a hose nozzle, and a hose rack installed on it.

The use of Class II systems with hoses preconnected to standpipe systems is becoming less prevalent because of two main concerns: whether untrained occupants can safely use a 100-foot (30.5-meter) long hose providing water at a flow rate of 100 gallons per minute (378 liters per minute), and whether it is a sound practice for occupants to be involved in fighting a fire instead of immediately evacuating an area. Many jurisdictions have entirely removed the requirement for occupant-use hose systems in facilities that are fully sprinklered.

Class III Systems

Class III systems provide both Class I and Class II hose connections supplied from a standpipe or combination riser for use by building occupants and a larger volume of water for use by fire departments and those trained in handling heavy streams of water.

The use of Class III systems is becoming less prevalent because of the same concerns listed under ''Class II Systems.''

Types of Standpipe Systems

''Standpipe types delineate the basic characteristics of system design, i.e. whether the piping will be filled with water or not (wet or dry), and whether the water supply for fire fighting will be automatically available or not (automatic, semiautomatic, or manual)'' (Shapiro, 1997, p. 6-250).

In high-rise buildings, there are three permissible standpipe systems. As explained by Shapiro (1997, p. 6-250), they are as follows:

> *Automatic-wet systems* have piping that is filled with water and have a water supply capable of supplying the fire-fighting water demand that is automatically available. [A prerequisite of such a system is that the area in which it is installed be kept at temperatures above freezing.]
>
> *Automatic-dry systems* have piping that is normally filled with pressurized air; systems are arranged, through the use of devices such as a dry-pipe valve, to automatically admit water into system piping from a water supply capable of supplying the fire-fighting water demand when the hose valve is opened.
>
> *Semiautomatic-dry systems* have piping that is normally filled with air; systems are arranged through the use of devices, such as a deluge valve, to admit water into system piping from a water supply capable of supplying the fire-fighting water demand when a remote actuation device located at a hose station* is operated.

The automatic-wet standpipe system is most commonly installed in modern high-rise buildings with a fixed water supply not exposed to freezing. It is considered more effective in fighting fires than the other two systems.

Zoning in Tall Buildings

In tall buildings, to keep water pressures within a safe limit and, for example, to reduce the possibility of hoses attached to the standpipe system bursting or being too difficult to handle, standpipe systems are frequently separated into multiple zones that limit the maximum height of the water column. ''The goal of zoning is to limit the pressure that can be developed in system piping and at

*A hose station is defined by the NFPA as ''a combination of a host rack, hose nozzle, hose, and hose connection'' (NFPA *Glossary of Terms,* 2001).

hose connections to reduce the need for high-pressure fittings and pressure-reducing valves'' (Shapiro, 1997, p. 6-254).

Fire Department Connections

As with automatic sprinkler systems, on the exterior of the building there are connections that can be accessed by the fire department to pump water into the standpipe system. This may be required if the building water supply system is unable to provide water at sufficient pressure for the standpipe system to disperse water effectively, or if the standpipe system is a dry standpipe without a permanent water supply capable of sending water to the system on demand. If the building has two or more zones, each pressure zone should have its own fire department connection.

These fire department connections are easily accessed, usually on the street side of the building, and are conspicuously marked with a sign stating ''STANDPIPE.'' If the hose connection also supplies an automatic sprinkler system, the sign or combination of signs will specify both services, for example, ''AUTOSPKR. and STANDPIPE.'' The connections usually are fitted with protective caps that can be easily removed by the fire department to attach their hoses. The fire department obtains water for these connections from water hydrants using fire department pumpers.

The sequence of automatic sprinkler and fire pump system operation in a typical modern high-rise building is detailed in Table 6.1.

Other Fire Protection Equipment and Systems

Annunciator or Status Indicators

In addition to water, which is the primary extinguishing agent for building fires, there are other special extinguishing agents used in a high-rise office building. Examples of these are carbon dioxide, halon and halon replacements, dry chemical, and wet chemical.

The authority having jurisdiction will require the Fire Command Center to supervise any such special extinguishing systems located within the building.

Carbon Dioxide Systems

Carbon dioxide is one and one half times heavier than air; it is a colorless, odorless, noncombustible, electrically nonconductive inert gas found in the atmosphere. It comprises a significant percentage of air and is a byproduct of the decay and burning of organic substances and respiration in humans and animals. Carbon dioxide can be used to extinguish fires because it reduces the amount of oxygen in the atmosphere to the point where combustion cannot be supported. Because it does not conduct electricity, it can be used on live electrical equipment. Also, it has the advantage that no cleanup is required after use because it does not leave behind a residue. One disadvantage, however, is that it produces solid dry ice particles on discharge that, because of their low temperature, may damage electrical equipment that they contact. Carbon dioxide is not used in normally occupied areas and would require a pre-discharge alarm because discharge of it may cause suffocation.

Four Basic Types of Application

NFPA 12, *Standard for Carbon Dioxide Extinguishing Systems* (2000), recognizes four basic types of systems for applying carbon dioxide to extinguish fires:

1. A *total flooding* system involves a fixed quantity of carbon dioxide that is stored in containers and, on activation of a manual control station (that is equipped with a manual override) or an automatic detector, is discharged through fixed nozzles attached to fixed pipes into a fixed enclosure surrounding the fire hazard. Because carbon dioxide is dangerous to human beings, the enclosed area must be evacuated of all occupants before the gas is discharged.
2. A *local application* system involves a fixed quantity of carbon dioxide stored in containers. On activation of a manual control station (equipped with a manual override) or an automatic detector, it is discharged directly onto the fire hazard through nozzles attached to fixed pipes.
3. A *hand hose line* system involves a fixed quantity of carbon dioxide that is stored in containers and has hand hose lines permanently attached and ready for immediate, usually manual, application to small fire hazards.
4. A *standpipe system and mobile supply* involves a mobile quantity of carbon dioxide that is stored in containers that in the event of a fire can be rapidly shifted into position and attached to a total flooding, local application, or hand hose line system.

Carbon dioxide can be used to suppress fires involving gas, flammable liquids, electrical equipment, and common combustible elements such as wood and paper.

Halon and Halon Replacement Systems

Since the evidence indicating the adverse effect of halon on the earth's stratospheric ozone layer, and the requirements of the 1993 Montreal Protocol, halon production ceased ''January 1, 2000, except to the extent necessary to satisfy essential uses, for which no adequate alternatives are available'' (Taylor, 1997, p. 6-281). Because halon can still be found in some buildings, it is addressed here.

In high-rise buildings, halon can still be found in electrical switchgear rooms and in tenant computer rooms and data centers. The *total flooding* system application involves a fixed quantity of halon, usually Halon 1301 within the United States, that is stored in containers and, on activation of a manual control station (equipped with a manual override) or an automatic fire detector, is discharged through fixed nozzles attached to fixed pipes into a fixed enclosure surrounding the fire hazard. Because it is not dangerous to human beings at low concentrations, halon can be discharged first, and then occupants can safely evacuate the area.

The *local application* system involves a fixed quantity of halon, often Halon 1211 within the United States, that is stored in containers and, on activation of a manual control station (equipped with a manual override) or an automatic fire detector, is discharged directly onto the fire hazard through nozzles attached to fixed pipes.

Halon Replacements

Inergen™ is an alternative agent for Halon 1301 in total-flooding operations within spaces or areas where people work and may be exposed to the agent on discharge. Produced by Ansul Fire Protection (Marinette, Wisconsin), it is a mixture of three inert gases: nitrogen, argon, and carbon dioxide. Like halon, it is colorless, odorless, non-corrosive, and electrically nonconductive. It does not raise the carbon dioxide level enough to prevent respiration and the absorption of oxygen (occupants, therefore, are still able to breathe), but it lowers the oxygen content below the level required for combustion.

Other halon replacement agents include FM-200®, Triolide™, Argonite, and Argon (DiNenno, 1997, p. 6-298), 3M Novec™ 1230, and FE-36.™ These agents should only be used with the approval of the authority having jurisdiction.

Dry Chemical Systems

A *dry chemical* is a powder composed of very small particles. ''The principle base chemicals used in the production of currently available dry chemical extinguishing agents are sodium bicarbonate, potassium bicarbonate, potassium chloride, urea-potassium bicarbonate, and monoammonium phosphate. Various additives are mixed with these base materials to improve their storage, flow, and water repellency characteristics'' (Hague, 1997, p. 6-341).

The exact way dry chemical agents extinguish fires is not yet fully understood. According to NFPA 17 (1998):

> It is now generally accepted that the flame extinguishing properties of dry chemicals are due to the interaction of the particles, which stops the chain reaction that takes place in flame combustion. Dry chemicals vary in their flame extinguishing effectiveness. Multipurpose dry chemical owes its effectiveness in extinguishing fires in ordinary combustibles, such as wood and paper, to the formation of a glow-retarding coating over the combustible material. (Appendix A-1-1)

Dry chemical is primarily used as an extinguishing agent for flammable liquid fires. The dry chemical system is ''a means of applying dry chemical that can be automatically or manually activated to discharge through a distribution system onto or into the protected hazard. The system includes auxiliary equipment'' (NFPA 17, 1998, 1-5 Definitions). Fixed nozzles or hand hose lines use expellant gas to discharge dry chemical.

In high-rise office buildings, dry chemical systems are used mainly for restaurant hood, duct, and cooking appliance systems located in tenant kitchens and cafeterias. NFPA 17, *Standard for Dry Chemical Extinguishing Systems* (1998), outlines pre-engineered dry chemical systems used for such equipment, including deep-fat fryers. These systems are activated automatically by a fusible link or heat detector located, in some cases, above each cooking appliance or group of appliances protected by a single nozzle or, in other cases, at or within the entrance to the ducting system. The systems are also designed so that when activated there will be an automatic shutdown of fuel or power to all the protected appliances (NFPA 17, 1998). This code even specifies which part of the duct system is the building owner's responsibility to protect and which is the tenant's responsibility.

Because dry chemical is electrically nonconductive, it is also used for electrical equipment susceptible to flammable liquid fires. However, in telephone switching, computer rooms, and data centers, where there are sensitive electrical contacts and relays, its use is not recommended. Application in these areas may cause the equipment to malfunction. Dry chemical should be removed as quickly as possible from surfaces to which it has been applied because it may be corrosive.

Wet Chemical Systems

A *wet chemical solution* is defined by NFPA 17A, *Standard for Wet Chemical Extinguishing Systems*, as ''generally potassium carbonate-based chemical, potassium acetate-based chemical, potassium citrate-based chemical, or a combination thereof, and mixed with water to form an alkaline solution capable of being discharged through piping or tubing when under expellant gas pressure'' (1998, A-2-6.1).

> Its effect on fires in common cooking oils and fats is to combine with these materials to form a vapor suppression foam that floats on a liquid surface, such as in deep fat fryers, and effectively prevents reignition of the grease. Wet chemical solution applied to flammable liquid surfaces will result in the rapid spreading of a vapor-suppressing foam on the fuel surface. The foam extinguishes and secures the flame by forming a barrier between the liquid fuel and oxygen. This barrier excludes oxygen from the fuel source and eliminates the release of flammable vapors from the fuel surface. The cooling effect of this solution also lowers the temperature of the flammable fuel, further decreasing fuel vapor release. (NFPA 17A, 1998, A-2-6.1)

Wet chemical systems are similar in their application to dry chemical systems. The wet chemical can be activated automatically or manually to discharge through fixed nozzles and pipes by way of expellant gas.

In high-rise office buildings, wet chemical systems are used mainly for restaurant hoods, plenums, ducts, and associated cooking appliances in tenant kitchens and cafeterias. NFPA 17A, *Standard for Wet Chemical Extinguishing Systems* (1998), outlines pre-engineered wet chemical systems used for restaurant, commercial, and industrial hoods, plenums, ducts, and associated cooking appliances. Like dry chemical systems, these systems are activated automatically by a fusible link or heat detector located in some cases above each cooking appliance or group of appliances protected by a single nozzle or, in other cases, at or within the entrance to the ducting system. The systems are also designed so that when activated, there will be an automatic shutdown of fuel or power to all equipment protected by the system (NFPA 17A, 1998). This code also specifies which part of the duct system is the building owner's responsibility to protect and which is the tenant's responsibility.

As with dry chemicals, wet chemicals should be removed as quickly as possible from the surfaces to which they have been applied.

Air-Handling System Controls and Status Indicators

Modern high-rise buildings are equipped with HVAC or air-conditioning and ventilating (ACV) systems. These systems allow the air within the building to be regularly exchanged, distributed, and maintained at certain levels of temperature, humidity, and cleanliness. The air within the building is thus rendered comfortable for the occupants, and the air temperature of certain areas, such as those containing sensitive equipment, is sustained at predetermined safe levels.

''Air conditioning and ventilating systems, except for self-contained units, invariably involve the use of ducts for air distribution. The ducts, in turn, present the possibility of spreading fire, fire gases, and smoke [and contaminants] throughout the building or area served'' (Schmidt, 1997, p. 7-175).

Purpose of HVAC Systems

NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems* (1999), outlines the purpose of these systems and prescribes minimum requirements for safety to life and property from fire. According to NFPA 90A (1999, p. 1-3.1), these requirements are intended to accomplish the following:

(1) Restrict the spread of smoke through air duct systems within a building or into a building from the outside
(2) Restrict the spread of fire through air duct systems from the area of fire origin whether located within the building or outside
(3) Maintain the fire-resistive integrity of building components and elements such as floors, partitions, roofs, walls, and floor- or roof-ceiling assemblies affected by the installation of air duct systems
(4) Minimize the ignition sources and combustibility of the elements of the air duct systems
(5) Permit the air duct systems in a building to be used for the additional purpose of emergency smoke control

It is not within the scope of this book to describe in detail the HVAC systems that may be found in modern high-rise buildings. To determine what specific equipment should be installed in a building, consult the laws, codes, and standards that have been specifically adopted by the authority having jurisdiction, equipment manufacturer's operation and service manuals, architectural specifications, the building engineer, a qualified HVAC professional, and possibly the local building or fire department. The *ASHRAE Handbook and Product Directory*, by the American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE), is a valuable source of information regarding such equipment.

In understanding these systems, it is helpful to know that HVAC equipment—heaters, fans, and filters—usually is located in service rooms separated from the remainder of the building by fire-resistive floors, walls, and floor-ceiling assemblies. These rooms generally are locked to deter unauthorized entry and may be equipped with automatic sprinklers for fire protection. They also contain smoke detectors that, on activation, will send a signal to the Fire Command Center, automatically shut down the HVAC system, and close fire and smoke dampers* serving that area.

Smoke Control within Buildings

The NFPA 101, *Life Safety Code*, and NFPA 90A acknowledge two approaches to smoke control, the passive and active approach. ''The passive approach recognizes the long-standing compartmentation† concept, which requires that fans be shut down and fire and smoke dampers in ductwork be closed in fire conditions. The active approach utilizes the building's heating, ventilating, and air-conditioning (HVAC) systems to create differential pressures to prevent smoke migration from the fire area and to exhaust the products of combustion to the outside'' (Schmidt, 1997, p. 7-178). In many high-rise buildings, when a fire alarm occurs, there is automatic pressurization of stairwells using fans that keep smoke out of the stairwells. However, each building's smoke control systems will differ according to the laws, codes, and standards required at the time the system was installed.

Status indicators for the HVAC systems and stairwell pressurization fans, and the controls that enable them to be operated manually, are located in the Fire Command Center.

Control of Chemical and Biological Contaminants within Buildings

In a high-rise, the impact of the release of airborne chemical or biological agents is accentuated by the fact that a building's HVAC systems could provide a means for the rapid spread of contaminants throughout a building. This fact has caused considerable debate among industry experts as to what actions should be taken with regard to these complex systems, whose operations often vary from building to building and system to system.

American Society of Heating, Refrigerating, and Air-Conditioning Engineers Initial Report

In an initial report, *Risk Management Guidance for Health and Safety Under Extraordinary Incidents*, issued in January 2002, ASHRAE stated, ''Do not close outdoor air intake dampers or otherwise block ventilation paths; do not change the designed airflow patterns or quantities; and do not modify the fire protection

---

*As defined by NFPA 90A (1999, p. 1-6), a *fire damper* is ''a device, installed in an air distribution system, that is designed to close automatically upon detection of heat, to interrupt migratory airflow, and to restrict the passage of flame;'' and a *smoke damper* is ''a device within the air distribution system to control the movement of smoke.'' There may also be a combination smoke and fire damper that meets the requirements of both.

†Compartmentation also involves the automatic closing of fire doors, such as stairwell and elevator vestibule doors, to protect occupant escape routes during the early stages of a fire.

and life safety systems without approval of the local fire marshal'' (Post, 2002, p. 12). Commenting in the *Engineering News-Record*, Nadine M. Post says that,

> Risk Management Guidance for Health and Safety Under Extraordinary Incidents also offers guidance on steps that can be taken to render buildings somewhat less vulnerable to bioterrorism and other attacks. But for the time being, unless the building is an obvious target, ASHRAE recommends operating buildings normally and, in every case, not making any changes without consulting a professional engineer or expert.
>
> The report, written by a 10-person committee, is not a ''definitive piece'' and not based on a specific building or HVAC system, said James E. Woods, committee chair and president of HP Woods Research Institute, Herndon, VA. It does advise owners to get to know their buildings before making changes and to develop a preparedness plan in case of an incident. It is important to look at the building operation as a whole and to avoid measures that can backfire, caution the authors. For instance, closing off air intake vents can decrease a system's ability to purge contaminants.
>
> Sensors and other warning devices are not available or are not reliable for many contaminants so they cannot be used as a control strategy, says the report. For protection against aerosol attacks from outside, openings ''must be capable of timely closure, located sufficiently remote from any launch site or the building must be equipped with adequate filtration.''
>
> Areas of refuge are not economically viable in many buildings. Consequently HVAC systems can be used to pressurize building egress paths and to isolate significant contamination to ''selected building volumes,'' says the report. Finally, enhanced air filtration alone is not sufficient to reduce airborne contamination. It should be coupled with pressurization of the interior relative to outdoors.

Post says that ASHRAE plans through a year-long exercise to develop more specific guidance and to coordinate its efforts with other engineering disciplines involved in similar studies. More information is provided on this subject in the section ''Chemical and Biological Weapons'' in Chapter 10.

System Reset Procedures

The status indicators, control panels, and procedures used to reset building fire and life safety systems will vary considerably from system to system, manufacturer to manufacturer, and even from model to model within the same manufacturer's line.

Elevator Status Panel Displaying Elevator Operations

Elevator annunciator panels usually are located in the Fire Command Center or at a designated location in the main building lobby. These panels visually display the location of passenger and freight/service elevators operating in the building. They indicate the number of the elevator *car* (sometimes called a *cab*) and the number of the floor on which the elevator is located at any particular time. Some elevator systems visually display on a computer monitor screen the floor that each elevator car is on, whether it is parked or traveling up or down, whether the elevator car door is opened or closed, and whether the elevator is empty or contains passengers.

Devices operated by key or by the computers controlling the elevators may also be provided so that elevator cars can be individually selected and their movement up and down manually controlled at the Fire Command Center, without anyone venturing near the elevators themselves.

Configuration of Elevator Systems

Before outlining elevator safety features and controls, it is appropriate to briefly outline the configuration of elevator systems in high-rise buildings.

Elevator Banks

Elevator cars are separated into *banks* that serve different levels such as low-rise, mid-rise, and high-rise. The number of banks will depend on the size of the building itself. For example, in the 36-floor high-rise tower Pacific Tower Plaza described in Chapter 4, there are 17 passenger elevators, one service/freight elevator, and three parking shuttle elevators. The configuration of the elevators is as follows:

- Low-rise bank—six elevators (numbered 1–6) serve floors 1–12
- Mid-rise bank—six elevators (numbered 7–12) serve floors 13–23
- High-rise bank—five elevators (numbered 13–17) serve floors 23–36
- Freight/service elevator—one elevator (numbered 18) serves floors 1–36
- Parking shuttle elevators—three elevators serve floors P3–1

Sky Lobby System

A sky lobby is where occupants can cross over from an express elevator to another group of elevators.

> As for the *sky-lobby*, the principle consists of a variation on the arrangement of elevators in batteries [banks], each serving a group of floors. In this case, each battery [bank] begins at the lowest level of the floors it serves. This level is reached by an express elevator directly linked to the ground floor. The sky-lobby therefore is the transfer area between an express elevator and a battery [bank] of local elevators . . . . The system is a requirement in the case of mixed-use buildings, where each group of floors—offices, apartments, a hotel—functions as a separate unit. (Mierop, 1995, p. 70)

The sky lobby system was conceived to address an elevator space problem in the construction of the 110-story New York World Trade Center Twin Towers (Sullivan, 1964, pp. 56–58). As described in *Twin Towers* by Angus Kress Gillespie (1999, pp. 74–76),

> The higher you go, the more people in the building. The more people in the building, the more elevators you need. The more elevators you have, the less floor space you have to rent. The problem was so serious that it was seen as the limiting factor, the real reason why skyscrapers seldom exceeded eighty stories.
>
> During the planning stage, Herb Tessler, one of the staff architects, came up with an idea to solve the elevator problem. [Tessler described the concept to

> Malcolm Levy and then to Guy Tozzoli, the head of planning for the project] ''We could divide each tower building into three parts, or zones. For express elevators from the lobby, we will construct the biggest elevators in the world each carrying 55 passengers. Then we will stick the three local parts on top of one another. Each zone will have its own lobby. People will transfer from express to local in the second and third zones by crossing the lobby. Therefore, all the locals will sit on top of one another within a single shaft, and it will solve the problem of usable space.''
>
> [After presenting the idea to Otis and Westinghouse elevator companies,] Herb Tessler came back and said that Otis could build elevators where the first person in was the first one out. Elevators could be built with doors on both the front and the back of the car. People could get through the front door at the lobby level, and get off through the rear door when they reached the desired floor .... It was a new thing.

In some very tall buildings, such as the Sears Tower in Chicago, ''double-deck express cabs serve the sky lobbies and single deck cabs provide intra-zone travel'' (Southerland, 1999, p. 22).

Sizes of Elevator Cars

Freight/service elevators in buildings usually are larger in size than the passenger elevators and are built to handle the demands of industrial applications and emergency medical responders. The larger size permits the transport of oversize items such as office furniture and equipment, and accommodates the use of gurneys by emergency personnel responding to medical incidents within these buildings.

Elevator Safety Features

Before discussing elevator controls, it is helpful to examine the development of elevators, how they operate, and the reasons why, under normal operating or nonemergency conditions, they are such a safe form of transport. The following material, with some adaptations, is from *Tell Me About Elevators* (Otis Elevator Company, 1974).

Elevators began with safety precautions. In 1878, the firm of Otis Brothers and Company not only developed the hydraulic elevator that was able to operate at speeds of 600 to 800 feet per minute, but also developed a governor-operated safety device to bring the high-speed car to a gradual stop in case of an emergency.

In 1903, the Otis Elevator Company designed *gearless traction electric* elevators, which today are used in office buildings over 10 stories high, for speeds varying from 400 to 1800 feet per minute, or a maximum of about 20 mph. (Elevators could be designed to go faster, but because it may take from 10 to 12 floors to bring the car up to speed and slow it down again, it is impractical to consider this. Also, some people may not feel comfortable traveling at high speeds.) Examples of these elevators can be found in the Empire State Building (where the elevators move at speeds of up to 1200 feet per minute), the John Hancock Building in Chicago (where express elevators are designed to move at speeds of up to 1800 feet per minute), and before its destruction, the Twin

Towers of the World Trade Center in New York City (express elevator speeds were up to 1600 feet per minute).

These elevators were followed by *geared traction* elevators, which operate similarly but are designed for lower speeds varying from 25 to 350 feet per minute, and for loads up to 30,000 pounds or more. As a result, geared systems are used for a wide range of passenger elevator, freight/service elevator, and dumbwaiter applications.

Both these types of elevators use six to eight lengths of wire cable, or ''hoisting ropes'' or ''hoisting cables'' as they are known in the industry, that are attached to the top of the elevator and looped around the *drive sheave*—a wheel with a grooved rim—in special grooves. The other ends of the hoist cables are attached to a counterweight that slides up and down in the elevator shaftway on its own guide rails. With the weight of the elevator car on one end of the hoisting ropes, and the total mass of the counterweight on the other, the cables are pressed down on the grooves of the drive sheave. Thus, when the motor turns the sheave, it moves the cables with almost no slippage. Actually, the electric hoisting motor does not have to lift the full weight of the elevator car and its passengers. The weight of the car and about half its passenger load is balanced out by the counterweight, which is sliding down as the car is going up (Figure 6.19).

In 1921, the American Society of Mechanical Engineers established safety codes for elevators and escalators. They were developed from informal ''laws'' pertaining to the safety of passengers in elevators and became the American Standard Safety Code for elevators. This has been the model code ever since and is updated continually. Most elevators in the United States conform to its standards, which accounts in part for their excellent safety record.

Safety Developments

Over the years, safety developments for elevators have included the following:

- A self-leveling device greatly reduces the tripping hazards for passengers as they step off elevators. (It is called the Microdrive and was developed in 1915 by Otis.)
- Hoistways and the sides and backs of elevators are enclosed.
- A door interlock system prevents an elevator from operating unless the door at each floor is closed and locked.
- An electronic safety device, the *photoelectric eye*, detects the presence of a person standing in the elevator's doorway, and causes the doors to return automatically to the fully open position.
- As mentioned earlier, six to eight hoisting ropes or steel cables are used to lower and raise the elevator. Any one of these cables is strong enough to support the weight of the car plus the maximum allowable weight of the passengers. (This serves as a safety feature, but the main purpose of the extra hoisting ropes actually is to increase the traction area on the drive sheave.)
- Weight sensors that stop an elevator car from operating if it is overloaded.
- The governor, a safety device that prevents an elevator car from falling or from moving downward too fast. A steel rope or *governor cable* runs from the elevator car to the driving wheel of this device. If the elevator car exceeds its normal design speed for any reason the driving wheel trips a safety switch that

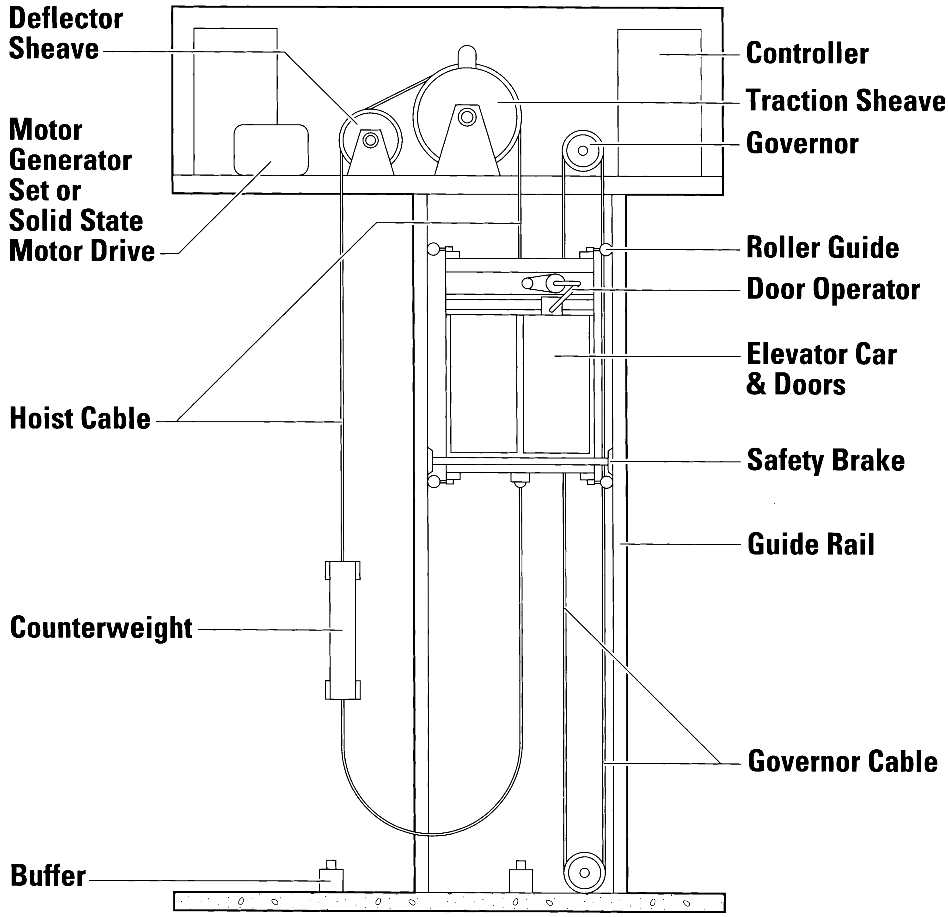


Figure 6.19 Working parts of a traction elevator. Reprinted with permission from *Ups and Downs*, Schindler Elevator Corporation, Morristown, NJ.

sets the brake on the elevator's driving machine. Usually this braking action is enough to stop the car. If for some reason it doesn't stop the car and its speed continues to increase, the governor causes safety clamps to be released against the elevator's guide rails, which are firmly secured to the building structure. This brings the car to a smooth, sliding stop.

- Seismic devices, designed to shut down elevators when the building itself moves, are incorporated into elevator systems in areas subject to earthquakes. On sensing movement, the device automatically sends a signal to the elevator control system and causes each affected elevator car to go to the nearest floor in its current direction of travel, makes its doors open automatically, and then shuts down the elevator. The elevator can only be restarted after the seismic device has been reset. After the probability of aftershocks has passed, a qualified individual—an elevator mechanic, building inspector, or possibly the building engineer—should inspect elevator shafts and elevator cars to check for any possible damage or safety hazards before resetting the seismic device. Possible damage could include loosening of counterweight guide shoes and counterweight rails, jammed hoist-way doors, failure of hoisting ropes or supports, and dislocated control equipment in elevator machine rooms.

Elevator Controls

Although elevator systems vary from building to building and even from model to model within the same manufacturer's line, there are basic similarities of elevator controls.

Inside the elevator car there is often an internal control panel that consists of two main parts: the passenger open control panel and the locked control or service panel.

Passenger Open Control Panel

The *passenger open control panel* or *main car station* consists of a floor selection panel that enables the passenger to select the desired floor by pressing the appropriately numbered button. The selected button then lights up, indicating that the selection has been registered. As required by code, Braille markings and raised numerals indicating the number of each floor are provided adjacent to the pushbuttons to assist people with disabilities. Some ultramodern elevators have incorporated high-fidelity synthesized voice systems for the visually disabled; these systems announce the floor, the direction of travel, and the next stop.

In elevator systems, manual floor selection can occur through completion of an electrical circuit either mechanically (like a door buzzer) or by heat sensed from the passenger's finger (the latter does not meet Americans with Disabilities Act [ADA] requirements). Other elevators use inductance of electricity (the application of the passenger's finger or other object causes a change in an electrical circuit).

In addition to the floor selection buttons, the following buttons usually are available to passengers:

- *OPEN DOOR*. Pushing and holding this button will extend normal door-opening time or re-open a closing elevator door so that the car doors can be kept open longer than the normally programmed time (e.g., to facilitate passenger loading).
- *CLOSE DOOR*. Pushing this button will close the elevator car door.
- *EMERGENCY CALL, EMERGENCY ALARM*, or *EMERGENCY ONLY*. Pushing this button (often red) will annunciate an audible and visual alarm in the Fire Command Center, or similarly supervised location within the building, to indicate that there is a possible emergency situation in the elevator concerned. The alarm will be also audible both within the car and outside the hoistway.
- *EMERGENCY PUSH TO STOP/PULL TO RUN*. Pushing this button (usually red) will stop the elevator car and annunciate an alarm similar to the one described earlier. Returning the button to its normal position will restore normal operation. In some jurisdictions this device is located in the locked control or service panel where it is not accessible to passengers. This prevents nuisance use and the associated unnecessary sudden stops.

There usually is a two-way emergency communication device such as a telephone housed in a compartment (that automatically connects to an elevator maintenance company or other answering service inside or outside the building), or an intercom (that is connected to the Fire Command Center or similarly-supervised location within the building). If the call is directed off-site, the caller will need to communicate the name of the building and the number of the elevator car in which they are located. The ADA requires new or modified elevators to provide a form of communication that is not totally based on voice in case the caller is hearing or speech impaired.

Locked Control or Service Panel

The *locked control* or *service panel* consists of key-operated controls or controls located in a locked cabinet. It usually is provided for the use of elevator maintenance, building security, building engineering, fire department, or other authorized personnel. Its control devices often include:

- A POWER OR MOTOR GENERATOR switch that is normally left in the ON position when the elevator car is in constant use. When moved to the OFF position, the elevator cannot be operated.
- An INDEPENDENT SERVICE device (or ''manual operation'' or ''service switch'') that permits the use of floor selector buttons to take the car directly to any floor, irrespective of any calls that have been registered inside or outside the elevator car. On independent service, if the car doors are open, the CLOSE DOOR button must be pushed continuously until the car starts to move. On arrival at the selected floor, the doors will open automatically and remain open until another floor selector button is pushed (this mode of operation may vary from system to system). If the operator wants to shut down the elevator while it is on independent service, the switch usually labeled POWER or MOTOR GENERATOR will need to be turned to the OFF or STOP position. Locking of the control panel door prevents any further use of the car without the appropriate key.
- An emergency door open switch that, irrespective of where the car is positioned in relation to the floor level, can be used to open the inner car door. Such a device may be useful if the car will not open normally because it is stalled above or below the floor level.
- An ON and OFF switch to control lighting inside the car. It must be in the ON position whenever the car is in use.
- An ON and OFF switch to control the car ventilation fan. It too should be in the ON position when the car is in use.
- An ON and OFF switch to control the electronic sensing devices (photoelectric or possibly infrared) that control automatic door opening when the elevator doorway is obstructed by a passenger or an object. This device will cause the elevator doors to remain open or to re-open if they have started to close.

Depending on the elevator system, some of the preceding devices, and additional controls, may be openly displayed on the control panel. These are usually key-operated to control their usage.

Also, the operating and inspection license is posted inside each elevator car.

Controls in Elevator Lobbies

In elevator lobbies, there are two controls for the operation of elevators.

Passenger Controls

Elevator call stations are located on the wall outside the elevator shaft and are pushed to summon a car to the floor. (The operating mechanism is similar to that described for operating floor selection buttons inside the elevator car.) The elevator call station will light up to indicate that the hall call has been registered by the elevator system. (Repeated pushing of the station has no effect on calling the elevator.) Some multiple-elevator installations have hall position indicators that visually inform waiting passengers of the location and direction of travel of elevators in the hoistways.

Fire Fighter Controls*

So that elevators are not available to building occupants during a fire, elevator systems in high-rise buildings are usually designed so that when an elevator lobby smoke detector is activated, all elevators serving the floor on which the alarm is occurring will be automatically recalled nonstop to a designated level or recall floor (generally the ground floor), the elevator doors will open to allow passengers to exit, and the elevators will shut down.† If the floor where the elevator lobby alarm is occurring is the designated recall floor, then the elevators will be recalled to an alternate floor.

For fire fighters to control fire-recalled elevators, a *FIRE BYP OFF ON device* (''Fireman's Return Override,'' ''Fireman's By-Pass,'' ''Fireman's Service,'' ''Fire Service,'' or ''Firefighter's Service'') is provided.

> At the main floor of a single elevator or for each of a group of elevators, there is a three-position (ON, OFF, BY-PASS) key-operated switch. During normal elevator operations, the switch is in the OFF position. When the switch is in the ON position, all elevators controlled by this switch and that are on automatic service will return nonstop to the main floor, and the doors will open and remain open. Any elevator moving away from the main floor will reverse at the next available floor without opening its doors. An elevator equipped with automatic power-operated doors and standing at a floor other than the main floor, with doors open, will have its doors close without delay, and then proceed to the main floor. (American Insurance Association, 1974, p. 3-45)

Insertion of a special key in the three-position switch and turning it to BYP will bypass the fire life safety system and allow control of each group of

---

*Whether fire fighters should use elevators during fire situations is a debated issue. As reported by Klaene and Sanders, ''Some fire service professionals say that elevators should never be used under fire conditions or suspected fire conditions until their safety can be verified from the fire floor'' (2000, p. 339). However, Donoghue states that, ''It is standard operating procedure in high-rise structures for fire fighters to use elevators not only to carry equipment for fire-fighting or evacuation purposes, but also to deliver fire personnel to nonfire floors'' (1997, p. 8-56).

†''The automatic or manual return, or recall, of elevators to a designated level or recall floor'' (Donoghue, 1997, p. 8-56) is known as *Phase I* operation. ''*Designated level* is defined as the main floor or some other level that best serves the needs of emergency personnel for fire-fighting or rescue purposes'' (Donoghue, 1997, p. 8-56). (Obtained from ASME A17.1, *Safety Code for Elevators and Escalators*, ASME, Fairfield, NJ, 1996.)

elevators.* "Another two-position on/off, key-operated switch may be provided in the building's central control station. In the on position, the switch instructs all controlled elevators to return nonstop to the recall floor. All registered calls will be canceled. An ascending elevator will stop and reverse direction, without opening its doors" (Donoghue, 1997, p. 8-56).

It is very important that the use of such elevator keys is strictly controlled.

State-of-the-Art Computerized Features

Some elevators have fully integrated, state-of-the-art, microcomputer-based systems that analyze calls, set priorities, dispatch cars on demand, and enable one to control every aspect of the elevator. For example, a simple stroke on the computer keyboard will enable one to program a particular elevator not to stop on a particular floor during certain times. Such controlled access is important from a security standpoint.

Emergency and Standby Power

During electrical power failures, for life safety reasons, emergency and standby power systems (discussed next) allow certain elevators to be operated. The emergency power control panel for elevator operation may be located at a separate locked control panel or within the Fire Command Center. Emergency power systems may vary but basically are designed to provide power to emergency lighting within the elevator car, permit the operation of each elevator to allow passengers to exit the car, establish reduced service during an emergency, and return the elevator system to normal service when electrical power has been restored. The NFPA 101, *Life Safety Code* (2000), requires that standby power must be available to at least one elevator serving all floors and that this power can be transferred to any elevator.

Emergency and Standby Power Systems Status Indicators

In the event of an electrical power outage, modern high-rise buildings are equipped with private, permanently installed power supply systems to mitigate this threat to building operations. Indicators of these systems' operating status are found in the Fire Command Center. NFPA 70, *National Electrical Code* (2002, Articles 700, 701, and 702), outlines two such power systems—emergency and standby.

Emergency Power Systems

Emergency power systems are legally required by local, state, federal, or other codes, or by any governmental agency having jurisdiction, to supply power

*"The provision that allows fire-fighting personnel to operate the elevator from within the car, or emergency in-car operation, is commonly referred to as *Phase II* [operation]" (Donoghue, 1997, p. 8-56).

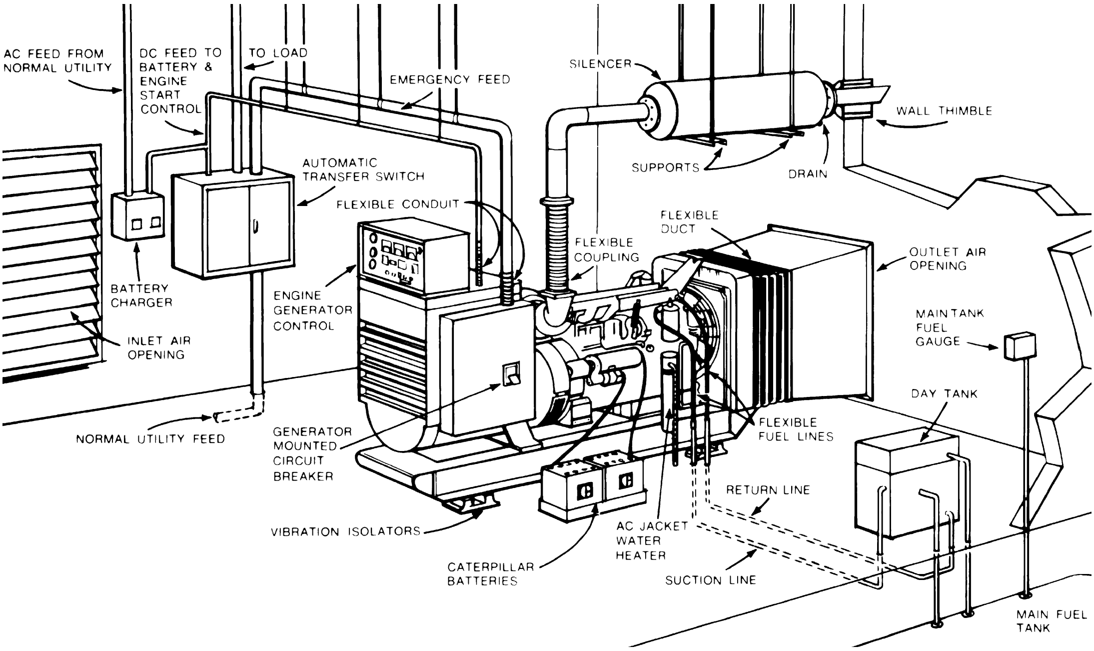


Figure 6.20 A typical package generator set installation used to supply emergency and standby power. Courtesy of Caterpillar.

and illumination automatically to areas that are essential for the life safety of building occupants. Typically these include public address systems, means of egress lighting and other lighting specified as necessary, fire detection and alarm systems, fire pumps, elevators, and other facilities that could pose a threat to life safety when electrical power is interrupted.

Usually, emergency power systems are designed to provide an automatic transfer to emergency power within 10 seconds after failure of normal electrical service to the building. This transfer can be powered by devices such as a storage battery or group of batteries, a generator driven by a fuel-supplied prime mover (Figure 6.20), a UPS, or any other means authorized by the authority having jurisdiction. Lead-acid or nickel-cadmium batteries are dependable but must be located in well-ventilated areas because gases given off by them may be a fire hazard. They must also be recharged after each use. (Batteries may also be used to power self-contained lighting assemblies on failure of electrical power.) For generators driven by a prime mover, if the prime mover is an internal combustion engine, an on-site fuel supply, usually with a fuel supply sufficient for not less than 2 hours full-demand operation of the system, will need to be provided. A UPS is an invaluable system for tenant rooms containing sensitive computer equipment, because it automatically "upon loss of normal power, continues to supply power without waveform distortion, and the load is totally unaware of normal power loss" (Flach, 1997, p. 3-63).

Standby Power Systems

Standby power systems are subdivided into two categories: legally required and optional standby systems.

Legally Required Standby Systems

Legally required standby systems are those mandated by local, state, federal, or other codes, or by any governmental agency having jurisdiction, to automatically supply power to systems other than those classified as emergency power systems, the loss of which could create hazards or have an adverse effect on fire fighting and rescue operations. Typically these include communication systems, ventilation and smoke removal systems, heating and refrigerating systems, and lighting systems.

Legally required standby systems usually are designed to provide an automatic transfer to standby power within 60 seconds of failure of normal electrical service to the building. This transfer can be powered by devices such as a storage battery or group of batteries, a generator driven by a fuel-supplied prime mover, a UPS, or any other means authorized by the authority having jurisdiction.

Optional Standby Systems

Optional standby systems are designed to protect property when life safety is not involved. These systems may supply power, either automatically or manually, to data processing and communication systems, to heating and refrigerating systems, or to any other areas where a loss of power could cause discomfort to people, or serious disruption or damage to the systems involved.

Use of the Terms ''Emergency Power System'' and ''Standby Power System''

The previous differentiation of emergency power systems and standby power systems was based on NFPA 70, *National Electrical Code* (2002). If, however, one considers NFPA 110, *Standard for Emergency and Standby Power Systems* (1999), the meaning of these terms may overlap and lead to confusion. The reason for this is that NFPA 110 places all such systems into categories defined in terms of type, class, and level. ''*Type* defines the maximum allowable time [in seconds] that the load is without acceptable electrical power. [For example, Type U refers to UPS systems, Type 10 refers to a maximum allowable time of 10 seconds, and Type 60 refers to a maximum allowable time of 60 seconds.] *Class* defines the minimum allowable time [in hours] that the alternate source has the capability of providing its rated load without being refueled. *Level* defines the equipment performance stringency requirements'' (Flach, 1997, p. 3-62). For instance, in the case in which 60 seconds is the maximum allowable time for the load to be without acceptable electrical power, according to NFPA 70, the correct term is *standby power system,* whereas according to NFPA 110, the correct term is *emergency power system.* These terms are different but, in fact, refer to the same thing.

Controls for Simultaneously Unlocking Stairwell Doors Locked from Stairwell Side

In modern high-rise buildings, locking systems that automatically unlock during a fire emergency often are provided for stairwells in the building tower. During normal building operations these locking systems, primarily for security reasons, permit doors to be locked from the stairwell side. However, during a fire emergency, these doors either automatically unlock on activation of the building fire alarm system (i.e., *fail safe*)—and remain unlocked until the fire protective signaling system has been manually reset, or they are unlocked manually at the door or by pressing or turning a switch in the Fire Command Center.

Table 6.1 outlines the sequence of operation of fire life safety systems in a typical modern high-rise building. This is provided as an illustration of how fire life safety systems may be designed to operate. The actual mode of operation will vary according to the building and the requirements of the laws, codes, and standards that have been adopted by the authority having jurisdiction.

Other Building Systems and Equipment

The Fire Command Center may also contain other building systems and equipment as sanctioned by the authority having jurisdiction. There may be automatic dialing equipment to send signals from the building's fire life safety system to an off-site monitoring location, and keys for the fire department to access elevators and all locked areas of the building. The provision of building and elevator keys in the Fire Command Center is not to be confused with Rapid Entry Systems described in Chapter 5. (Rapid Entry Key Vaults or Fire Department Lock Boxes, as they are commonly called, are designed for emergency access from the *exterior* of a locked building.)

Building Emergency Procedures Manual

Many jurisdictions require that the Fire Command Center contain the Building Emergency Procedures Manual so that it is readily available for immediate reference by building emergency staff, fire departments, and other emergency response personnel. Chapter 11 details the content of a Building Emergency Procedures Manual. Also, the authority having jurisdiction may require certain equipment operating licenses and permits to be displayed in the Fire Command Center.

Before completing this description of fire life safety systems and equipment, with its particular reference to the Fire Command Center, it is appropriate to describe two other valuable types of equipment for the fire life safety of building occupants and property—*portable fire extinguishers* and *automated external defibrillators*.

Portable Fire Extinguishers

There are a number of portable fire extinguishers used in high-rise office buildings. They can be used as a first line of defense in handling fires of limited size. The selection of the most appropriate fire extinguisher depends on the specific hazard it is designed to address, the effectiveness of the fire extinguisher on that type of hazard, and the ease with which the extinguisher can be used. A portable fire extinguisher is ''a portable device, carried or on wheels and operated by hand, containing an extinguisher agent that can be expelled under pressure for the purpose of suppressing or extinguishing a fire'' (NFPA *Glossary of Terms,* 2001).

Classes of Fire and Recommended Extinguishing Agents

NFPA 10, *Standard for Portable Fire Extinguishers* (1998), classifies fires, depending on fuel type, as Class A, Class B, Class C, Class D, or Class K. Class D fires involve combustible metals such as magnesium, titanium, zirconium, sodium, lithium, and potassium. Because the occurrence of Class D fires is unusual in high-rise office buildings, neither they nor the dry powder used for extinguishment will be discussed.

The ensuing review of classes of fire and recommended extinguishing agents, followed by the description of portable fire extinguishers, has been compiled using NFPA 10 and the *Fire Protection Handbook* article ''Fire Extinguisher Use and Maintenance'' (Conroy, 1997, pp. 6-368–6-382).

Classes of fire in high-rise buildings and their recommended extinguishing agents are as follows:

1. Class A—fires in ordinary combustible materials, such as wood, cloth, paper, rubber, and many plastics.

Class-A-rated extinguishers are often used for ordinary building protection. The agents used are water-based, loaded stream, aqueous film-forming foam (AFFF), film-forming fluoroprotein foam (FFFP), multi-purpose (ammonium-phosphate-base), dry chemical, and halogenated types.

2. Class B—fires in flammable liquids, combustible liquids, petroleum greases, tars, oils, oil-based paints, lacquers, alcohol, and flammable gases.

Carbon dioxide, dry chemical, AFFF, FFFP, and halogenated extinguishers are recommended for Class B fires. Water should not be used on Class B fires except in the very rare case where the burning substance is known to be capable of being mixed with water. The water may then be applied in a spray form.

3. Class C—fires that involve energized electrical equipment and therefore require the extinguishing media to be nonconductive.

Carbon dioxide, dry chemical, and halogenated extinguishers are recommended for Class C fires. When the electrical equipment is de-energized, extinguishers for Class A or Class B fires may be safely used.

4. Class K—fires that involve cooking appliances and combustible cooking media such as vegetable or animal oils and fats.

Wet chemical-based and dry chemical-based extinguishers can be used for Class K fires.

Figure 6.21 shows the marking recommended by the NFPA to indicate the fire extinguishers suitable for use on each type of fire. ''These pictographs are designed so that the extinguisher's proper use may be determined at a glance. When an application is prohibited, the background is black and the slash is bright red. Otherwise, the background is light blue'' (Petersen, 1997, p. 6-389).

Most high-rise office buildings have Class A fire hazards in public access or common areas and within tenant areas; Class B and Class K fire hazards in

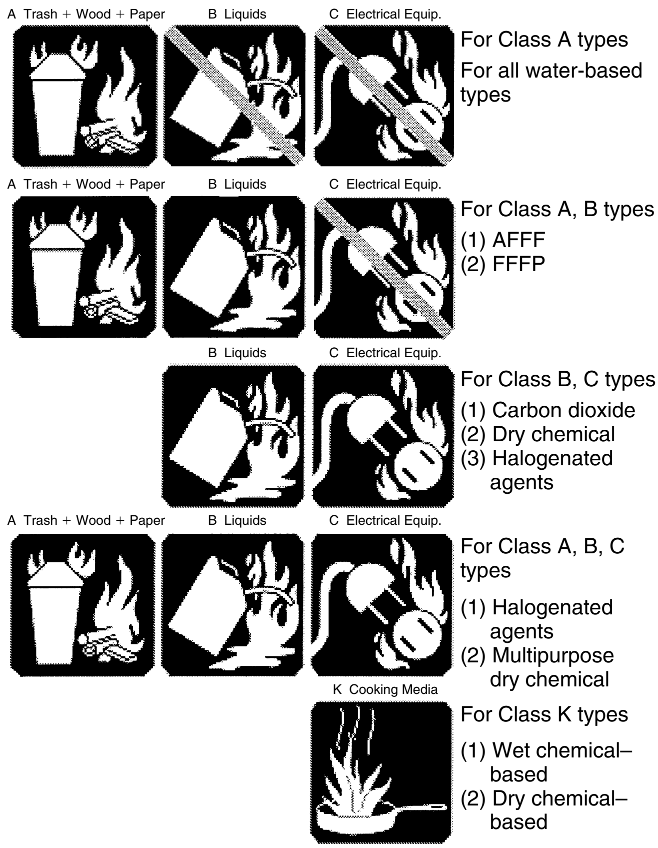


Figure 6.21 Markings recommended by the NFPA to indicate the suitability of a fire extinguisher for each type of fire. When an application is prohibited, the background is black and the diagonal slash is bright red. Otherwise, the background is light blue. The top row of symbols indicates an extinguisher for Class A fires; the second row indicates an extinguisher for Class A, B fires; the third row indicates an extinguisher for Class B, C fires; the fourth row indicates an extinguisher for Class A, B, C fires; and the bottom row indicates an extinguisher for Class K fires. Courtesy of NFPA 10, *Standard for Portable Fire Extinguishers* (1998), Figure B-2.1.

special areas such as kitchens; and Class C fire hazards in maintenance spaces such as electrical switch gear, generator, or elevator machine rooms and in tenant computer rooms and data centers. Fire extinguishers in these locations should correspond to the hazards of that area, have sufficient extinguishing capacity, and be immediately available in adequate numbers for persons trained in their operation.

The following sections describe the types of portable fire extinguishers that may be found in buildings.

Water-Based Extinguishers

Water-based extinguishers use water or water solutions that have a cooling, heat-absorbing effect on fires, particularly those of Class A. (The water solutions include antifreeze and wetting agents.) Older, inverting types of water extinguishers, such as soda-acid and cartridge-operated water, are no longer manufactured.

Water extinguishers that contain water, stored under pressure, are still in use today for Class A fires (Figure 6.22A). They can be used even in areas where temperatures may go below freezing, as long as they are charged appropriately or an antifreeze solution is added to the water. Wetting agents allow water discharged from the extinguisher to spread and penetrate more effectively by facilitating a reduction in the surface tension of the water.

How to Use

When using a water extinguisher, the first step is to place the extinguisher on the ground, hold the handle in one hand, and pull out the ring pin with the other hand. The ring pin normally keeps the operating lever locked and

(A) (B)

Figure 6.22 (A) Portable stored pressure water extinguisher. (B) Portable carbon dioxide extinguisher. Courtesy of Amerex Corporation, Trussville, AL.

prevents accidental discharge of the extinguisher. Then take hold of the hose and squeeze the operating lever (usually located directly above the handle) with the other hand. ''The stream initially should be directed at the base of the flames. After extinguishment of flames, it should be directed generally at smoldering or glowing surfaces. Application should begin as close as possible to the fire. Deep-seated fires [i.e., smoldering fires such as those involving upholstered furniture] should be thoroughly soaked and might need to be 'broken apart' to effect complete extinguishment'' (NFPA 10, 1998). NFPA 10, *Standard for Portable Fire Extinguishers* (1998, Table A-2-1), states that a 2½ gallon water extinguisher has a horizontal stream range of 30 to 40 feet and an approximate discharge time of one minute.

A person operating a water or water-based extinguisher may be injured, or the fire spread further, if the extinguisher is discharged on an electrical or flammable liquid fire.

Carbon Dioxide Extinguishers

Carbon dioxide extinguishers stop fires by using carbon dioxide to reduce the amount of oxygen in the atmosphere to the point where combustion cannot be supported. For a description of the gas, and its advantages and disadvantages in fire life safety, see the ''Carbon Dioxide Systems'' section in this chapter.

Carbon dioxide can be used to suppress fires involving gas, flammable liquids, electrical equipment, and, although less effectively, common combustible elements such as wood and paper. Figure 6.22B shows a portable carbon dioxide extinguisher.

How to Use

When using a carbon dioxide extinguisher, the first step is to place it in an upright position using its carrying handle, hold the carrying handle in one hand, and pull out the ring pin with the other hand. The ring pin normally keeps the operating lever locked and prevents accidental discharge of the extinguisher. Then direct the extinguisher as described below, taking care not to take hold of the discharge horn (because it may become very cold during discharge), and squeeze the operating lever (usually located directly above the carrying handle) with the other hand. When discharging the extinguisher on flammable liquid fires, the extinguisher should be aimed at the near edge of the flames and swept from side to side toward the back of the fire or aimed downward at a 45-degree angle toward the center of the area that is burning with the discharge horn kept stationary. The risk in discharging the extinguisher too close to oil and grease fires is that it may cause these substances to splash and thereby spread the fire.

For fires involving electrical equipment, the extinguisher should be aimed at the base of the fire. To prevent re-ignition, the equipment should be switched off promptly. NFPA 10, *Standard for Portable Fire Extinguishers* (1998, Table A-2-1), states that a 2½- to 5-lb hand portable carbon dioxide extinguisher has a horizontal stream range of 3 to 8 feet and an approximate discharge time of 8 to 30 seconds.

Halon and Halon Replacement Extinguishers

To extinguish fires involving expensive electrical office equipment such as computers, halon generally was used in the past. However, due to environmental concerns, halon has been severely restricted to essential purposes and production has ceased. Halon replacement extinguishers are now available.

The technique for using these types of extinguishers is very similar to that used for carbon dioxide extinguishers.

Dry Chemical Extinguishers

For a description of dry chemical agents, and an estimate of their function as fire extinguishers, see the ''Dry Chemical Systems'' section earlier in this chapter.

Ordinary dry chemical extinguishers (sodium bicarbonate, potassium bicarbonate, urea-potassium bicarbonate, or potassium chloride base) are primarily for use on Class B and Class C fires.

Multi-purpose (ABC) dry chemical extinguishers (multi-purpose ammonium phosphate base) are used primarily on Class A, Class B, and Class C fires. When introduced in 1961, multi-purpose dry chemical ''had the added advantage of being approximately 50 percent more effective than ordinary dry chemical on flammable liquid and electrical fires, and also was capable of extinguishing fires in ordinary combustibles'' (Petersen, 1997, p. 6-387).

How to Use

A dry chemical agent can be discharged from an extinguisher in two ways. These ways depend on the basic extinguisher design. The *cartridge-operated* extinguisher uses an external pressurized gas cartridge to discharge the dry chemical, while the rechargeable *stored pressure* extinguisher pressurizes the dry chemical chamber to discharge the dry chemical itself.

The operation of dry chemical extinguishers varies not only with extinguisher type, but also with fire type. Ordinary dry chemical extinguishers, when used on flammable liquid fires, should be aimed at the near edge of the flames and swept from side to side toward the back of the fire. There will be a sizable force generated by the initial discharge from the extinguisher; thus it should not be used at a range closer than 5 to 8 feet (1.5–2.4 meters) for flammable liquid fires, because it may cause the liquid to splash and thereby spread the fire.

Multi-purpose dry chemical extinguishers are used in the same manner as ordinary dry chemical extinguishers on Class B fires. However, on Class A fires it is important to attempt to coat all burning areas because the multi-purpose agent tends to soften and adhere to burning materials and creates a coating that smothers and isolates the fuel from air.

NFPA 10, *Standard for Portable Fire Extinguishers* (1998, Table A-2-1), states that a 1- to 2½-lb dry chemical (sodium bicarbonate stored-pressure) extinguisher has a horizontal range of 5 to 8 feet and an approximate discharge time of 8 to 12 seconds. These ranges and discharge times vary according to the type of dry chemical being used.

Because dry chemical is electrically nonconductive, it is also useful against Class C fires. However, in telephone switching rooms, computer rooms, and data centers, where there are sensitive electrical contacts and relays, its use is not recommended. Application in these areas may cause the equipment to malfunction. After any use of dry chemical, it should be removed as quickly as possible from the surfaces to which it has been applied, as it may be corrosive.

Wet Chemical Extinguishers

For a description of wet chemical agents, and an estimate of their function as fire extinguishers, see the ''Wet Chemical Systems'' section earlier in this chapter. Wet chemical extinguishers are primarily used in restaurants to combat fires in cooking oils and fats.

Positioning of Portable Fire Extinguishers

The distribution of the portable fire extinguishers throughout a building is determined by a physical survey of the areas that need to be protected. After the selection of the appropriate number and type of extinguishers is made, they should be located conspicuously in positions that make them readily available in the event of a fire. Often this will require that they be located in areas where there are specific hazards and along the normal paths of egress from a space to an exit.

The NFPA states in its codes that 75 feet (22.9 meters) is the maximum travel distance a fire extinguisher can be from Class A hazards; 30 to 50 feet (9.15–15.25 meters) for Class B hazards (unless the fire is in a flammable liquid of appreciable depth), for Class C hazards the distance will depend on whether the electrical equipment is a Class A or Class B hazard; and the maximum travel distance is 30 feet (9.15 meters) from a Class K hazard (NFPA 10, 1998, Chapter 3).

In high-rise office buildings, portable fire extinguishers normally are located in public access or common areas such as freight/service elevator lobbies and outside entrances to stairwells; within tenant spaces in kitchens, cafeterias, photocopier rooms, computer rooms, or data centers; and in maintenance spaces such as electrical switch gear, generator, and elevator machine rooms.

The extinguishers are mounted on hangers or brackets, kept in unlocked cabinets (Figure 6.23), locked cabinets (provided the latter can be accessed in an emergency), or placed on shelves. They should be mounted in such a way that the operating instructions are immediately visible and the extinguisher is readily accessible to the user.

Automated External Defibrillators

Automated (or sometimes, automatic) external defibrillators, or AEDs, are increasingly popular devices to allow nonmedical personnel, such as security staff, to administer potentially life-saving shocks to a person in cardiac arrest.

Figure 6.23 Portable stored pressure ABC multipurpose extinguisher housed in a cabinet. Photograph by Roger Flores.

> Sudden cardiac arrest is usually caused by an electrical malfunction of the heart called ventricular fibrillation (VF)—an ineffective quivering of the heart muscle that makes it unable to pump blood through the body. Once the blood stops circulating, a person quickly loses consciousness and the ability to breathe, and will die without effective treatment. The chance of survival drops about 10 percent each passing minute. Defibrillation is the definitive treatment for VF—but it is effective only if it reaches the victim in time. A brief but powerful electrical shock is applied to the person's chest, interrupting the VF and allowing the heart's natural rhythm to regain control. (''Cardiac response works for high-rises,'' May 1998, p. 47)

Due to the large numbers of tenants and visitors using high-rise buildings, a cardiac arrest may occur at any time. Placement of AEDs at strategic locations within a building offers a potential solution for administering immediate attention to a victim before emergency medical responders arrive. This is particularly important in tall skyscrapers where a victim could be stricken on an upper floor, a considerable travel distance away for responders entering the building at the ground level. Because they are small, portable devices, AEDs can be quickly and easily carried to the emergency scene.

First responders need to be properly trained to use this equipment. Certified courses are available through various agencies, such as the American Red Cross. Also, refresher training is recommended to help ensure that responders can effectively and efficiently use the equipment.

Potential liability exposure is being reduced by the passing of public laws that protect the person administering the AED treatment, as long as gross negligence or intentional misuse are not involved. An interesting viewpoint expressed by a representative of a commercial high-rise building owner and manager is, ''Because of AEDs' low cost and ease of use, we believe that having AEDs available will be the accepted standard and that within a few years there will be legal liability for businesses and properties that do not have AED programs'' (Schoettler, May 1998, p. 47).

Selection of Fire Life Safety Systems and Equipment

To assist in determining what specific systems and equipment are installed and operating at a building, one should consult the building engineer (particularly the chief engineer) or the operations manager of the site concerned, equipment manufacturer's operation and service manuals, architectural specifications, and the local building or fire department. Further expertise may require the services of a fire life safety consultant, such as a registered fire protection engineer. When changes are contemplated for any life safety systems, it is critical that only properly qualified and licensed personnel are consulted for professional advice.

Maintenance of Fire Life Safety Systems and Equipment

To maintain a building's fire life safety systems and equipment in an operable condition, the authority having jurisdiction will require periodic inspection, testing, and maintenance according to specified guidelines and for these activities to be thoroughly documented.

Buildings commonly employ a licensed contractor and support team specializing in life safety system operations to perform major testing and maintenance work. Typically in large high-rise buildings, building engineers do not have the time to perform these labor-intensive duties and sometimes they do not possess all the skills necessary to work on the diversity of equipment involved.

Summary

There are many types of fire life safety systems and equipment that may be found in high-rise office buildings. To maintain the systems and equipment in working order they must undergo periodic testing, inspection, and maintenance. To determine what is actually required at a specific site, one must review the law, codes, and standards that have been specifically adopted by the authority having jurisdiction.

References

Abbott, Richard J., ''Sprinkler systems, standpipe systems, detectors'' (*Fire Science Institute Office Buildings Fire Safety Directors Course*, New York, 1994).

American Insurance Association, ''Elevator emergencies,'' *American Insurance Association Special Interest Bulletin*, No. 55 (February 1974).

ASHRAE Handbook and Product Directory (American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc., Atlanta).

Bryan, John L., ''Fire detection systems,'' *Fire Suppression and Detection Systems* (Macmillan Publishing Co., Inc., New York, 1982).

''Cardiac response works for high-rises'' (*SECURITY* magazine, Highlands Ranch, CO, May 1998).

Clarke, Frederick B., ''Fire hazards of materials: an overview,'' *Fire Protection Handbook*, 18th ed. Arthur E. Cote, editor-in-chief (National Fire Protection Association, Quincy, MA, 1997).

Conroy, Mark T., ''Fire extinguisher use and maintenance,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

DiNenno, Philip J., ''Direct halon replacement agents and systems,'' *Fire Protection Handbook,* 18th ed. Arthur E. Cote, editor-in-chief (National Fire Protection Association, Quincy, MA, 1997).

Donoghue, Edward A., ''Building transportation systems,'' *Fire Protection Handbook*, 18th ed. Arthur E. Cote, editor-in-chief (National Fire Protection Association, Quincy, MA, 1997).

Flach, George W., ''Emergency and standby power supplies,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Gillespie, Angus Kress, ''It can't be done,'' *Twin Towers: The Life of New York's World Trade Center* (Rutgers University Press, Piscataway, NJ, 1999).

Hague, David R., ''Dry chemical agents and application systems,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Hall, John R., Jr., ''The U.S. experience with sprinklers,'' (*NFPA Journal,* November/December 1993).

Hall, John R., Jr., ''U.S. experience with sprinklers,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997), p. 1-14.

Hoover, Stephen R., *Fire Protection for Industry* (Van Nostrand Reinhold, New York, 1991).

Klaene, Bernard J., ''Ben,'' Sanders, Russell E., *Structural Fire Fighting* (National Fire Protection Association, Quincy, MA, 2000).

Martin, P.E., Wayne, M., ''Water supplies for sprinkler systems,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Mierop, Caroline, ''The heights of technology,'' *Skyscraper Higher and Higher*, (Institut Francais D'Architecture, Paris, France, 1995).

Moore, Wayne D., ''Automatic fire detectors,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

NFPA 10, *Standard for Portable Fire Extinguishers* (National Fire Protection Association, Quincy, MA, 1998).

NFPA 12, *Standard for Carbon Dioxide Extinguishing Systems* (National Fire Protection Association, Quincy, MA, 2000).

NFPA 13, *Standard for the Installation of Sprinkler Systems* (National Fire Protection Association, Quincy, MA, 1999).
NFPA 14, *Standard for the Installation of Standpipe, Private Hydrant, and Hose Systems* (National Fire Protection Association, Quincy, MA, 2000).
NFPA 17, *Standard for Dry Chemical Extinguishing Systems* (National Fire Protection Association, Quincy, MA, 1998).
NFPA 17A, *Standard for Wet Chemical Extinguishing Systems* (National Fire Protection Association, Quincy, MA, 1998).
NFPA 70, *National Electrical Code* (National Fire Protection Association, Quincy, MA, 2002).
NFPA 72, *National Fire Alarm Code* (National Fire Protection Association, Quincy, MA, 1999).
NFPA 90A, *Standard for the Installation of Air Conditioning and Ventilating Systems* (National Fire Protection Association, Quincy, MA, 1999).
NFPA 101, *Life Safety Code* (National Fire Protection Association, Quincy, MA, 2000).
NFPA 110, *Standard for Emergency and Standby Power Systems* (National Fire Protection Association, Quincy, MA, 1999).
NFPA *Glossary of Terms* from the National Fire Code (National Fire Protection Association, Quincy, MA, 2001).
Otis Elevator Company, *Tell Me About Elevators*, 6th printing (United Technologies, Otis Elevator Company, Farmington, CT, 1974).
Petersen, Marshall E., ''The role of extinguishers in fire protection,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
Post, Nadine M., ''Defending against bioterrorism'' (*Engineering News-Record*, McGraw Hill, New York, January 21, 2002, p. 12).
Schmidt, William A., ''Air conditioning and ventilating systems,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
Schoettler, John, as quoted in ''Cardiac response works for high-rises'' (*SECURITY* magazine, Highlands Ranch, CO, May 1998).
Shapiro, Jeffrey M., ''Standpipe and hose systems,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
Solomon, P.E., Robert, E., ''Automatic sprinkler systems'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
Southerland, Randy, ''Modernizing a legend,'' (*Access Control & Security Systems* magazine, Atlanta, GA, July 1999).
Sullivan, Richard C., ''New concept in vertical transport,'' (*Westsider 29,* Fall 1964). As quoted in Gillespie, Angus Kress, *Twin Towers: The Life of New York's World Trade Center* (Rutgers University Press, Piscataway, NJ, 1999).
Taylor, Gary M., ''Halogenated agents and systems,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
Webb, William, ''Review of Chapter 6,'' *Fire Life Safety Systems & Equipment* (Rolf Jensen & Associates, Deerfield, IL, 1994).
Wilson, Dean K., ''Fire alarm systems,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Additional Resources

NFPA Journal Buyer's Guide (National Fire Protection Association, P.O. Box 9101, One Batterymarch Park, Quincy, MA 02269-9101). A comprehensive listing of manufacturers and suppliers of fire life safety systems and equipment.

Further information on fire life safety systems and equipment may be found in the NFPA *Fire Protection Handbook* and the *ASHRAE Handbook and Product Directory*.

The following NFPA codes, standards, and recommended practices are suggested references to obtain additional information on fire life safety systems and equipment:

NFPA 10	*Standard for Portable Fire Extinguishers*
NFPA 12	*Standard for Carbon Dioxide Extinguishing Systems*
NFPA 12A	*Standard for Halon 1301 Fire Extinguishing Systems*
NFPA 13	*Standard for the Installation of Sprinkler Systems*
NFPA 14	*Standard for the Installation of Standpipe, Private Hydrant, and Hose Systems*
NFPA 14A	*Standard for Testing, Inspection, and Maintenance of Standpipe and Hose Systems*
NFPA 15	*Standard for Water-Spray Fixed Systems for Fire Protection*
NFPA 17	*Standard for Dry Chemical Extinguishing Systems*
NFPA 17A	*Standard for Wet Chemical Extinguishing Systems*
NFPA 20	*Standard for Installation of Stationary Fire Pumps for Fire Protection*
NFPA 22	*Standard for Water Tanks for Private Fire Protection*
NFPA 24	*Standard for Installation of Private Fire Service Mains and their Appurtenances*
NFPA 25	*Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems*
NFPA 51B	*Standard for Fire Prevention During Welding, Cutting and Other Hot Work*
NFPA 70	*National Electrical Code*
NFPA 70B	*Recommended Practice for Electrical Equipment Maintenance*
NFPA 72	*National Fire Alarm Code*
NFPA 75	*Standard for the Protection of Electronic Computer/Data Processing Equipment*
NFPA 80	*Standard for Fire Doors and Fire Windows*
NFPA 90A	*Standard for the Installation of Air-Conditioning and Ventilating Systems*
NFPA 92A	*Recommended Practice for Smoke-Control Systems*
NFPA 96	*Standard for Ventilation Control and Fire Protection of Commercial Cooking Operations*
NFPA 101	*Life Safety Code*
NFPA 110	*Standard for Emergency and Standby Power Systems*
NFPA 111	*Standard on Stored Electrical Energy Emergency and Standby Power Systems*
NFPA 921	*Guide for Fire and Explosion Investigations*
NFC	*Glossary of Terms*

The NFC *Glossary of Terms* is a compilation of definitions used in the National Fire Codes©.

7 *Security Policies and Procedures*

Security programs for high-rise office buildings, and for individual tenants, involve policies and procedures designed ''to prevent unauthorized persons from entering, to prevent the unauthorized removal of property, and to prevent crime, violence, and other disruptive behavior'' (American Protective Services, 1990, p. 17). Security's overall purpose is to protect life and property.

Access Control of Building Users

There are many different people who may, at any one time, try to enter a high-rise facility. They include building owners and management staff, building contractors (such as engineering, security, janitorial or maintenance, parking personnel, and elevator technicians), tenants, visitors, salespersons, tradespeople (including construction workers, electricians, plumbers, carpenters, gardeners, telephone repair persons, persons replenishing vending machines, and others who service equipment within the building), couriers, delivery persons, solicitors, building inspectors, vagrants, panhandlers, sightseers, teenagers on a lark, people who are lost, and mentally disturbed individuals. There also may be others who enter the building—or an individual tenant space—with the sole purpose of committing a crime.

It is primarily the building owner and manager and individual tenants who determine the access control measures for this wide spectrum of persons. These measures aim to sift out unwanted persons or intruders and at the same time provide a minimum of inconvenience to legitimate building users. When a security program is designed, factors such as the type of building tenancy, pattern of building use, and the time and day of building use (normal business hours or after hours, weekends, and holidays) need to be considered.

As explained in Chapter 1, a building can be single-tenant/single-use, single-tenant/multiple-use, multiple-tenant/single-use, or multiple-tenant/multiple-use. A single-tenant/single-use building is much more conducive to strict access control of employees and members of the public: standard security rules and procedures can be communicated and enforced more easily with employees of one tenant only. ''Access control may be tight and involve a badging system for regular employees and a careful monitoring of visitors through direct observation, or video displays and other devices'' (Geiger and Craighead, 1991, p. 11B). Implementation of strict access control for a multiple-tenant/multiple-use building, however, is much more difficult because each tenant may have different expectations of the degree of security the building should have.*

Once building management formulates access control measures, it and the security staff must clearly communicate these rules and procedures and obtain the support of tenants. Tenants, in turn, will need to decide what additional access control measures should be implemented for their own space. The tenant must then communicate both its own and the building's rules and procedures to its employees.

Building Access Controls

Building access controls include vehicle access to parking lots, garages, and loading dock/shipping and receiving areas; pedestrian access to building lobbies, elevator lobbies, and passenger and freight/service elevators; and access routes to retail sales spaces, restaurants, promenades, mezzanines, atria, and maintenance areas. Measures for controlling access to these areas vary from site to site, depending on building management's policy, but generally will incorporate some or all of those described in the following sections.

Vehicle Access to Parking Lots or Garages

Access to parking lots or garages may be gained by a variety of methods, including:

1. Entering at will
2. A vehicle presence detector embedded in the roadway, which automatically opens a gate or raises a gate arm
3. A parking attendant, a valet, or a security person stationed either at the point of entry or at a remote location linked to the point of entry by an intercom and/or a closed-circuit television (CCTV) system and a control device that opens a gate, raises a gate arm, or lowers a surface-mounted traffic barrier
4. A ticket (imprinted with the date and time of entry) obtained from a machine at the point of entry, that when withdrawn from the control unit automatically opens a gate or raises a gate arm
5. An electronic access card, key pad, or radio control device that opens a gate, raises a gate arm, or lowers a surface-mounted traffic barrier

When exiting the parking lot or structure, the driver usually will be required to submit to a similar procedure to that encountered on entry, make a monetary payment, or use a token. If an access card has been used, modern card access systems with entry and exit card readers incorporate an *anti-passback* feature. This prevents a card from being used again to authorize entry of a second vehicle before the first vehicle has exited the parking lot or structure.

*Prior to the September 11, 2001, terrorist destruction of the New York World Trade Center, access controls in multiple tenant high-rises were generally loose during normal business hours, Monday through Friday, and tightened up after hours. Since that incident, many buildings have implemented strict access controls 24 hours per day, 7 days per week (as detailed in Chapter 3).

Vehicle Access to Loading Dock/Shipping and Receiving Areas

Vehicles entering loading dock/shipping and receiving areas either may do so at will and park at whatever loading bays are available, or they may be permitted to enter and be directed to park in certain areas by a loading dock attendant who will then supervise subsequent loading or unloading. (Some buildings keep loading dock doors and gates closed between deliveries and pickups. Also, docks that are normally unattended may have an intercom or buzzer system, possibly in conjunction with CCTV, to allow drivers to summon building staff for assistance.)

Some higher-security buildings require vehicles, particularly vans and trucks, and especially those that will proceed to under-building loading dock/shipping and receiving areas, to undergo an on-street visual inspection before being allowed to enter (as a result of September 11, 2001, some businesses have utilized bomb sniffing dogs or a mobile x-ray vehicle to screen, prior to entry, vehicles, including trucks, for explosives).

For security purposes, the dock attendant normally will maintain a log or record of the vehicle license plate number, the driver's name and company, the time in, and the time out. Depending on building policy, the vehicle keys may remain in the vehicle, or be given to the dock attendant for safekeeping and to allow the vehicle to be moved if necessary. Movement of drivers and delivery persons usually will be confined to the loading dock/shipping and receiving areas. For this reason, rest areas, toilet facilities, and pay phones often are provided.

If drivers and delivery persons must enter the building for drop off or pick up of items, they are usually required to notify the dock attendant of the specific building area they will be visiting and the approximate duration of their stay. They may also be issued special identification badges and required to leave some form of personal identification (such as a driver's license) with the attendant. Since September 11, 2001, in many buildings the control of drivers and delivery persons has become much more stringent.

Pedestrian Access to Buildings

Pedestrians entering multiple-tenant/multiple-use buildings during normal business hours may simply enter at will and proceed to whatever area they desire, or be asked to submit to some form of credential procedure before they are permitted to enter the facility and proceed to various areas. The procedure in place may depend on the time (normal business hours or after hours) and the day (standard working days or weekends and holidays) that access is requested.

Normal Business Hours

During normal business hours, access control for some buildings and their common areas is relaxed and may consist solely of a security staff member or receptionist trained to observe both incoming and outgoing pedestrian traffic.

Persons who do not appear to belong in the business environment may be challenged with a simple ''May I help you?'' Specific questions can then determine the particulars—for example, whether the person is a tenant, is visiting a tenant (if so, which one?), is delivering or picking up items (if so, to whom? from whom?), or is servicing or inspecting equipment in the building (if so, where? at whose request?). These questions not only help screen out intruders with no legitimate reason for entering, but also assist persons who need directions to their destination.

The degree of access control permitted by building policy will determine the percentage of unwanted persons successfully screened out. ''The security program should be designed just tight enough to screen out as many intruders as it takes to reduce problems to the level that can be accepted. This means that a useful security program will rarely screen out *all* intruders'' (American Protective Services, 1980, p. 11). If all intruders were screened out, it would undoubtedly result in what could be considered unacceptable delays or inconvenience to the legitimate occupants and visitors of the building. (However, since September 11, 2001, many buildings have implemented such strict access controls for all incoming persons 24 hours per day, 7 days per week.)

Access control to building maintenance spaces—mechanical rooms and floors, air-conditioning rooms, telecommunications and utilities access points, elevator machine rooms, janitorial closets—and areas under construction or renovation usually will be tight. Depending on building policy, persons accessing these areas may be logged in and out, required to wear special identification badges, given keys to a particular area (although issuing keys to vendors or visitors can be a security risk), or provided a building escort. Some contractors servicing certain types of equipment in specific building areas may be permitted to install their own locking devices at access points leading to this equipment (see further comments in the ''Key Points to Consider'' section later in this chapter). Main electrical switchgear and power transformer rooms are usually deemed such a life safety risk that not even building personnel are issued keys to these areas.

After Normal Business Hours

After normal business hours, access control to all areas should be strict. The obvious way to provide off-hours access to a high-rise facility would be to furnish keys to all building occupants or to those who need to enter after hours. This approach, however, can have disastrous consequences proportional to the size of the building and the number of occupants. A gigantic workload and expense can be created by lost keys, keys not returned by departing tenant employees, and the necessity of re-keying building entrances and reissuing keys to building key holders every time a key has gone astray. In addition, there may be the problem of unauthorized duplication of keys. To avoid all this, most high-rise buildings never issue building access keys to tenants but rely on some way of verifying a person's right to enter the building. This verification may involve the following procedures.

Visual Recognition

Building security staff or a receptionist may verify on sight a person's right to enter. Several problems may result, however, from this form of verification. For example, someone who closely resembles a person authorized to enter may be admitted in error. Also, particularly if the building is large with a high population, it will be difficult for security staff or the receptionist to learn to recognize all persons authorized to enter. If there is a change or substitution of the security staff or receptionist, the new person will not be familiar with the persons authorized to enter. This may also result in the unnecessary questioning of authorized persons who normally are never challenged and subsequent complaints to building management. Finally, if the security staff is distracted by another duty, an unauthorized person may gain entry without being observed.

After-Hours Authorization Documents

A document (either a letter, a memorandum, or an e-mail) listing those authorized for after-hours access is provided in advance to security staff at the building entrance. Persons requesting access will identify themselves to building security staff. Security will check their name (which should be confirmed by a driver's license or other photo identification) with the names listed in the document. In many buildings, tenants will provide management with a written request on their own stationery listing the names of the persons involved and the period of time after-hours access is permitted. Building security staff or the receptionist often will set up a file sorted alphabetically by tenant name, or by the last name of the person to be granted access, to minimize time spent searching for the appropriate authorization.*

Building security staff must thoroughly check all documents authorizing access to ensure that the decision to grant access is valid. An unusual example illustrates this point. Building management of a major Los Angeles high-rise gave building security staff a memorandum to allow access of a pest control company to a specific tenant suite on a particular Friday night. The pest control company failed to appear on the night authorized but did arrive the following Monday evening. Building security staff did not thoroughly check the paperwork and permitted the pest control company to enter and carry out their work. The next business day several of the tenant employees became ill from the lingering effects of the pest treatment. The reason for authorizing entry on Friday evening had been to allow 2 days for any residual pesticide to dissipate. Permitting the work to occur on a Monday evening negated this precautionary safety measure.

After normal business hours most tenant areas are locked, so once a person's right to enter a building is verified, that individual may gain entry

*To handle visitors, some buildings are using Web-based visitor management systems. Tenants authorized by building management to use such a system can dial-up a password-protected website and specify the name of the visitor and the date and time the person is permitted entry. On arrival at the building, security staff or a receptionist verify similarly using a computer that the visitor is authorized to enter. In some larger facilities a separate visitor center is provided to facilitate the processing of visitors.

to an office by using a key he or she has previously obtained, or one that has been left ahead of time with the document authorizing entry. The latter practice is not recommended because it can lead to misplaced or lost keys. Alternatively, if someone is present in the tenant space, they may be telephoned and asked to come to the building lobby to provide admittance and escort the person.

In the case of providing access to maintenance areas or other locations with restricted access, building security or engineering may be required to escort the individual concerned. Some buildings have a permanent list of local and state agencies whose inspectors have authorized entry, but it is absolutely critical to thoroughly verify such persons' identification, and to make building management aware (if possible) of these persons' presence before they are granted entry. It is important to escort anyone claiming to be an inspector while he or she is in the facility. On occasion, professional burglars posing as local or state inspectors have been granted entry to buildings.

Building Identification Cards, Passes, and Badges

Sometimes a building identification card, pass, or badge is used to verify the bearer's identity and privilege to enter after hours. The identification should be numbered sequentially, list the person's name and the company's name, and contain the person's signature, a color photograph, and in some instances an expiration date. It should be laminated for durability, and be tamper-resistive (this will not necessarily eliminate the potential for the plastic envelope being cut and the card, pass, or badge being modified and then re-laminated). The development of laser technology to create holograms (three-dimensional images) may lead to their use for building identification cards, passes, or badges, but the present high cost does not currently justify it. In case it is lost, the card, pass, or badge can include text such as:

IF FOUND DROP IN ANY MAILBOX. P.O. BOX NO.___, CITY & STATE. POSTAGE GUARANTEED.

The credential can be presented by the bearer to security staff for entry to the building or used to verify identification within the building. However, if the card, pass, or badge is not thoroughly checked for details, this form of access control soon loses its effectiveness. Also, it must be retrieved from holders whose employment is terminated, or else it might remain in use after the person no longer has a legitimate reason for gaining access to the building.

Building Access Cards

Building access cards usually provide after-hours access by operating an entry door to the building. An intercom, a telephone, or a CCTV camera also may be provided at the point of entry. If there is a problem using the card, the person requesting access can use the intercom or telephone to communicate with building staff or an off-site central monitoring station. If the person's right of entry is confirmed, the monitoring staff can grant access remotely. Some high-rise buildings have a card reader installed at the main lobby security desk. Tenants entering the building are asked to insert, swipe, or place their building card in proximity to the card reader (depending on the type of reader). If a green light is displayed, the tenant is permitted to proceed into the building and the event is recorded in the system database. This system can be used to generate its own after-hours access register or log (described later). In some buildings, when the tenant card is validated, elevators are automatically released for travel to floors that the cardholder has the right to access.

If this card access system is installed in passenger and freight/service elevator cars, the same card may be used to provide controlled access to building floors. Some systems can be programmed so that during certain times, the elevator car will only respond to a particular floor if an authorized access card is used. The person will enter the elevator, insert, swipe, or bring the card into proximity to the card reader, and select the desired floor by pressing the appropriate button on the floor selection panel.

Building access cards can feature the same data, tamper-resistive protection, and lost-card notice as identification cards, passes, or badges. However, some buildings, for security reasons, prefer no details be listed on the card apart from its sequential number and, if it is used with an insertion or swipe-type card reader, an arrow depicting the correct way to insert or swipe the card. Then, if a card is lost, there are no identifying marks to indicate where it may be used. An advantage of a building access card is that if the employment of a cardholder is terminated, the card can be deactivated immediately by computer without the need to retrieve the card itself.

After-Hours Access Register or Log

Whatever access control procedures are used, many high-rise buildings maintain an *after-hours access register* or *log* to record after-hours access activity. In this log details such as the person's name (printed for legibility) and signature, the name of the company they represent or tenant they are visiting, the date, and time in and out are included. In case of an after-hours building emergency, such a log can be used to help ascertain who is in the building. However, the register or log does not provide a record of *all* persons in the building after hours, because some persons will have accessed the building before the access control log was in use. To determine exactly which tenants are in the building after hours, it would be necessary either to telephone or to personally visit every tenant. Such a procedure, particularly in large high-rises, is not considered practical.

Right to Pass Signs or Plates

Signs or sidewalk plates, generally located outside the property, may clearly state:

> "RIGHT TO PASS BY PERMISSION, AND SUBJECT TO CONTROL, OF OWNERS" or "PERMISSION TO PASS REVOCABLE AT ANY TIME,"

and they may include a reference to the code that states this right (Figure 7.1).

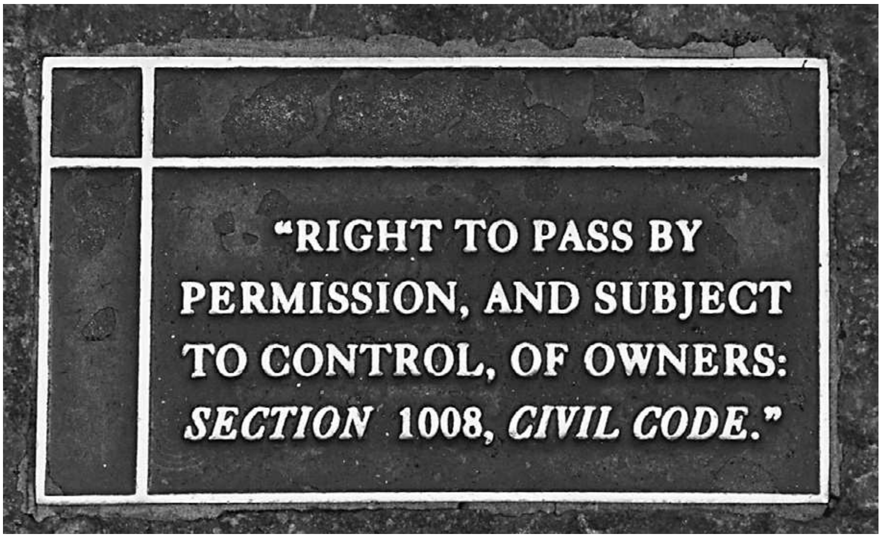


Figure 7.1 An example of a sidewalk plate. Photograph by Roger Flores.

If a person is discovered who does not have a legitimate reason for being in the building, then the right to remain may be revoked by the owner, manager, or agent acting on behalf of the building. After being told to depart the premises, those who refuse to leave may be arrested for trespassing. Also, anyone reentering a building after having been warned that he or she is not authorized to enter may be treated as a trespasser.

Tenant Access Controls

Tenant access control involves *rented* or *assigned occupancies*. These are leased or owner-occupied spaces on various floors and are either open to public access during normal building hours or restricted to identified and authorized persons. The access control measures for tenant areas will vary from tenant to tenant, depending on their type of business activity, the design of the tenant space, and the individual tenant's policy.

In some cases, visitors entering tenant space may simply enter at will and, in some instances, proceed directly to any area in the tenant space. However, in today's security-conscious world, it is more likely that the visitor will be greeted by someone and asked to submit to some form of verification procedure before being permitted to enter the tenant space.

Tenant Space Access during Normal Business Hours

Tenants in most high-rise office buildings practice some form of access control to their space. For larger tenants, often a receptionist is present at the main point of entry to act as the first line of defense.

Tenant space layout varies from tenant to tenant; however, if possible, it is helpful to channel incoming persons through one area and keep all other access points properly secured. Some tenants establish a staffed reception area that is separated by physical barriers from the interior tenant space. Once a person has been cleared for admittance, the receptionist can allow entry.

Large companies that occupy several full floors served by one elevator bank can establish access control to their elevator bank at the street level. If there is no single elevator bank serving the tenant floors exclusively, the elevators can be programmed to stop at only one floor of that particular tenant. A reception area at this point can be used to control access to that tenant's other floors by way of an internal staircase or card-controlled access to the elevator. It is the responsibility of the receptionist (often in addition to answering telephones and handling other duties) to monitor both incoming and outgoing pedestrian traffic. Only if the receptionist is properly trained to screen and handle incoming persons will the security of the space be enhanced.

The receptionist must question people of all types to determine whether they are authorized to enter. A ploy in office buildings has been for a person to pose as a photocopier or telephone repairperson and, after gaining entry, proceed to steal purses, billfolds, petty cash, credit cards, and other small valuable items left unattended in the tenant space. These criminals are aided by two common practices: businessmen often hang their suit coat or jacket, containing their billfold, on a clothes stand or behind their office door; businesswomen, similarly, sometimes drape their handbag on a chair or leave it under their desk. Such items can then be easily stolen. Another trick has been for an intruder, having gained access to a tenant space, to memorize a name from a desk or a directory board. If challenged by an occupant, the intruder simply states the name to avoid detection:

"Oh, I'm looking for Mr. Searcy!"

Unfortunately, on hearing such a reply, many an unknowing occupant has escorted the person to Mr. Searcy's desk, and left them there to continue with their deception. Such criminal behavior can occur more easily on *open* floors, where elevator lobbies open into corridors which, in turn, open without any form of barrier into the main floor areas (Figure 7.2).

Once it is established that a person is permitted to enter tenant space, the receptionist should arrange for entry in a manner that does not compromise security. The person may be issued a temporary "visitor" or "contractor" identification badge for the day and asked to fill in and sign the appropriate register. Then the receptionist may telephone the employee who is expecting the visitor to come to the reception area to escort the guest. Also, some large firms provide a mailroom with a separate entrance where all couriers or others dropping off or picking up merchandise from the tenant space can be directed. This eliminates the need to separately escort these individuals.

Figure 7.2 An example of an open floor viewed from the passenger elevator lobby. Photograph by Roger Flores.

Unwanted Solicitors

Receptionists also can play an important role in building security by reporting solicitors they encounter. As defined in the United States, *solicitors* are persons who come to facilities and attempt to sell their wares to tenants. They often come to buildings with items for sale secreted in a bag or a briefcase. If they can obtain entry through the building lobby, they will open up the container, take out their product, and proceed from floor to floor, tenant to tenant, touting their merchandise. Even though many solicitors may be legitimate, their presence can be disruptive to tenant business; furthermore, many criminals pose as solicitors. If a tenant receptionist detects an unwanted person such as a solicitor or someone who is behaving suspiciously, it is helpful to security staff if the receptionist can delay the person as long as possible until security assistance arrives. If possible to arrange, it is better to have a co-worker call for security personnel out of the hearing of the solicitor. Using a signal or code phrase—''Sarah, could you watch the phones for me? I'm going to be busy with the flower seller for a few minutes''—can successfully delay the individual until security staff arrive.

One way to detain a solicitor is to feign interest in the product, call other ''interested'' employees to look at the merchandise, and thereby preoccupy the solicitor. Suspicious persons may be detained by carrying on a friendly conversation, offering an employment application, or using some other ruse. Simply telling the solicitor that soliciting is not permitted generally is not enough. Having left that particular tenant they will often then proceed to other tenants.

For the protection of all tenants, it is best to have security personnel escort the solicitor out of the building. The tenant should never buy anything the solicitor is selling. To do so provides an excuse for the solicitor to attempt to return to the building. If it is not possible to delay the solicitor, it is helpful if the receptionist can at least notify security staff as soon as possible and supply a good description of the person involved, including physical characteristics as well as clothing.

Tenant Security Systems

Some tenants have installed their own access control systems—electric locks, mechanical or electrical push-button combination locks, card-operated locks, or biometric system-operated locks—that control the operation of entry door(s) to tenant areas. Sometimes, CCTV systems, intercoms, and intrusion detection systems are used in conjunction with these devices. When considering a system, the local fire authority having jurisdiction should be consulted to determine whether such an installation is permitted by local and state codes—this is particularly important when the access control devices are to be installed on doors leading directly from elevator lobbies to the tenant space. These doors involve paths of egress during emergency evacuation and therefore require special locking arrangements permitted by the local codes.

Tenant Space Access After Normal Business Hours

After normal business hours in most high-rise office buildings, access control to all areas is strict. Perimeter doors to the tenant space usually are locked when normal business is completed. Each tenant needs to establish a specific policy and procedure for access after this time. One possible solution is to furnish keys to all employees who require access. This approach, however, can lead to the same problems discussed earlier, under ''Pedestrian Access to Buildings.'' Instead, some tenants issue keys only to a few select individuals. This alleviates some key control problems but creates the need for one of these persons to be present when special after-hours access is required. In some instances, building management has permitted some tenants to leave keys with security staff for special after-hours access. The tenant's employees must then return the keys to their representative on the next business day.

There is no clear-cut answer to the issue—factors such as the number of employees requiring after-hours access, the frequency of after-hours access, and tenant management's attitude toward its employees, as well as building management policies, all need to be taken into consideration for a well-defined policy to be formulated. As noted previously, some tenants have installed their own access control systems to operate entry doors to the tenant area, possibly in conjunction with CCTV systems, intercoms, and intrusion detection systems. Other large companies who have around-the-clock operations provide security staff or receptionists to control after-hours access. Some maintain an after-hours access register or log similar to that required for the building itself (as described earlier in this chapter). If the tenant is a theater or restaurant that is open after normal business hours and on weekends and holidays, there will be a need to provide easy access for the patrons and additional measures to ensure these persons do not stray into other building areas.

Building or Office Creeper

For buildings that do not maintain strict access control during normal business hours, a ''building or office creeper'' may slip through the net. For example, late in the afternoon, dressed in conservative business attire, the creeper might confidently enter through the main lobby and nonchalantly pass by building security staff. Taking an elevator to an upper floor, this ''businessperson'' enters a restroom and quietly sits in a cubicle until the tenants on the floor are about to close business for the day. He or she then exits the restroom and systematically walks the corridors checking doors to see if they have been secured. On finding one unlocked, the creeper enters the tenant space and proceeds through it looking for small items such as laptop computers, personal data assistants, cash, checks, credit cards, and other things that can be easily placed in a jacket or briefcase. On being challenged in one suite by building janitorial staff, a tenant business card (which moments before was lifted from an executive's desk) is politely presented with the statement of gratitude, ''I'm so glad to see that even the janitorial staff in our building are so security conscious!''

After 15 minutes of work, the creeper descends to the lobby in a passenger elevator and warmly waves to the security staff as he or she exits the building. To prevent this from happening, tenants should ensure that all perimeter doors not supervised by their staff be kept locked at all times.

Locked Doors

It is important that tenants *never* open their doors after normal business hours for anyone not personally known to them. In a Los Angeles high-rise office building, a temporary female employee working alone after hours one night opened the door to a man claiming to be the window washer. The intruder raped the woman, then even had the nerve to say goodnight to the security officer posted in the lobby. Tenants should be educated that if someone belongs in their space, either building management or tenant management would have already provided them the means of obtaining access.

Escorts of Building Users

Escorting of people may be done for a variety of reasons. It may be to accompany individuals for the purpose of protecting them or the property that they are carrying. It also may be to show a person where to go, or to ensure that they do not remove property. In the high-rise setting, building users can be escorted to and from the building and within tenant space.

Escorts to and from the Building

Escorts to and from a building usually occur after normal business hours. Security staff generally conduct these escorts. When tenants finish business, their employees, frequently females, may request building security to escort them to unsupervised areas of the property, such as parking structures. Building policy should dictate how, when, and where the escorts are to be conducted. For liability reasons, escorting people off site, particularly across streets, is not encouraged.

Escorts within the Building

Building policy may require that persons needing access to certain maintenance spaces and areas under construction or renovation be provided with an escort to accompany them whenever they are in these areas. Building engineering or security staff may be required to provide such escorts.

Also, janitorial staff may require escorts when they are removing trash material from building floors and transporting it to trash compactors and dumpsters. The purpose of the escort is to reduce the possibility of janitors transporting stolen items along with the trash from tenant floors, and depositing them in places where they can be picked up later.

Escorts within Tenant Space

It is usual for visitors, such as salespersons, tradespeople, couriers, and delivery persons, to be escorted within tenant space. This will depend on the type of business the tenant conducts, tenant policy, and staff availability. For example, a tenant may require an employee to accompany such persons at all times while they are inside tenant space, or just accompany them to particular areas and leave them unsupervised to carry out the tasks they have been authorized to perform.

Property Control

There are various property acceptance and removal systems that can be implemented by building managers and tenants to provide some control over the property that on a daily basis moves in and out of office buildings and tenant areas. The degree of control will vary from building to building and tenant to tenant and will depend largely on the policies established by building management and the tenants themselves. The effectiveness of these policies is impacted by how thoroughly they are communicated to building staff, tenants, and occupants; how strictly they are enforced; and the support afforded the program. It is sometimes difficult to implement strict property control measures in a multiple-tenant/multiple-use commercial office building, primarily because each tenant may expect a different degree of security.

Objectives of a Property Control System

According to American Protective Services (1980, p. 24), the objectives of a property control system are threefold:

- *To prevent stolen property and other unauthorized items from leaving*. Stolen property may include computers (personal, laptop, and notebook), personal data assistants, fax machines, calculators, and office equipment. An unauthorized item might be something like a sensitive or classified document that is not to be removed from a certain area or from the building.
- *To prevent dangerous items entering*. Bombs are the usual concern, but other items such as cameras or firearms might be prohibited. (As a result of September 11, 2001, metal detectors and x-ray systems, although not in common use in high-rise office buildings, are deployed in some sensitive facilities as a screening measure for weapons and explosive devices concealed on people and contained in parcels, packages, and carried possessions.)
- *To prevent unnecessary or disruptive delivery traffic*. By keeping out misdirected deliveries, unnecessary traffic is avoided. By routing deliveries through proper entrances, such as loading docks and freight/service elevators, disruptive traffic is avoided and, in some cases, the building and passenger elevators are protected against damage from hand trucks and bulky crates. By intercepting deliveries at these entrances to the building, it may be possible to detect intruders posing as delivery persons.

Property Removal Pass System

Unauthorized removal of property from high-rise buildings can be controlled to a degree* by requiring *property removal passes* for business and personal items taken through an egress point controlled by security staff. The time when the property removal pass system is to be in effect is set by building management and communicated to the tenants. (Some buildings only permit the checking of property removal after normal business hours.) Property removal passes can be supplied by building management to key tenant representatives who then supervise their distribution to tenant employees and visitors on an as-needed basis. The passes may vary both in design and in the information recorded on them.

Required Information for a Property Pass

For the property pass to be of value in the security program, it should address at least the following areas of information:

- Name and signature of the person authorized to remove the property
- Name and room or suite number of the tenant or company from whom the property is being removed

*Small items can be easily concealed on a person or in a briefcase or carrying bag. Also, a thief working in a building can circumvent a property control system by using commercial mail services to send stolen items out from the building. Unless electronic tracking of assets is provided, a thief can thereby bypass the building system.

- Printed name and signature of the tenant representative who has authorized the property removal
- Brief description of the property, including any model, serial, or asset tag numbers
- Date the property will be removed
- Date and time of removal of the property
- Signature of the person (usually a member of the building security staff or a receptionist) collecting the pass and permitting removal of the property

Property passes should be sequentially numbered and a record kept of which tenants received which numbered passes. They should also be in duplicate (following the removal of the property, the original is returned by the building security staff to the tenant representative and a copy is kept on file by the building security department).

A sample property removal pass for a high-rise office building is shown in Figure 7.3. After the authorized tenant representative has signed the form, any blank lines on the pass should be crossed out to prevent unauthorized entries.

Whenever building security staff receive property removal passes, they should always scrutinize the pass to ensure that it is complete and contains all the necessary information. The identity of the person actually removing the property should be confirmed by means of a valid driver's license or other photo identification.

It is best if each tenant has already provided an authorization letter containing sample signatures of each representative authorized to sign a property removal pass. Building security staff can then compare the signature on the pass with the signature on the letter. If it matches, security will sign the pass, keep it for distribution, and permit removal of the property. If it does not match, security personnel will keep the pass and may attempt to contact either an authorized tenant representative or building management to resolve the matter. Such a system can be effective in controlling the removal of some business and personal property. However, as previously mentioned, many computer-related items are small enough to be carried out unobserved in a carrying case, or, in the case of personal data assistants, in a pocket.

Permanent Property Pass

Some high-rise buildings permit the use of a *permanent property pass*. This pass eliminates the need to continually issue property passes for personal or company property that is being frequently removed from the building. The permanent property pass is similar both in design and recorded information to a regular property pass, except that it can be used repeatedly for the time stipulated on the pass. The card is often laminated to prevent damage and affixed at all times to the item being brought in and out of the facility. Building security staff should keep a photocopy of each pass and a log that documents all such passes in use. Of course, if the pass is lost or the tenant cancels its usage, building security must be immediately notified.

Pass No: 000001

PACIFIC TOWER PLAZA

PROPERTY REMOVAL PASS

Name of Person Removing Property: ______________________________

Signature of Person Removing Property: ______________________________

The following material/items are authorized for removal on: (Date)______________________

____

____

____

(Brief description of the property, including any model, serial, or asset tag numbers)

Person Authorizing Removal

Signature: ______________________________

Printed Name: ______________________________

Tenant or Company Name: ______________________________

Room/Suite Number: ______________________________

Person Allowing Removal and Collecting Pass

Signature of Building Security Staff: ______________________________

Date of Removal: ____________________ Time of Removal: ____________________

White Original--Tenant Copy Yellow Copy--Building Security

Figure 7.3 Sample property removal pass.

Asset Tracking Systems

As outlined in Chapter 5, small asset tags—some being embedded into desktop and laptop computers at the time of manufacture—can be assigned to an asset that is permitted to leave a high-rise building. Integrated with a building's access control system, asset tracking can be utilized to control the movement of computer equipment and other assets from the building.

An asset tagging and tracking proximity system ''allows free egress when authorized assets are removed, but prevents unauthorized removal of property. Without electronic tracking, assets can be removed by concealing them in a briefcase, package or gym bag'' (Macklowe, February 1998, pp. 21, 22). This system can also be adapted to screen assets being mailed out of a building through a central shipping area such as the loading dock.

Dangerous or Illicit Items

To prevent someone from entering the building with dangerous or illicit items is not as easy a task as it would at first appear. Bombs are a concern. As was demonstrated by the New York World Trade Center 1993 bombing incident, vehicles entering into parking garages can carry explosives. This subject is discussed in Chapter 10.

As a result of September 11, 2001, metal detectors and x-ray machines, although not in common use in high-rise office buildings, are deployed in some sensitive facilities as a screening measure for weapons and explosive devices concealed on people and contained in parcels, packages, and carried possessions; also, some businesses are utilizing bomb-sniffing dogs or a mobile x-ray vehicle to screen, before entry to building areas, vehicles, including trucks, for explosives.

Other items such as illegal drugs and chemical and biological weapons might easily be secreted on a person and brought into a building. Searching persons, suitcases, briefcases, handbags, carryalls, and so on, is not an acceptable practice in today's high-rises, although, as is discussed later in this chapter, many buildings do permit visual inspections of items carried by janitorial staff.

Couriers and Delivery Persons

In many facilities, couriers and delivery persons have free access to a building to conduct deliveries to and pickups from tenants of letters, parcels, and packages.

However, there is an alternative for owners and managers who desire to prevent unnecessary, disruptive, or undesirable delivery traffic in their facilities. Some buildings have instituted special programs whereby outside couriers, on arrival at a building, are directed to a separate entrance, such as the loading dock or a central mailroom. At that location, couriers employed by a contract courier or security company assigned to the building sign for the items and deliver them within the building by way of the freight/service elevators. When items are to leave the building, these same building couriers pick up the articles from the tenants, bring them to the central location, and then outside courier companies sign for them before taking them from the facility. (As a rule, regular courier services such as Federal Express, UPS, DHL, Airborne Express, and so on, who performing regular, multiple deliveries in a building, are permitted to perform their own pickups and deliveries. Special deliveries or pickups can be facilitated by providing temporary badges for outside couriers to enter or by providing an escort for these couriers while they are in the building.)

Such programs have been very successful. When dedicated building courier or security staff perform multiple deliveries and pickups from tenants, the overall number of couriers roaming throughout a building is diminished: a valuable security advance when a million-square-foot high-rise office building may have 300 or more individual deliveries per normal business day. In addition, the number of couriers using elevators is reduced. Also it can enhance security by providing an added presence in the building (particularly if security staff are used), and because these building couriers should have already been ‘‘security-vetted’’ (i.e., a background check of these individuals has been conducted), there is less chance of possible theft or vandalism than when using outside courier services. Delivery to secured or normally ‘‘locked off’’ floors is also easier because dedicated building couriers can more readily be entrusted with the access codes or cards that allow them to enter such restricted areas.

Like any well-run operation, such programs need to be meticulously documented to provide an audit trail to track deliveries and pickups and ensure that these tasks are conducted in a timely manner. If there is a question about the time property was picked up or delivered, or about the individual who signed for it, accurate records should be immediately available for review. Some individual tenants, particularly larger ones that occupy full floors and multiple floors, have addressed the issue of outside couriers roaming within their space by establishing a separate mailroom from which only tenant messengers perform all deliveries within the tenant area.

Package Acceptance Policy

During normal business hours, tenants usually handle their acceptance of packages. For packages delivered after hours, their acceptance or rejection will largely depend on the policy established by the building owner or manager. For security and safety reasons, most commercial office buildings do *not* permit after-hours acceptance of packages by security staff. The building does not want to accept the responsibility and potential liability of accepting packages the tenant may not want to have accepted; also, these packages may contain dangerous or illicit items. Some buildings do permit the acceptance of after-hours packages on certain occasions and under special circumstances. This will usually require a written request by the tenant and an explicit understanding that the building and its agents are absolved from any liability resulting from accepting the package on behalf of the tenant.

Lost and Found Property

Handling lost and found property is an often-neglected but critical part of an effective security program. Most people can recall the anguish they felt on discovering that a valuable personal possession or business item was missing. Likewise, one can remember the exhilaration at being contacted and informed that the missing property had been found and was available for pickup.

If property is lost in a high-rise building and is subsequently found and handed to building security staff, the item(s) must be kept in a secure place, and, if possible, expeditiously returned to its rightful owner. Such action can considerably enhance the trust and confidence that occupants and visitors in high-rise buildings will have in the building security operation. Just the opposite will be true if a tenant learns that the found item was handed to building security staff and was then lost or went missing.

Lost and Found Property Log

Building security staff should maintain a list of lost and found items in a *lost and found property log*. The log should contain details such as the following:

- A brief description of the property, including any serial or asset tag numbers
- The date, time, and place the property was lost or found
- The identity of, and means to contact, the person who lost or found the property
- If the property is claimed, the identity of, and means to contact, the claimant and the signature of the person who received the property
- The name of the security staff member who took the report of the lost property, logged in the found items, or handled the return of the property to the rightful owner

Handing Over to Local Authorities

If the lost property is particularly valuable or sensitive, it may be necessary for the local law enforcement agency to be contacted; if the property is later handed over to them, this fact, including the identity of the receiving law enforcement officer, should be noted. A receipt for the property should be obtained. Local and state laws often determine the handling of property.

In California, for example, section 2080 of the California Civil Code does not require a person to take charge of found property, but if they do, they can be sued for the negligent handling of it. The law provides further that if the owner of lost property is known, the property must be returned to that owner. If the owner is not known, and the property has a value above ten dollars, the property, within a reasonable time, must be turned over to the local police (American Protective Services, 1993, p. 4).

Some localities allow found property, when its owner is unknown and its value is below a certain amount, to be distributed to local charitable organizations. Others, after a certain waiting period, auction the property or allow the finder to assume ownership of it.

Trash Removal Control

There are a number of controls that can be placed on trash removal from tenant space and from a building. The design and implementation of controls will depend largely on the specific cleaning operations in effect at the building. Some operations ''gang clean'' using a team (including dusters, cleaners, waxers, polishers, and trash removers) to clean tenant spaces and restrooms on a series of floors. Others assign specific janitorial staff to perform all functions on particular floors. From a security standpoint, the latter is preferable because regular staff are more likely to detect unauthorized persons who do not belong in a particular tenant space, and because investigations involving janitors are easier when the same janitors regularly work in a particular tenant space.

Sensitive Information

Depending on the sensitivity of the business, tenants may shred certain proprietary documents themselves, or employ contract-shredding agencies that will come to the building on a scheduled basis to remove and destroy documents. These documents may include sensitive business data, client lists and billing information, those that are confidential within the company, and any proprietary information that would be useful to competitors. Depending on the sensitivity of the data, it may be passed through a standard shredder or through a crosscut shredder, which more severely deters re-assembly of the shredded material.

Importance of Supervision

Routine removal of trash from a tenant floor should be carried out under constant supervision by janitorial supervisors or building security staff. No interruption should take place in supervision during the janitors' passage from the tenant floor to a service or freight elevator, or to designated receptacles such as dumpsters, compactors, or holding areas, usually located at the building loading dock. Such supervision will deter janitorial staff from secreting stolen articles in trash bags, and then dropping the articles in locations within the building where they or an accomplice can later retrieve them.

To make scrutiny of trash easier, the bags themselves should be made of transparent plastic. If, because of staffing limitations, direct supervision of trash removal is not possible, then CCTV cameras in the dock areas are recommended to deter the removal of items from trash bags before they are placed in dumpsters, compactors, or holding areas, or later from the receptacles themselves.

Special Trash Holding Areas

Trash holding areas can be found in multiple-tenant high-rise buildings, particularly where refuse from financial institutions is being handled. To avoid accidentally discarding important documents such as negotiable instruments (checks, bank drafts, savings bonds, securities, etc.), the trash from financial business tenants often is separated and held in a secured area for a period of time as determined by the financial institution concerned. The holding time permits losses to surface before the trash has been removed from the site for destruction.

Janitorial Screening

Janitorial staffs in many high-rise buildings are subject to certain property screening procedures on arrival and departure from work. The object of the screening procedure is to observe any prohibited items being brought into the building, and to detect any stolen property being removed from the building. As part of a pre-employment or pre-assignment agreement they may be asked to submit to a visual inspection of any items they are carrying to and from work—lunch pails, bags, packages, and so on. The frequency of the inspections can be established as part of the agreement: inspections may be conducted every time the employee enters or leaves the building for work, at random, or only with cause.

Janitorial supervisors or building security staff usually conducts such inspections. They are visual only, and employees are requested to open appropriate items themselves. Under no circumstances does the inspecting person touch the items being inspected or attempt to inspect any part of the employee's person or clothing. All persons have a legal right and expectation of privacy, so purses will be subject to inspection only under special circumstances, the nature of which should be established in writing beforehand. Some operations require janitorial staff to wear special clothing or smocks in which it is difficult to conceal items.

Importance of Controlled Ingress and Egress

The success or failure of any property control system will depend largely on whether there are ''controlled'' exits or entries to the high-rise facility for use by building occupants and visitors. For example, if building users need to pass through one particular point to enter or leave the building, and if this point sometimes is not supervised, then the property control system can be circumvented. Similarly, if there are other unsupervised exits or entry points, persons can defeat the property control system by using these areas when they want to bring in or take out property.

Some high-rise buildings with under-building parking garages have passenger elevators that allow people to travel directly up from the garage to the tower, and similarly for people to travel directly down from the tower to the parking garage. Such an arrangement affords no control over ingress and egress of people and property. To address this problem, if possible, the elevators should be reprogrammed to cause elevators from the garage to stop at the building main lobby and thereby compel passengers seeking access to the tower to cross to elevators that service it. To provide effective control the main lobby should be staffed by trained personnel. If such staffing is not possible because of budgetary constraints, card readers may be provided in the elevators serving the tower and CCTV cameras placed inside all elevators, or in the main and parking garage lobbies. By placing the tower elevators on card access, tenants will be required to use their cards to access their floors. If the cameras are constantly monitored or the images constantly recorded, the unauthorized movement of property might be observed either at the time it occurs, or at a later stage.

Key Control and Accountability

In high-rise office buildings, keys to the facility usually remain under the control of building management, security, and engineering personnel. Building management personnel obviously need to have keys to gain entry to all areas of the facility they manage. Building engineers, because of the nature of their work, also need access to virtually all areas, including tenant spaces. Depending on how the building is managed, security staff also will have access to most areas.

Some buildings do make it a practice to keep tenant office keys out of the normal possession of security staff but provide a controlled, documented means for these keys to be obtained when necessary. During emergencies and other special circumstances, security staff can obtain these keys quickly. After the situation has been resolved, the keys are again placed under supervision, perhaps in a locked or sealed key cabinet with the cabinet's key in strict custody.

Key Points to Consider

Keys should only be issued to those persons who can be entrusted with them and who have an *absolute* need for them. The status a key holder may feel by possessing certain keys should not enter into the decision-making process. The following points are important to consider:

- Building tenants should be issued keys that pertain to their particular area only.
- Building tenants should never be issued building entrance keys. (If issuing entrance keys is unavoidable, the locks should be changed periodically and new keys issued to the tenants authorized to have them.)
- Building tenants should not be allowed to duplicate keys. (Keys duplicated by building management should be distinctively marked to help identify unauthorized keys.)
- When an employee ceases to work for a tenant, all the employee's keys should be returned to the tenant representative. Depending on the situation, locks may need to be changed.
- When tenants move into a new space, all locks should be changed and new keys issued.
- Janitorial staff should be issued keys only for the time they require them and for the particular areas to which they require access. Depending on the size of the janitorial staff, designated supervisors within the janitorial operation may be issued master keys that, for instance, provide access to all tenant spaces on an individual floor. In this way, the general cleaning staff does not need to be issued keys. In some buildings no janitorial staff are issued keys, and security

staff must unlock the appropriate doors and relock them after the work is completed. Procedures will vary from building to building depending on size, complexity, and the manner in which cleaning is conducted and trash is removed.

- Elevator, escalator, dumbwaiter, rubbish chute, and moving walk technicians may be permitted to carry keys that provide access to their equipment, or the building may retain possession and issue them only as needed.

In some buildings maintenance personnel (telecommunications technicians, water and power utility workers, etc.) are permitted to attach their own locking devices to areas containing their equipment. This practice is convenient because building staffs are not required to open these areas, but it compromises security because control of keys and the areas themselves has been lost. These areas can be used to store unauthorized or stolen items, and general housekeeping may become a problem. If this practice is permitted, no one should be allowed to place a lock on a door without building security or other building departments (such as engineering) having a key. In an emergency, keys must be available for access. A possible alternative is for contractors to be permitted to stow their equipment in lockable gang boxes.

In the event of a lost key, the circumstances surrounding the loss should be fully investigated and thoroughly documented.

The following information regarding key control has been largely obtained (with slight modifications) from *Security Supervision: A Handbook for Supervisors and Managers* by Eugene D. Finneran.

Before an effective key control system can be established, every key to every lock used to protect the facility and property must be accounted for. However, the chances are good that it will not even be possible to account for the most critical keys, or to be certain that they have not been copied or compromised. If this is the case, there is but one alternative—to rekey the entire facility.

Once an effective locking system has been installed, positive control of all keys must be gained and maintained. This can be accomplished only if an effective key record is kept. When not issued or in use, keys must be adequately secured. A good, effective key control system is simple to initiate, particularly if it is established in conjunction with the installation of new locking devices. One of the methods that can be used to gain and maintain effective key control follows.

Key Cabinet

A well-constructed steel cabinet for keys is essential. The cabinet must be of sufficient size to hold the original key to every lock in the system. It also should be capable of holding any additional keys that are in use in the facility but are not a part of the security locking system. (Of course, high-rise tenants will have files, safes, and locks whose keys are not supplied to building management.) The cabinet should be well installed to make it difficult, if not impossible, to remove from the facility. It should be secured at all times when the person designated to control the keys is not actually issuing or replacing a key. The key to the cabinet itself must receive special handling, and when not in use, it should be placed in a locked compartment inside a combination-type safe. (Note that new technology is changing the ways keys are secured. See the section below on ''Computerized Key Control.'')

Key Record

Some administrative means must be set up to record key code numbers and indicate to whom keys to specific locks have been issued. This record may take the form of a ledger book or a card file. Many buildings use computerized key control records.

Key Blanks

Blanks to be used to cut keys for issue to authorized personnel must be distinctively marked for identification to ensure that no employees have cut their own keys. Blanks must be kept within a combination-type safe (or electronic key cabinet as described in ''Computerized Key Control'') and issued only to the person authorized to cut keys and then only in the amount authorized by the person responsible for key control. Such authorization should always be in writing, and records should be made of each issue, to be matched with the returned key. Keys damaged in the cutting process must be returned.

Inventories

Periodic inventories must be made of all key blanks, original keys, and duplicate keys issued to employees. Merely telephoning employees, supervisors, or executives and asking them if they still have their keys will not suffice. Key control personnel must inspect each key personally.

Audits

In addition to the periodic inventory, a member of management should perform an unannounced audit of all key-control records and procedures. During the course of this audit, a joint inventory of all keys should be conducted.

Master Key Control

Master keys and control keys for removable core cylinders should be kept under strict control by building management. Keys should be issued only to those who have a critical need for them. The decision as to whether master keys should be issued to building security staff will vary from building to building. (If they are not issued master keys, they will often be issued a ring of keys permitting them to enter various parts of the facility.) Keys issued to the security staff should never be permitted to leave the facility. They should be passed from shift to shift and a receipt should be recorded each time they change hands. The supervisor must ensure that all security personnel understand the importance of not permitting keys to be compromised.

Computerized Key Control

Beyond the traditional key log or mechanical key box, a popular device for key control and accountability is an electronic cabinet or drawer where keys and key sets are individually secured until released by an authorized user. The steel cabinet or drawer may be accessed using a keypad, logging onto a computerized system with a user name and password, or using a biometric reader. One such system has software that ''tracks who enters the system, which keytags are removed, when they are taken from the drawer, why the keytags are needed, and when, or if, the keytags are returned to the drawer'' (KeyTrak®, Inc.). Such a system offers the flexibility that not only keys, but also items such as access control cards and visitor badges, can be attached to keytags with semiconductor computer chips and then stored in computerized slots in the lockable steel drawer.

Tenant Security Education

There are many ways to educate building users and tenants about the security program in place. All building users, particularly tenants and their visitors, must understand the program and how various rules and procedures impact them. If people are aware of the logic behind security regulations, they usually will be more willing to comply with them. This communication can be achieved in the following ways:

1. Explain the regulations on an informal, as-needed basis. For example, building security staff may explain the purpose of an after-hours access register to a tenant when asking him to sign it; or may inform a visitor leaving the building that she must have a property removal pass signed by the tenant she just visited before the computer she is carrying can be permitted to leave the building.
2. Use posted signs, written policies and procedures in the Tenant Information Manual, pamphlets, leaflets, flyers, newsletters, video training materials, computer disks, and public address messages supplied by building management to the tenant or by tenant management to their employees. Appendix 7-1 is a sample *Tenant Security and Safety Awareness Checklist* that could be revised and sent to tenants at appropriate times during the year. Early to mid-November is often an opportune time to disseminate such information, as the approaching festive season often brings a higher incidence of theft in high-rise office buildings.
3. Have building management or the tenants themselves conduct security orientation lectures, classes, workshops, and seminars. Such events can be an effective medium not only for communicating to tenants what is required of them in the building security program, but also as an opportunity to educate employees about basic security measures they can adopt at work, home, and on their way to and from their place of work. Such tips could include not leaving valuable items in view in parked vehicles; securing all vehicle doors and windows; securing desks, filing cabinets, and business and personal property; and observing a ''clean tabletop'' policy. If practiced by tenants, these would contribute substantially to reducing theft at a building.

The length of security briefings will vary, but 45 minutes to 1 hour is probably the maximum that busy tenants will permit. As with all effective teaching, the use of audiovisual aids—films, videotapes, overheads, and slide programs—can help gain the attention of participants and assist in effectively communicating the required message. The frequency of classes, meetings, conferences, seminars, and workshops will vary from building to building; they may be regularly scheduled or conducted when a specific need arises. Security training can be incorporated effectively into occupants' fire life safety training classes. The training of occupants, floor wardens, and building emergency staff is discussed further in Chapter 11.

The tenants are an important part of any building security program. They must be educated to know that they are the ''eyes and ears'' of the building. If they see anyone who does not appear to belong, particularly someone within their own tenant space, a ''May I help you?'' type of approach will reveal much about the person. Specific questions can determine if the person is an employee, is a visitor (if so, who are they visiting?), or is delivering or picking up items (if so, where? at whose request?), and so on. Although the tenants are not expected to be trained security professionals, they are expected to be active participants in the building security program by being aware of their surroundings and promptly reporting potential security problems to tenant management, building management, and building security staff.

Summary

From the time a vehicle enters the parking structure and pedestrians proceed to the building, travel in the tower elevators, and enter an individual tenant space, there is a need for access control measures that sift out unwanted persons and intruders and yet constitute a minimum of inconvenience to legitimate building users. In multiple-tenant commercial office buildings, the three lines of defense—the main lobby, the elevators and lobbies on each floor, and the entrances to tenant space—provide points at which access control can be effected.

Personal and business property that is moved into and out of building and tenant areas must be controlled. To establish a successful property removal control system, there must be supervised egress points through which all property and trash should pass. Also an essential part of a security program is to strictly control all keys used at the building. Tenants are a vital part of security and must be educated in security awareness.

References

American Protective Services, *Administrative News* (American Protective Services, Inc., Oakland, CA, 1993).

American Protective Services, *Commercial Building Security: The Notebook Lesson Series for Security Officers* (American Protective Services, Inc., Oakland, CA, 1980).

American Protective Services, ''Objectives of a security program,'' *High-Rise Training Course* (American Protective Services, Inc., Oakland, CA, 1990).

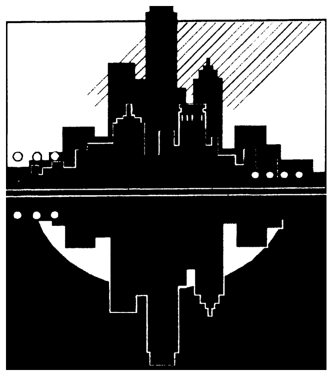
Finneran, Eugene D., *Security Supervision: A Handbook for Supervisors and Managers* (Butterworths, Stoneham, MA, 1981), as reported in *Handbook of Loss Prevention and Crime Prevention* by Lawrence S. Fennelly (Butterworth–Heinemann, Newton, MA, 1996, pp. 227, 228).

Geiger, Geoff, Craighead, Geoff, ''Minding the store: office security is big business,'' *Los Angeles Business Journal* (Los Angeles, July 1991).

KeyTrak®, KeyTrak System information provided by Jeff Caley, Field Manager (KeyTrak, College Station, TX; available at: http://www.keytrak.com).

Macklowe, Harry, comments in ''The glass shield'' (*Access Control & Security Systems* magazine, Atlanta, GA, February 1998).

Appendix 7-1 Sample Tenant Security and Safety Awareness Checklist



TENANT SECURITY AND SAFETY AWARENESS

The following security and safety tips may be of assistance during the upcoming holiday season.

Safety in the Parking Structure and When Driving

- On leaving your vehicle, always lock its doors. If you possess a parking access card, do not leave it in your vehicle when at the office.
- Secure any belongings in the trunk or out of sight. Do not leave any valuables or possessions in plain view.
- Be alert to your surroundings and people, and avoid using stairwells, alleyways, poorly lighted locations, and areas that are out of the way or isolated.
- If you observe any suspicious person or activity, immediately report this to building security possibly using a parking intercom or dialing 555-8395.
- When approaching your vehicle, be aware of anyone following you. Have the keys ready in your hand, and on reaching your vehicle check the back seat before entering. Once you enter, immediately lock your doors and keep them locked when driving.
- Observe speed limits and drive safely at all times.

Safety in the Building and Your Office

- Do not assist outsiders or strangers to enter the building or your tenant space.
- Challenge any strangers with a simple ''May I help you?'' Immediately notify building security, by telephoning 555–8395, of suspicious persons or if any unauthorized persons are found in your office.
- Notify building security if any solicitors visit your office.
- Physically secure desktop PCs, laptop and notebook computers, or other valuable equipment, such as personal data assistants, CDs, floppy disks, and cellular (mobile) telephones, or lock these items up when not in use.
- Record serial numbers and engrave identifying marks on equipment to assist in its recovery if it is ''borrowed'' by a fellow employee or is stolen.
- Never leave items such as billfolds, purses, wallets, blank checks, petty cash, and keys unattended or in plain view. If necessary, lock them in a desk drawer or cabinet.
- Keep a ''clean desk'' policy and secure all confidential files and information before leaving your office.
- Keep office and restroom keys on a separate key ring and be cautious about who you lend them to.
- When working alone in the office, lock all perimeter doors and activate any security systems.
- When working late, notify your supervisor or a friend or relative. When you are ready to leave, notify building security and request an escort.
- Immediately report to building management any security or safety hazards.
- If you are the last to leave, check that electrical appliances, such as the coffeepot, are switched off.
- If you are in an elevator with a suspicious person, stand near the elevator control panel. If emergency assistance is required, press the EMERGENCY CALL, EMERGENCY ALARM, or EMERGENCY ONLY button.

Christmas Tree Safety

- All ''live'' cut trees must be fireproofed. The signed fireproof certification tag must be given to building management before any tree can be brought into your office.
- Lights may not be placed on ''live'' cut trees.
- Artificial trees may have lights, but these must be turned off during nonbusiness hours.

The Building Management of Pacific Tower Plaza Wishes You a Happy and Safe Holiday Season!

This Page Intentionally Left Blank

8 *Management of the Security Function*

The security function encompasses the security-related activities and duties performed in a facility. Within a high-rise office building these activities and responsibilities usually are performed by a security department acting on behalf of the building owner or manager. The size and makeup of the security department varies depending on the complexity of the facility and requirements of its security and fire life safety program. The head of the department may have one of various titles—*Director of Security, Security Director, Security Manager, Chief of Security, Head of Security*, *Security Supervisor*, or, in a smaller building, *Post Commander*. For our purposes, this person will be called the Director of Security. Whether the security department comprises contract or proprietary staff, the Director of Security has an important role in determining the quality and performance of the department. According to Keating (1994, p. 9), the Director of Security

> Must have security experience, leadership ability, be an excellent communicator both verbally and in writing, be organized and a strong time manager, enjoy and interface well with all kinds of people, be intelligent and able to understand and teach complex systems, be patient, upbeat, positive, outgoing, self-disciplined, caring, energetic.

''In today's business and industrial world, the designated security chief is a person of impressive credentials and experience in safety and security management'' (Giambalvo, 1998, p. 61).

The remainder of the security department consists of supervisors and staff with job titles determined by the functions they perform; for example: *Lobby Director, Lobby Ambassador, Lobby Officer, Concierge*, *Console Operator, Command Center Operator, Patrol Officer, Rover, Courier, Dockmaster, Watch Commander*, *Shift Supervisor*, and *Security Officer*. Just as the term *night watchman* was replaced years ago by security guard, *security officer* in most areas of the United States now has largely replaced *security guard*.

The Security Budget

In today's business world, the costs of security in a high-rise building need to be justified to the building owner and manager so that the security department remains adequately funded. *Webster's College Dictionary* defines *budget* as ''an estimate, often itemized, of expected income and expenses for a given period of time in the future . . . A plan of operations based on such an estimate.'' When the budget is reviewed, it is often difficult to quantify the value of the services that the security department provides and convince building management that the security function does in fact generate income for the facility, if only indirectly. How does one, for example, place a monetary value on the security benefit closed-circuit television (CCTV) cameras installed in elevators have on building operations? Other departments, such as parking, can justify their activities based on actual income produced, measured in dollars and cents. The Director of Security needs to demonstrate that the security function's activities and duties performed within a particular time (usually the previous 12 months) have produced value commensurate with the funds allotted to it. This will lay the foundation for the budget for the ensuing fiscal period. For instance, with our aforementioned example, it would be helpful to cite previous expenses incurred to repair damage caused by vandalism in the elevators for a time before and after CCTV installation. If the incidence of reported vandalism is lower after the installation, the monetary value of the security measure can be demonstrated.

Not all aspects of the security function, however, can be assessed in dollars and cents. For instance, how can one evaluate in monetary terms the absence of crimes of opportunity, such as thefts by intruders in tenant areas, which resulted from an effective tenant security awareness program* that the building security department provided for tenants?

For building owners and managers, an essential budget issue is whether costs are escalatable or not. The term *escalatable* refers to costs the building incurs that may be charged proportionately to tenants based on lease provisions. For example, costs associated with the building parking operation may be *non-escalatable* if parking operations are considered to be a separate profit center, whereas costs associated with the security operation are escalatable because they are typically part of the building's routine operating expenses.

Key Items

A security budget may include as line items the estimated cost of the following:

- The itemized capital cost of security systems, equipment, and fixtures (e.g., physical barriers, lighting, access control systems, communication systems, CCTV systems, intrusion detection systems, and equipment used by security staff), including installation and maintenance costs. Security budgets also may include costs pertaining to fire life safety systems, equipment, and fixtures, if these costs are not part of a separate safety budget.
- Legal, professional, and consulting charges.
- Permits and licenses.

*''It has always been difficult to quantify the contribution that a security program makes to the overall operation of an organization. In addition, by the nature of what security does, the better the program that exists the more difficult it is to see the need. If we have a very secure environment, we will have few or no incidents. When management sees few or no incidents, it tends to downplay the need for the security function'' (Azano, 1995, p. 25).

- Security staff, including (1) wages and benefits, payroll taxes, worker's compensation claims and insurance, costs of uniforms, hiring, training, supervision, administration, liability claims, and insurance; (2) sundry items such as office and stationary supplies, administrative help, and so on; (3) utilities such as lighting, electricity, telephone, and network fees; and (4) maintenance of equipment used by security staff.

Depending on the building owner or manager, certain of these line items may be amortized over time, equipment may be leased, or other arrangements may be made to suit the building operation. It must be kept in mind that "one does not plan or budget for the unknown or the unpredictable; one budgets for intelligently anticipated and predictable conditions, based on known conditions in the present and the past" (Sennewald, 1998, p. 160). Natural disasters and other catastrophic events are not predictable; budgeting, therefore, usually will not take them into consideration. However, some buildings provide various supplies and equipment in case of a major emergency. Of these items, food, water, and some medical supplies have a predetermined shelf life, and their replacement costs should be included in annual cost estimates.

Contract versus Proprietary Security Staff

Security staff that makes up a security department in a high-rise building can be either employed directly by the building owner or manager (i.e., proprietary or in-house) or employed by a contract security company (the process of contracting out is referred to as *outsourcing*). Today, most high-rise office buildings employ contract security personnel. A building or property manager usually does not have the luxury of a large human resource department to handle the many facets of recruiting, hiring, personnel management, and training required for security staff who work in a building.

The use of proprietary security staff has certain advantages to building owners and managers; the use of contract security staff has others.

Advantages of Proprietary Security Staff

- Staff is recruited, screened, and selected using procedures and methods stipulated and controlled by the client.
- Staff can share the same benefit programs as other building employees.
- Staff are under the direct "employer–employee" control of the building owner or manager.
- Staff, as employees of the building, usually have an undivided loyalty to the building.
- Building management does not need to communicate with a contractor to supply their security staffing needs and provide direction to security staff.

Advantages of Contract Security Staff

- Staff employed at the building are recruited, screened, selected, uniformed, equipped, trained, supervised, insured, and paid by the contractor; building management does not need to be involved in the process.
- Because security staff are employees of the contractor, most liability burdens and responsibilities reside with the contractor, not the building owner or manager.

- A contractor, particularly a major one, has access to a large labor pool of employees and has the resources to provide additional personnel and supervision during emergencies and special events.
- Building management can request under the terms of the contract that unsuitable staff working at the building be removed quickly.
- Replacements for employees who are absent from work because of sickness, personal leave, holidays, vacations, and so on are the responsibility of the contractor.
- The security department can be rapidly downsized and employees reassigned by the contractor rather than being laid off.
- The contractor will supply forms, records, reports, office supplies, and auxiliary equipment required to carry out the security operation.
- The security contractor, if properly selected, will have staff within their company who can provide professional expertise to building management. A professional security contractor can conduct surveys, formulate and document policies and procedures for the security staff, conduct investigations, provide advice and knowledge regarding developments in the security and life safety field, and assist building management in developing relationships with local law enforcement and the fire department.
- ''An important benefit to all parties is that a guard now can aspire to advancement, and to promotion to a salaried status that includes the more attractive benefits that a major company is able to provide. Consequently, the job attracts better-qualified guards and results in improved job placement'' (Giambalvo, 1998, p. 62).

In some major high-rise projects, there is a *hybrid* proprietary-contract security operation. In-house employees staff the Director of Security and supervisory positions, while the remainder of the security staff are contract employees. ''In close communication, the chief liaisons of both the client and security contractor share clear understandings of the requirements for both guard and supervisory personnel. The new dimension of these programs is that the supervisors are selected from the contracted guard force itself'' (Giambalvo, 1998, p. 62).

Selection of a Contract Security Service

Building owners or managers who employ a contract service to staff their security department and operate their security program must take special care to select a *professional* contractor. A professional security contractor does business based on the highest ethical and industry standards, providing properly selected, screened, trained, and supervised staff. The building owner or manager also must ensure that the fundamental provisions of the security services agreement between their facility and the contractor constitute an attainable goal—that the contractor reasonably can be expected to provide the requested level of service.

Prerequisites for a Successful Program

Competitive wages and benefits for hiring competent staff, adequate working conditions and amenities, and a reasonable profit margin for the contractor providing the services are prerequisites for a successful security program. In addition to these factors, the client-contractor relationship must be clearly delineated, and an essential element of trust must be established. One does not have to go far to ascertain the root cause of high turnover of unsuitable, poorly trained, poorly supervised, poorly motivated, and unkempt security personnel—a predicament that, if it persists, will have devastating effects on any building security program. If this happens, the chances are that a professional contractor has not been selected, or that the provisions of the security service agreement are not adequate for quality service.

According to Allied Security, Inc., (1983, p. 2), ''the traditional contracting process for security guards involves few, if any, performance specifications. The user relies on the assumption that he [or she] is requesting and receiving proposals on a service with generally accepted performance standards.'' Such assumptions, however, can be problematic, for performance varies from one contractor to another.

Vital Issues

The following issues need to be addressed in the contracting process:

- The state and local business licenses of the contractor should be examined.
- The history, ownership, and financial stability of the contractor should be reviewed.
- The liability insurance coverage to be provided by the contractor should be specified and proof of such insurance furnished.
- The requirements for each position that needs a contract security staff member (including a job description of the basic work to be performed, specific qualifications, and the expected hours of coverage) should be outlined in the proposal specifications.
- The wages and (especially) the benefits of the security staff need to be specified. These factors will not only impact the quality of service to be provided but will also permit the building owner and manager to make an ''apples to apples'' comparison between contractors. It should not be enough for a contractor to say, ''Yes, we provide vacations, holidays, and health insurance benefits to our security officers''; further information should be ascertained: How many days of vacation? What holidays are recognized? What is the health plan? What benefits does the plan provide? Does the employee contribute to its premiums? How much? What is the qualifying period before the plan is in effect? What is the deductible? What is the maximum allowable claim?
- A contractor's management approach and depth of organizational staffing also need to be examined. Who are the managers and supervisors? How will

they interface with the client and the site operation? What are their security qualifications, background, and experience both within the security industry and with the present contractor? How would they handle the start-up and transition of security staff at the client site? How do they formulate and document policies and procedures for security staff working at client sites? How do they conduct training at client sites? How will they audit and evaluate performance at the job site?

To evaluate operational capabilities, it is a sound move to visit the contractor's office and meet with the administrative staff responsible for supporting the contract. A guided tour of the operation should include how essential tasks such as recruiting, screening, selecting, outfitting and cleaning of uniforms, issuing equipment, training, scheduling, supervising, administering the payroll, and billing are performed. One should also request sample personnel files to see whether the contractor has kept employment applications and records and has conducted thorough background checks. If time permits, one should attend a training session to examine the quality of training and materials provided.

- To determine whether the contractor has the necessary proven expertise, examine references of comparable clients to whom the contractor is currently providing service. Such references should reveal whether the contractor has fulfilled contractual requirements and performed at the level of service agreed upon, and also show the contractor's responsiveness to problem solving and other requests. One might even visit and inspect client sites where the contractor provides a comparable type of service with similar wages and benefits to those being requested.

Costs for Contract Service

Contractors usually base their charges on an hourly billing rate for security staff working on a client site, commonly using the terms *spreadsheet* and *spread*. The *spreadsheet* usually details each hourly pay rate and its associated billing rate (or provides a weighted average or composite billing rate, or percentage markup, for all hours worked). The difference between pay and billing rates is the *spread*. The spread may include costs of background checks; uniforms; training; estimated overtime; paid holidays; sick leave and vacation; payroll taxes; health, life, and accidental death and dismemberment insurance; miscellaneous benefits; worker's compensation and liability insurance; administrative overhead; and profit. The administrative overhead can include branch management, account management, human resources, scheduling, field supervision, legal expenses, training and communications, information systems, risk management, accounting (payroll, billing, accounts payable, and general ledger), credit and collections, purchasing, sales and marketing, quality assurance, and executive costs. The costs of purchasing and maintaining equipment—vehicles, portable radios, mobile phones, and patrol management systems—usually are itemized separately.

Importance of a Thorough Process

Only after an exhaustive investigative proposal process can a client make a thoroughly informed and sound selection of a contract security provider. Once this is accomplished, a security services agreement outlining the general and specific terms of the contract, including terms of payment, should be fully executed with both the client and contractor agreeing on its contents. If the selection process is pursued thoroughly, the client will not only be completely familiar with the selected company's policies, procedures, and operations, but also will have established a working relationship with key members of the contractor's management team.

Determining Adequate Levels of Security Staffing

The level of security staffing needed to administer an adequate security and fire life safety program for any facility requires a two-step analysis. According to Colling (2001, p. 139), ''It is necessary first to analyze the security mission, to determine the organization's security [and fire life safety] vulnerabilities, and to identify the services to be rendered. The next step is to design a program that will address the mission, properly manage these vulnerabilities, and implement the intended services. Only then can the number of staff required to operate the program be determined.'' In the high-rise setting, building management will first need to conduct a security and life safety survey. After that, a security and fire life safety program needs to be designed; only then can the adequate levels of staffing be determined for the building.

The required levels of staffing for most high-rise office buildings are higher during normal business hours than after hours. During normal business hours, most tenants are open for business and there is an increased population of tenant employees, visitors, salespersons, tradespeople, building management staff, building contractors, couriers, delivery persons, solicitors, building inspectors, and others who may require the attention of building security staff. After hours, pedestrian (and vehicle) traffic usually lessens and only the number of janitorial staff increases (unless special activities are occurring in the building).

Typical Positions

Levels of security staffing, hours of coverage, and specific functions vary from building to building. The following supervisory and non-supervisory positions (with actual job titles varying from building to building, region to region, and country to country) often are found in larger high-rise buildings:

- *Director of Security* (or *Security Director*, *Security Manager*, *Chief of Security*, *Head of Security*, *Security Supervisor*, or, in a smaller building, *Post Commander*). He or she oversees and coordinates the activities of the security department.

- *Fire Safety Director*. This person establishes, implements, and maintains the Building Emergency Plan. In some buildings the Director of Security and the Fire Safety Director are the same person.
- *Shift Supervisor* and *Watch Commander*. These persons are assigned to the various shifts—usually designated as day, swing or mid, and graveyard; or perhaps first, second, and third. They oversee and coordinate the activities of security staff assigned to their shift. Shift supervisors usually report to the Director of Security.
- *Lobby Director, Lobby Ambassador*, and *Lobby Officer*. These persons, assigned to lobby areas, control access to the building, provide information to building users and visitors, and perform other duties as specified by the facility.
- *Concierge*. This person, often assigned to building lobby areas, performs a similar function to a hotel concierge, providing information and services to building tenants and visitors, and performing other duties as specified by the facility.
- *Console Operator* and *Command Center Operator*. These are the persons assigned to the Security Command Center who monitor and operate building security and fire life safety systems and equipment.
- *Dockmaster*. This individual supervises the loading dock, including all loading and unloading operations.
- *Freight/Service Elevator Operator*. This person operates the freight/service elevator and screens all such elevator users for authorization to travel to various floors of the building.
- *Security Officer*. This officer performs security and fire life safety functions as determined by the building operation.
- *Patrol Officer, Parking Patrol*, and *Rover*. These persons patrol various parts of the building and parking areas and perform other duties as specified by the facility (patrols may be performed on foot or by using a motor vehicle, golf cart, or bicycle).
- *Training Officer*. Particularly in larger projects, the training officer is responsible for training and testing all building security staff regarding their duties and responsibilities.

The essential functions required for each of these positions should be specified in a *job description*. This description also should mention the abilities and skills necessary to effectively carry out these functions. Job descriptions can be used for training and as a basis for employee performance reviews and the determination of wage and salary ranges.

Security Staff Duties and Written Instructions

The primary role of security staff in a high-rise is to implement the building's security and fire life safety program. Some buildings may have a separate safety department; in others, the security department may assume safety responsibilities. Duties of the security staff vary from building to building, and depend largely on the policies and procedures determined by management.

Security staff duties should be written clearly, concisely, and accurately, and kept readily accessible for training and for reference. These *security instructions* (commonly called *post orders* or *standard operating procedures*) should be periodically reviewed and regularly updated.

What Should Post Orders Contain?

Post orders should contain at least the following information:

- Statement of purpose and a notice of confidentiality.
- An overview of the building and a profile of the tenants doing business there.
- List of emergency telephone numbers for police and fire departments, emergency services, paramedics or ambulance services, utility companies, and other agencies.
- List of after-hours telephone contact numbers for building management, engineering, security, janitorial and parking staff, elevator company representatives, security and fire alarm companies, haz-mat contractors, window board-up contractors, and so on.
- Description of the building and its operation, including possibly floor plans and maps, and the security and fire life safety systems and equipment. This should include an explanation of how systems operate under normal and emergency conditions. Photographs and diagrams will make such descriptions more effective.
- Review of subjects such as building access control, handling trespassers, tenant access, handling service of process (writs, complaints, summonses, etc.), key and equipment control, property removal, escorts of building users, mobile patrols, arrests, and other policies and procedures.
- Specific instructions on handling emergency situations such as fires, fire alarms, explosions, bombs, bomb threats, aircraft collisions, violence in the workplace (including assaults or other criminally-threatening behavior), aberrant behavior (such as that caused by substance abuse), medical emergencies, power failure, elevator stoppages, natural disasters, water leaks, hazardous materials, chemical and biological weapons, strike and labor disturbances, demonstrations, riots and civil disorders, hostage taking and barricade situations, and assaults or other criminal activities.
- List of security staffing levels, their hours of coverage, and their specific functions and job duties. Wherever possible the duties should be described by shift, day of the week, and specific time.
- Instructions on public relations, including how to handle hostile situations, telephone and radio communications, and how to conduct interviews and write reports. (These subjects either may be included in the instructions or may be communicated to security staff through other means.)
- A Code of Ethics and Standards of Conduct. These should be established to help foster a strong ethical climate throughout the security department and to provide clear and specific guidance to employees.

    - Code of Ethics
      Adherence to professional ethics is critical in any organization, but particularly so in one entrusted with the security of a high-rise building. *Webster's College Dictionary* defines *ethics* as "a system or set of moral principles . . . the rules of conduct recognized in respect to a particular class of human actions or governing a particular group." According to Ferrell and Gardiner (1991, p. 2), an ethical act or decision is "something judged as proper or acceptable based on some standard of right or wrong. Although people often have different morals and standard of right and wrong, many are shared by most members of our society."

      Professional ethics are very much a matter of *conscience*, which is defined by *Webster's College Dictionary* as "the inner sense of what is right or wrong in one's conduct or motives.'' Because ethics require this inner sense, there is no guarantee that the existence of a Code of Ethics will prevent undesirable actions by an employee. However, such a code does clarify to staff what is expected of them. Appendix 8-1 reproduces the *Security Officer Code of Ethics* established by the National Association of Security Companies (NASCO).

- Standards of Conduct
  Standards of conduct specify actions that may be subject to disciplinary action: unexcused absences or excessive tardiness, unacceptable appearance or attire, use of profane language, making racial or ethnic slurs, engaging in sexual or other forms of harassment, disorderly conduct, sleeping or dozing on the job, being insubordinate, unauthorized disclosure of confidential information, making false statements, unauthorized use of company property, unauthorized acceptance of gifts, failure to observe security and safety rules and regulations, and so on.

These instructions may be housed in one binder (preferably a ringed one that permits easy removal and replacement of pages), or in separate binders or folders. The binders or folders should be clearly labeled for easy reference. All copies should include the date the instructions were established or last revised, by whose authority the instructions were made, and which individuals have the authority to change them. Modifications made to operating procedures should be dated and incorporated into all existing copies of written instructions as soon as possible. Outdated instructions should be retained for a period varying from 5 to 7 years (as determined by the building's document retention policy or legal counsel), because they may be needed later in litigation defense.

Writing Post Orders

Instructions for complex procedures and systems must be written in easy-to-understand, action-oriented terms, keeping in mind that,

According to Bennet H. Berman (1980) of the University of Michigan's Institute for the Study of Mental Retardation and Related Disabilities,

> One of every four Americans in the work force is functionally illiterate, that is, unable to comprehend at least 50 percent of reading material beyond the fourth grade level.
>
> A significant number of work errors result not from an inability to do the job but from a misunderstanding of what the job is. Many employees can't read the memos from the boss, the company's rule book, the training manual or other written instructions . . .
>
> However, 90% of all meaning can be conveyed with a vocabulary of 600 words. For maximum readability, company manuals should follow this average guideline per 100 words: seven to nine sentences, 12 to 14 words per sentence and 140 to 160 total syllables. (POA, 2000, p. 33-3)

Those who write these instructions should avoid cumbersome writing and overuse of the passive voice. For example, ''Building console operators while away from the Security Command Center are required to maintain a two-way radio on their persons at all times'' can be understood more easily if written, ''When away from the Security Command Center, always carry a two-way radio with you.''

Like any extensive document, the instructions should have a clearly labeled table of contents and numbered pages and, for ease of reference, each subject should be separately tabbed, and there should be an index. Photographs, diagrams, checklists, summary sheets, and flow charts should be included to make the material more interesting and easier to comprehend.

Written Records and Reports

Security staff in a high-rise building must make observations and provide thorough and accurate reporting and recording of security and safety operations, activities, and incidents. Observation may involve any or all of the senses—sight, hearing, smell, or touch—and requires the capacity to understand the meaning of what has been observed. ''In security work it is important to determine whether what has been observed is significant for security or safety and is routine or unusual'' (American Protective Services, 1990, p. 33). After observation and appropriate action, security personnel must furnish an accurate record of important observations.

Forms, records, and reports used by security staff may vary from building to building, but all aim to provide a thorough, accurate, and permanent account of events that have occurred. Such documentation can be used to generate statistical data that may be useful to justify existing or future expenditures for security and fire life safety systems and equipment.

Types of Forms, Records, and Reports

Some common forms, records, and reports found in high-rise facilities are as follows:

- *Daily or Shift Activity Report*—includes date and time of duty; name, badge or employee number (if appropriate), and signature of the reporting officer; position or post to which the officer is assigned; equipment the officer has received (including keys, patrol monitoring devices, radio, pager, etc.); and a chronological narrative of events and incidents that have occurred while the officer was on duty. It generally does not contain detailed descriptions of unusual events and incidents such as crimes and accidents. The report should be in duplicate so that an original is available to building management and the security department can retain a copy. Some reports are compiled using shift log database software.
- *Incident Report*—elaborates on unusual events and incidents in the Daily or Shift Activity Report and may include name, badge number (if appropriate), and signature of the reporting officer; the incident's date, time, type, and location; a full description of the incident; names and contact details of any victims, suspects, and witnesses; action taken (including who was notified of the situation); and follow-up action that may be required. Any photographs, sketches, or exhibits should be noted on the report and clearly labeled. The report should be in duplicate or triplicate so that the original can be

supplied to building management and the security department can keep at least one copy. Some reports are compiled using incident reporting software (see later section, ''Computerized Incident Reporting'').

- *Safety Hazard Report*—similar to the Incident Report but reports a hazard rather than an incident.
- *Vehicle Accident Report*—includes name, badge or employee number (if appropriate), and signature of the reporting officer; date, time, and precise location of the accident; description of the accident (including a sketch of the accident scene) and property damage; posted speed limits, stop signs, and traffic lights and signals; license number of vehicle(s) involved; estimated speed of vehicle(s); weather and light conditions; indication of whether seat belts were in use; any evidence of substance abuse; name, driver's license number, and contact details of driver(s); details of insurance companies of driver(s); name(s) and contact details of injured person(s) and witnesses; the action taken (including who was notified of the situation and whether a traffic citation was issued); and follow-up action that may be required. Any photographs, sketches, or exhibits should be noted on the report and clearly labeled. The report should be in duplicate or triplicate, as in the case of an Incident Report.
- *Tenant and Visitor Log*—includes the names (printed for legibility) and signatures of persons entering or leaving the building, the names of the companies they represent or tenants they are visiting, the date, and times in and out.
- *Courtesy Notices*—vary in format depending on designated purpose. The security or parking department may use special parking courtesy notices to inform a driver that his or her vehicle was found parked (1) illegally (with a reminder to park in designated areas only); (2) incorrectly (with a reminder to park correctly in a designated parking stall); (3) in a space reserved for the disabled; (4) with the vehicle unlocked, with windows open, or with personal property in view; or (5) some other vehicle-related matter that needs to be brought to the driver's attention. These notices should be designed so that an original can be left on the vehicle windshield and a duplicate copy retained by the issuing department.
- *Tenant Security Notice*—used by security staff to notify a tenant, for example, that a door to their area was found unsecured and subsequently locked by security at a specific time. The notice could be designed to hang on a door and a copy or tear-off portion retained for future reference. The building security department also should notify the designated tenant contact person of the security violation on the next business day.

There also may be contractor sign-in logs; personnel escort logs; elevator malfunction reports; security and fire life safety systems and equipment checklists; fire alarm report logs; stairwell inspection reports; lost and found property reports; and various other forms, records, and reports designed for use in the building.

Use of Notebooks

Security staff may also use *notebooks* to record details that, at a later stage, can be produced as legal evidence. These books should be small enough to fit snugly in a pocket, equipped with hard covers to protect the pages, bound, and sequentially numbered to make the removal of any pages immediately evident. ''A bound notebook creates a more favorable impression in the courtroom than the looseleaf type, since its form does not suggest the possible removal of pages.... Obviously, ink is preferred to pencil for permanence'' (O'Hara and O'Hara, 1994, p. 31). The pages should be lined and an entry written legibly and in chronological order as soon as possible after an observation is made. Any changes to entries should be lined out and initialed rather than erased or obliterated.

Who, What, When, Where, Why, and How

The six essential components of any successful report are who, what, when, where, why, and how. The *Protection Officer Training Manual* (Fawcett, 1992, pp. 42, 43) outlines them as follows:

- *Who*—relates to who was involved in the event, the name of the complainant, client, witnesses, suspects, accused parties, or [security staff].
- *What*—relates to the type of incident or event, what actually occurred.
- *When*—this is the time and date that the incident occurred.
- *Where*—this is the location that the event took place, with subsequent locations depending on the type of incident.
- *Why*—this is the motive. It can frequently be determined by proper investigation. It may explain the reason for the occurrence, but cannot be speculation or unfounded opinion [by security staff].
- *How*—how did the event come to your attention? How did it occur? This means the complete details on how the event happened from start to finish.

All six of these will be present in even the simplest event. Not recording some details because they seem unimportant at the time results in lost information that eventually may prove valuable; it also may lead to an embarrassed security staff member having to explain a sloppy report to an irate security supervisor, a building manager, or an investigator.

Legible, Thorough, Accurate, Clear, Concise, and Prompt

Legible, thorough, accurate, clear, concise, and prompt documentation of incidents has been of inestimable value to many building owners and managers, particularly when litigation occurs. Incidents, such as trip, slip, and falls, do occur in high-rise buildings, and much of the potential for liability can be mitigated substantially by handling, recording, and reporting these incidents in a thoroughly professional and competent manner. ''For clarity's sake the author should write reports in the first person. The narrative should never make judgments regarding responsibility or blame for any loss or injury and should not refer to prior similar events'' (Bates 1995, p. 79).

Reports of security staff should be reviewed by supervisors and ''any spelling or structural errors should be noted, and the report rewritten by the original author. Substantive changes—normally made by the author—should only be made after discussion [by a supervisor] with the author. Otherwise, an opposing party in litigation might infer that an effort was made to hide something'' (Bates, 1995, p. 79).

How Long to Keep Reports?

The retention period for reports will depend on the type of report, the requirements of state law, and the building's policy. This period may vary from a few months for daily activity reports, to 3 to 7 years for incident reports. It should be considered that ''reports help identify future security needs and that a claim of inadequate security can be brought anytime during a state's statute of limitations for negligence (two or three years from the date of injury in most jurisdictions). With that in mind, reports should be kept at least until the local statute of limitations expires'' (Bates, 1995, p. 80).

Computerized Incident Reporting

In the past, all records and reports were recorded on paper. Today, because of technological developments, information can be managed using computer software programs. *The PPM 2000 Security Management Software InCase System*, for instance, allows a personal computer to sort data contained in incident reports by time of day, day of week, month, year, type of incident, suspect, or any other user-defined field in the reports. This allows an incident reporting system to be tailor-made for a facility and the analyses it conducts. Trends in certain types of incidents can be discovered, weaknesses revealed, investigations assisted, and loss prevention strategies devised. ''Computers allow a security department to work smarter since vast amounts of information can be stored in a small space and retrieved at any time. Operations reports no longer have to be done manually. Budget figures can be obtained and expenses monitored at will'' (Denekamp, 1989, p. 43).

Selection, Training, Testing, and Supervision of Security Staff

Security staff for a high-rise facility must be properly selected, trained, tested, and supervised. All these processes must be thorough and well documented, especially in today's litigious society.

Selection

Selecting the right person to work in the high-rise environment begins at recruitment. A comprehensive employment application should be filled out by the applicant and a thorough background check conducted. A good background check should include the following: proof of identity and right to work; aliases; current address and previous addresses for the previous 10 years; educational background; current and past employers and supervisors (for the previous 5 years), with explanations of any breaks in employment greater than 30 days; details of any military service; criminal convictions and records check; surety that the applicant can comply with all applicable state and local security personnel registration and licensing laws; a check of financial responsibility and character references; drug screening; integrity testing; and if driving is a job requirement, proof of a valid driver's license and a driver's record check.

Honesty, trustworthiness, helpfulness, and loyalty are important character traits to look for in a candidate. Because certain security positions require specific physical prowess or mental ability, an applicant should be evaluated for meeting essential performance standards. According to Geiger and Craighead (1991, p. 11B),

> Today's security officer must successfully operate equipment that is at times highly technical, particularly that installed in high-rise towers. He or she must operate hand-held radios and monitor CCTV systems, elevator recall panels, fire annunciator panels, and card access and intrusion [detection] systems. Most importantly, from the perspective of fire and life safety, the modern security officer must respond [appropriately] during building emergencies such as fire, earthquakes, bomb threats, medical emergencies, and power failures.

Individuals monitoring security and fire life safety systems and equipment in the Security Command Center require a certain level of intelligence to handle these complex tasks. In the United States, the Americans with Disabilities Act prohibits employers from discriminating against qualified individuals with disabilities; however, if an applicant cannot perform an ''essential job function'' (in this case, carrying out complex monitoring duties) because of a physical or mental disability for which the employer cannot make a ''reasonable accommodation,'' such an applicant can be rejected. Applicants also should be tested to determine if they are able to read, write, understand, and speak effectively. Security personnel often are required to understand complex verbal and written instructions and to write detailed reports. They must be able to maintain language comprehension and fluency not only during the performance of regular duties but also under the emotional duress of an emergency or crisis situation.

Applicants should be evaluated for standards of personal appearance and hygiene, and they must possess public relations skills sufficient to allow them to interact in a positive manner with tenants and visitors, building management, fellow security staff, law enforcement and fire department personnel, the media, and the general public.

Training and Testing

Once appropriate individuals have been selected, they must receive sufficient training to perform all duties required of their positions. *Training* is defined as, ''the formal procedure which a company utilizes to facilitate learning so that the resultant behavior contributes to the attainment of the company's goals'' (Yoder and Heneman, 1979, p. 33-1). In our case, the company is the security department, and the goal is to administer the building's security and fire life safety program effectively.

Three Key Training Areas

A high-rise training program can be separated into three distinct areas.

New Employee Orientation

This basic training can introduce basic security concepts as they relate to high-rise building security and fire life safety programs. Areas to consider are:

- What is security and fire life safety?
- Building and assets protection
- Security systems and equipment
- Security rules and procedures
- Mobile patrol techniques
- Fire life safety systems and equipment
- Fire prevention
- Standards of Conduct and Code of Ethics
- Security and the law (including private security powers)
- Role of public relations
- Effective communications
- Interview techniques
- Observation techniques and report writing
- Uniform policies and grooming standards

Such training may include written materials, audiovisual aids, interactive computer programs, and classroom instruction from competent personnel. Testing, whether it is written, verbal, or practical, should be used to evaluate the trainee's performance.

On-the-Job Training

On-the-job training, basic orientation training referred to as OJT, will commonly vary in length from 8 to 40 hours, depending on the complexity of the building and the position for which the person is being trained. The training should orient the person to the building and its security and fire life safety program, equip the trainee with the necessary skills and job knowledge to carry out the responsibilities of the designated position, and help build confidence through hands-on experience. Activities to include are:

- A tour of the building exterior, selected tenant floors, passenger and freight/service elevators, stairwells, parking areas, loading dock areas, roof areas, and maintenance spaces (including mechanical areas and elevator machine rooms)
- Inspection of building fire life safety systems and equipment,* including the types of fire detection and fire suppression devices
- Inspection of building security systems and equipment
- Review of building security rules and procedures
- Review of building occupant fire life safety instruction
- Review of security instructions or post orders, including the complete job description for the trainee's position, and emergency response procedures
- Explanation of the chain of command within building management and the security department
- Orientation to the designated position
- Any specialized training such as first aid, cardiopulmonary resuscitation (CPR), and automated external defibrillator (AED) may be administered during the training session, or within an agreed-on period following assignment

There are several problems associated with OJT. Its quality will depend largely on the competency of the trainer; if this person has performance defi-

*How to conduct a building walkthrough focusing on its fire life safety features is detailed in Chapter 11, in the ''Building Emergency Staff Training'' section.

ciencies, they will be passed on to the trainee. What is learned will depend on what events occur during the training (some areas may be missed simply because on that particular day some routine events did not occur), and the training itself may interfere with the job that is being demonstrated. Written, verbal, and practical tests should be used in OJT to evaluate comprehension and performance and help ensure that the trainee has acquired the necessary skills to assume the responsibilities of the position. The extent and complexity of these tests will depend on the size, intricacy, and requirements of the security operation. Appendix 8-2 shows a *Sample Security Officer Basic Training Test*.

Ongoing or In-Service Training

After employees have been assigned to work, follow-up checks must be made on their performance. Employees should be kept constantly informed of changes in the security program and undergo ongoing instruction and testing in key areas. Nowhere is this better demonstrated than with security personnel who handle building emergencies such as fires and fire alarms. Such events usually do not occur on a daily basis in buildings (if they do, an investigation should be conducted to determine the reason), but security staff need to be in a state of readiness to handle them competently. This is only possible if staff periodically rehearse the procedures that are involved. Hands-on practice, drills, and testing (verbal and written) are all components that assist in this learning process.

Ongoing training can also be facilitated by handouts of written policies and procedures, pamphlets, newsletters, films, videos, interactive computer programs, meetings, briefings, conferences, panels, seminars, and workshops. Also, staff may be given self-instructional material and then be required to satisfactorily pass a written test.

Quality assurance audits by security supervisors are essential. If certain procedures are not being performed correctly or with confidence, the procedure may need to be re-evaluated and retraining administered. Inconsistencies or perceived problems in security may be a prompt for training. For example, tenants may complain to building management that after normal business hours they sometimes are challenged to produce passes to remove property from their building and sometimes are not. The supervisors should check that all security personnel fully understand the building property removal control policy and are aware of the need to consistently apply it.

The training program for each person should be thoroughly documented. Training files should be established for every member of the building security department. A *Security Officer Training and Testing Log* (see Appendix 8-3 for a sample) can be used to summarize each individual's training and testing.

Supervision

When an individual is appointed to a supervisory position, special training may be needed to equip him or her with supervisory skills. *Webster's College Dictionary* defines *supervise* as, ''to watch over and direct (a process, work, workers).'' A *supervisor* is a person who watches over staff or the labor performed by others. In high-rise security, supervisors guide and direct staff to perform assigned responsibilities determined by the building's security and fire life safety program. Let us examine this further.

There are various ways to watch over staff employed in a high-rise facility.* First, managers and supervisors might visit each position or post staffed by security personnel to observe and evaluate an individual's performance. Visits may include watching officers carry out their duties and responsibilities, asking them to demonstrate the operation of equipment, reviewing their written reports, and posing hypothetical situations to evaluate officers' responses. Some other aspects of supervision are now explored.

Patrol Monitoring Devices

Security staff activities, such as mobile (or beat) patrols or rounds, can be supervised using portable patrol monitoring devices. These devices may be mechanical clocks fitted with a graduated paper roll or disk or electronic guard tour systems. Both systems generate a record of patrol activity and can be used to evaluate and control the performance of the patrolling officer. ''They provide the security manager with a consistent record of rounds and occurrences at a facility without the need for human supervision to ensure that rounds are completed as assigned'' (Roughton, 1989, p. 52). A description of these two patrol management devices follows.

Mechanical Clock

Patrol officers may carry the *mechanical clock* (commonly called a *watchman's clock* or *watchclock*) around on patrol. At certain tour locations, pre-installed keys are inserted into an opening in the clock. This causes the date, time, and key number to be recorded on paper housed within the clock. Supervisors are provided a master key that enables the clock to be opened to review records of tours, to wind the clock or to replace batteries, to reset the date and time, and to replace the paper roll or disk.

Unfortunately, an unscrupulous security officer working alone in an area can fabricate a patrol. This is done by removing keys from the designated tour stations at the beginning of the shift, taking them (lined up in their original order) to a central location, and then turning them in the clock at the required times (for instance, every hour), thereby simulating the tour. The keys are then returned to their original locations at the end of the shift. Supervisors can defeat this scam by firmly securing the keys to their stations using screw flanges and requisite screw head ''seals'' to prevent tampering, visiting a patrol officer at unannounced times during a shift and inspecting key stations, or reviewing CCTV recordings of aspects of the officer's patrol.

Patrol personnel should never be issued a master key to the clock (although provision might be made to provide supervised access to the master

*High-rise tenants can also contribute to the supervisory process by promptly communicating any difficulties with security staff either to building management or directly to the security department.

key in the event that the clock malfunctions). As an added precaution, the tape or disk is automatically marked each time the clock is opened so supervisors can inspect for non-authorized access.

The mechanical clock can sometimes be cumbersome to carry and made inoperable by being dropped or impacted with a heavy object. Since the 1980s, it has met with stiff competition from electronic guard tour systems.

Electronic Guard Tour System

An *electronic guard tour system* functions either alone or with software. It consists of a *reader* that may be of various shapes and sizes and includes either a contact wand or a non-contact laser scanner. The reader or data acquisition unit is carried around during the patrol by the officer and at certain tour stations preinstalled data strips or disks are ''read'' by the reader, recording information such as date, time, station number, and location. The stations may be barcodes, magnet strips, chips, or metal disks. Data can be transferred from the reader to a computer or printer by placing the reader in a cradle or data transfer unit or by connecting the reader directly to a printer.

Advantages of Electronic Guard Tour Systems

Some advantages of electronic guard tour systems over mechanical clocks are:

- Readers are smaller and lighter than traditional mechanical clocks.
- The data strips are small, unobtrusive, and easy to install and can be colored to match their surroundings.
- Some readers allow the patrolling officer to include information such as observations made at each tour station.
- The printout of information is easier to read than that generated by traditional mechanical clocks. Some systems have the additional advantage of being able to print the data out in various ways, showing the name of the patrolling officer, the length of the tour, tour stations completed, and exceptions to the tour (including stations missed or duplicated). Data also can be saved to a computer file for later reference.
- Most systems are virtually tamperproof.

''Guard tour management systems not only provide the security officer with a sense of added responsibility and feeling of self-worth, but generate accurate reports that verify the effectiveness of each tour or patrol'' (Minion, 1992, p. 10).

Patrol monitoring devices frequently are deployed in building towers, zigzagging from floor to floor at stairwells; in mechanical rooms and other areas that may contain sensitive equipment that needs to be regularly monitored; in exterior areas, such as plazas, parks, and gardens; and in parking areas. These systems not only provide a documented means to monitor the patrol activity of security staff, but also can provide valuable evidence to explain, for example, why there was a delay in an officer observing an incident (if the officer is shown to have been at another location). They also can be used to determine the approximate time of an occurrence (for example, if an officer is seriously injured while on patrol, the last station visited will assist in determining the time the incident occurred).

In addition to the two systems just described, electronic card access systems can be used to monitor patrol activities. Each patrol officer can be issued a card to access certain areas while on patrol. The records obtained from the card access system can then be used to review patrol activities.

Patrols in High-Rise Buildings

Mobile patrols may be conducted in high-rise buildings for a variety of security and fire life safety purposes. "Guards [security officers] are typically highly visible thus offering something of a deterrent effect and at the same time imparting a sense of security to the building's tenants and visitors" (Vitch and Nason, 1995, p. 60). Patrolling increases this visibility. Patrols can also be used to note and quickly address anything significant or unusual affecting security or safety. The frequency and route of these patrols can be predetermined by building management and the security department and then documented.

Some municipalities require security officers to perform fire loss prevention duties to protect facilities that do not have an "approved protective signaling or electronic monitoring system" (NFPA 601, 2000). Starting within one-half hour after operations in a facility normally cease, these persons must perform *hourly* rounds unless the authority having jurisdiction allows the rounds to be conducted at less frequent intervals. NFPA 601, *Standard for Security Services in Fire Loss Prevention*, outlines such security officer functions and duties.

Fire Watch

A *fire watch* may be required when a building or premises has exceptional hazards or the fire protection system is impaired. In this case, additional patrols at appropriate intervals determined by the fire department are conducted with the purpose of "notifying the fire department and/or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety danger" (NFPA *Glossary of Terms*, 2001).

Patrols in High-Rises

Unless otherwise specified by the authority having jurisdiction, patrols in high-rise office buildings may be conducted as follows:

- For approximately the first hour after opening the building on a regular business day, when there are not many occupants in the building, to provide a security presence throughout common areas and tenant floors
- After the building is closed at the end of the business day, on tenant floors, to check for suspicious persons and doors left unlocked
- When the building is closed, throughout all common and maintenance areas (including stairwells), to monitor equipment and report obstructions, fire hazards, water and/or gas leaks, wet floors, holes, defects in floor coverings, unsecured areas, signs of forced entry, unauthorized or suspicious persons, etc.

- Continuously in parking garages to deter theft of vehicles and property within them; note parking violations and issue warnings or citations; observe vehicle lights or engines left on, leaks from vehicles, or other unusual conditions of parked vehicles; and provide for the general safety of tenants (bicycles and motorized vehicles, such as golf carts, may be used for patrolling large parking areas with long travel distances)
- Depending on a building's usage, in areas such as retail arcades, public parks, and other common areas (in some facilities, the patrol officer carries a pager, mobile telephone, or hand-held panic alarm so that tenants, particularly retailers, can summon the officer for assistance)

In some high-rise office buildings, security personnel perform periodic patrols within tenant spaces. This practice might place the patrol officer in ''difficult and sensitive'' situations, particularly after normal business hours. If it is necessary for a security officer to enter a tenant area after hours, another officer, an engineer, or other building staff should accompany him or her. They should knock on the door before opening it, and call out loudly to identify themselves and their intentions. Such actions can help avoid embarrassing and awkward situations and protect staff from unfair accusations. Intrusions into tenant space should always be documented.

Guiding and Directing Security Staff

Various ways and means can be used to guide and direct security staff to perform responsibilities as determined by the building's security and fire life safety program. First, employees need the following basic tools to do their job:

- A well-defined security and fire life safety program with clearly documented and communicated building policies and procedures
- Security and fire life safety systems and equipment that are adequate for the building's program and are maintained in good working order
- Up-to-date, thorough, accurate, concise, and clearly defined security and fire life safety instructions that are readily available for reference
- Comprehensive and well–designed orientation, training, and testing programs for security staff

Importance of Adequate Amenities

Security staff personnel need a working environment in concert with their required professional image. Building owners and managers often overlook amenities such as well-maintained changing areas, secure storage areas for personal belongings, adequate restrooms, and break areas, but these are essential to the welfare and morale of security staff. Supervisors should, if possible, have access to a private area where counseling can be conducted in a professional setting with minimal distractions. If the security department is large enough to warrant a Director of Security, a private office should be provided where the director can work and safely store reports and confidential employee files. It is not uncommon to find high-rise buildings in which security staff are required to change uniforms in corridors or public restrooms, security uniforms are stored in building fan rooms, there are nonexistent break areas, and the Director of Security is housed ''under the stairs'' or in an area where no privacy or adequate work space is afforded. These conditions lower the morale of the entire security department and can contribute to a less than professional attitude of security staff at work.

How to Motivate

To motivate employees to perform better, work harder, and stay interested in what they are doing, the following actions produce positive results when practiced by security supervisors.

- Taking a genuine interest in employees and treating them with courtesy and respect.
- Knowing the strengths and limitations of employees and assigning them to positions of responsibility that match those strengths and limitations.
- Adequately training and testing employees so they know what is expected of them.
- Communicating clearly, concisely, and in a timely fashion so that employees can adjust to any requested changes in duties and responsibilities.
- Actively listening to employees and encouraging their ideas and input—''Sarah, what do you think we can do about the recent vehicle break-ins?''
- Being decisive and avoiding vacillation.
- Viewing each staff member as a unique individual and approaching him or her in an appropriate manner.
- Making requests of employees rather than giving direct orders—''Kevin, would you help Philip over at the Loading Dock?'' The problem with direct orders is that people sometimes disobey them. If a person refuses to comply, then the supervisor's authority and ego are challenged. Of course, direct orders are needed under certain circumstances.
- Giving positive feedback, compliments, and recognition to employees—''Searcy, thank you so much for the great job that you did handling the special event today.''
- Performing periodic employee performance reviews and evaluations.
- Assisting employees to develop skills and self-confidence and encouraging them to accept responsibility.
- Assisting employees' advancement and promotion within the organization.
- Supporting employees, particularly during difficult personal situations that they may be experiencing.
- Handling complaints from employees in a timely, fair, and equitable manner.
- Not making promises or commitments that cannot be met.
- Admitting a mistake when it has occurred, and apologizing when necessary or appropriate.
- Maintaining a professional Code of Ethics and Standards of Conduct and not compromising personal standards.

Employee recognition programs are an important tool in staff retention, boosting morale, raising the quality of service rendered by security staff, and reducing overall operational costs. It decreases staff turnover, thus reducing the amount of training and supervision required. Security staff who carry out responsibilities in a competent and professional manner may be recognized by an award for employee of the month, quarter, or year; or for an outstanding job performed in handling a particular situation; or for length of service. The recognition program may take the form of a letter of appreciation, newsletter write-up, certificate, plaque, personalized badge, tie tack, pin, gift voucher, or a cash award. Such recognition of security staff members often motivates others to excel.

Discipline

Discipline is an effective and necessary tool of supervision. The word *discipline* is derived from the Latin word *discipulus*, which means learning. *The Encyclopedia of Security Management* states that ''the word conveys an important concept in supervision, i.e., that discipline is a mechanism for correcting and molding employees in the interests of the organization. Punishment, the negative aspect of discipline, is tangential to the larger purpose of fostering desirable behavior'' (Fay, 1993, p. 234). Fay adds that there are certain principles that need to be taken into consideration when an employee is being disciplined:

Principle 1—Assume Nothing. Ensure that everyone knows the rules. Put the rules in writing; make them a regular item of discussion in formal and informal sessions; disseminate and display them prominently. An employee who does not know the rules cannot be expected to follow them, and a supervisor should not discipline an employee when there is doubt that the employee was aware of the rule.

Principle 2—Discipline in Privacy. Receiving discipline is never a pleasant experience and can be particularly unpleasant in the presence of co-workers or others who have no legitimate role in the process. Embarrassment, anger, and resentment are the natural emotions that follow criticism given publicly. Discipline is a private matter to be handled behind closed doors or in a setting that ensures absolute privacy.

Principle 3—Be Objective. Rely on facts, not opinions and speculations. Consider all the facts and examine them with an open mind. Look for and eliminate any biases, for or against the offender. Make sure there is in fact a violation and determine the relative severity of the violation. Was the offender's act aggravated or mitigated in any way?

Principle 4—Educate the Violator. Administer discipline that is constructive. The purpose is to bring about a positive change in the violator's conduct or performance. Discipline should be a learning experience in which the violator gains new insights that contribute to personal improvement.

Principle 5—Be Consistent. Inconsistent enforcement of policy and rules should be totally unacceptable. For example, if the policy of the department is to terminate officers who sleep on the job, then all officers so [found] must be terminated. To fire one and not another will breed contempt for the rules and those who set the rules [and can result in formal labor complaints and/or lawsuits].

Principle 6—Do Not Humiliate. The intended outcome is to correct, not hurt. When humiliation is made a part of the process, the offender will come away angry, resentful, and perhaps ready to fail again. Both the offender and the organization will suffer as a consequence.

Principle 7—Document Infractions, Counseling, Discipline, and Corrective Actions. Make a record of violations. This is not to say that a negative dossier should be maintained on each employee, but it does mean that instances of unacceptable performance have to be recorded. The record of an employee's failures is valuable as substantiation for severe discipline, such as termination, or as a diagnostic aid to counseling professionals.

Principle 8—Discipline Promptly. With the passage of time, an uncorrected violation fades into vagueness. The violator forgets details, discards any guilt he or she may have felt at the time of the violation, and rationalizes the violation as something of little importance. When opened for discussion, an uncorrected violation is likely to lead to disagreement about what ''really happened'' and any disciplinary action at that point can appear to be unreasonable (Fay, 1993, pp. 234–235).

Generally speaking, most employees want to do a good job. If an employee is having performance problems, however, the supervisor must discipline in a professional manner and focus on the problem, not the personality of the offender. The intention is to train, develop, and improve performance and, perhaps, to rescue a valuable employee from failure.

Training Supervisors

In providing comprehensive training to new or experienced security supervisors, the following areas should be addressed:

- Responsibilities and duties
- Leadership skills
- Communication skills
- How to develop relationships
- How to avoid sexual harassment
- How to avoid favoritism
- How to handle complaints
- How to conduct inspections
- How to document inspections
- How to counsel and discipline
- How to conduct performance evaluations
- Organizational skills
- Time management
- Stress management

Sometimes when non-supervisory employees are promoted to supervisory positions, they need to be taught to think and behave as supervisors rather than as line employees, and to alter their interactive relationships from ''peer-to-peer'' to ''supervisor-to-subordinate.'' If they do not make this transition they will not become effective supervisors. As Vail (1993, p. 56) states,

> The best leaders know themselves, their strengths, their weaknesses, their skills, and their abilities. Most of all, they know how to control themselves and present a commanding image that will inspire subordinates. They commit themselves to continually developing leadership characteristics in themselves and their subordinates.

Uniforms and Equipment

There are various types of uniforms and equipment that can be supplied to security staff working in a high-rise environment. Uniforms are an essential part of the security staff image. Those who are well groomed; out-fitted in well-tailored, clean, and pressed uniforms; and have clean, well-polished, and appropriate footwear exhibit a professional appearance. In so doing, their overall effectiveness is considerably enhanced. (A side benefit of each staff member having a professional appearance is the boost in confidence they receive.)

The image that building owners and managers desire security staff to exhibit will determine the style and selection of uniforms. Because many security personnel are viewed as service providers and ambassadors of the building, uniforms tend to project a military-law enforcement image less, and the professional concierge image more.* Instead of security patches and badges, staffs usually are outfitted in a 'soft-look' uniform of tailored slacks, white dress shirt, business tie, and blazer, or, in some instances, a tailored business suit. Often a discreet nameplate identifying the wearer, and possibly a monogram of the building's logo on the blazer or suit coat pocket, are the only identifying marks on the uniform.

It is highly unusual for security staff assigned to high-rise office buildings to be armed with weapons of any type. The type of businesses conducted and the large number of people who frequent these facilities make it undesirable and potentially dangerous for the use of weapons such as firearms, chemical agents, aerosol propelled agents, and nightsticks or batons. The chances of a building tenant, visitor, or innocent bystander being injured in a situation involving a weapon are high.

However, some high-rise building tenants (such as retail banking institutions) do employ armed security personnel within their premises, and some corporate executives retain armed executive protection staff. Also, for example, during periods of civil unrest, some buildings have used civilians trained and certified to carry concealed weapons to supplement unarmed security staff. However, such deployment is unusual in the high-rise setting and is generally reserved for special and unusual circumstances.

The Role of Public Relations

Public relations play a vital role in the administration of the security function in a high-rise building. Security personnel are exposed to all types of people in their daily work. They are expected not only to provide directions and information about the building and its locale, but also to persuade people to cooperate willingly with the security program. In carrying out these responsibilities, they are required to conduct themselves in a professional manner at all times. How effectively they interact with these people directly influences the overall image of security in the building and indirectly reflects on the building owner or manager and the tenants. High-rise building owners are always

*However, some high-rise security officers, particularly those conducting exterior patrols and working in ''back-of-the-house'' areas such as vehicle inspection areas, parking garages, loading docks, shipping and receiving areas, and freight and service elevators, are dressed in ''military-style'' uniforms.

striving to attract and retain good tenants. Building security especially can contribute to the achievement of this goal.

Public relations entails creating kindly feelings and positive interaction between an organization and the public. It should not be identified with the image of a slick salesperson promoting a product. Rather, in the security context, it implies professional and well-trained staff interfacing with the public in a manner that favorably reflects upon their department and the building. Good public relations helps staff to carry out the roles and objectives of the building security program effectively, and can be an invaluable tool in getting people to comply willingly with security rules and procedures. To create the positive impression so essential in human relations, security staff should:

- Be well groomed with good personal hygiene
- Be outfitted in clean, well-tailored, and pressed uniforms with clean, well-polished, appropriate footwear
- Have what is best described as a ''military bearing,'' whether he or she is sitting or standing
- Have a smile on his or her face at the appropriate time
- Maintain good eye contact with people, particularly when talking with them.
- Use hands, arms, or head in a nonthreatening way
- Practice good listening skills and speak politely and courteously, using key phrases and words such as ''May I help you?'', ''Please,'' and ''Thank you''
- Remain calm, avoiding outward displays of emotion when confronted with hostile or hazardous situations
- Carry out duties and responsibilities with decisiveness and consistency

> Good human relations for the security officer begins with an interest in people and in their safety and welfare. When successful, it produces mutual good feelings and willing cooperation. Cooperation is the real meaning of good human relations at all levels. . . . It is only through cooperation of all concerned that security officers can carry out the mission of protecting people and property. Good human relations is the basis of good security. (American Protective Services, 1980, p. 2)

Security System Maintenance and Replacement

An important function of the security department is to ensure that building security systems and equipment continue to work properly. Depending on the building, this responsibility may vary from simply communicating problems to building management, to calling for maintenance service from system vendors, to actually having a systems specialist on staff responsible for the entire security system.

Also, when systems and equipment become unreliable and outdated, the responsibility for upgrading or replacing them may reside with the security department. Because the security requirements of a building may have changed since the original system was installed, a system upgrade presents an opportunity to re-evaluate needs and acquire a system that will more comprehensively and efficiently address those needs.

Summary

In carrying out a successful security program in a high-rise office building, it is essential that it be adequately funded. The security staff that oversee and implement the program may be directly employed by the building owner or manager (i.e., proprietary or in-house) or by a contract security firm (i.e., contract). If the latter, it is critical that special care be taken to select a professional contractor. There should be adequate numbers of quality security personnel to carry out the responsibilities and duties of a building's security program. These duties should be documented in comprehensive security instructions that are clear, concise, accurate, periodically reviewed, and regularly updated. All security staff must be properly selected, trained, tested, supervised, uniformed, and equipped to perform their job in a professional manner.

References

Allied Security, Inc., *A Guide to Contracting for Guard Services* (Copyright Allied Security, Inc., Pittsburgh, PA, 1983).

American Protective Services, Inc., ''The meaning of human relations,'' *Human Relations: The Notebook Lesson Series for Security Officers* (American Protective Services, Inc., Oakland, CA, 1980).

American Protective Services, Inc., ''Skills of the security officer,'' *High-Rise Training Course* (American Protective Services, Inc., Oakland, CA, 1990).

Azano, Harry J., *Fire Safety and Security for High-Rise Buildings*, (Abbott, Langer & Associates, Crete, IL, 1995).

Bates, Norman D., ''The power of paperwork'' (*Security Management*, Arlington, VA, May 1995).

Colling, Russell L., ''Security staff organization,'' *Hospital and Healthcare Security*, 4th ed. (Butterworth–Heinemann, Woburn, MA, 2001).

Denekamp, Mark L., ''PCs and security: a perfect match,'' *Security Management* (Arlington, VA, January 1989).

Fawcett, Martin A., International Foundation for Protection Officers (IFPO), ''Field notes and report writing,'' *Protection Officer Training Manual*, 5th ed. (Butterworth–Heinemann, Stoneham, MA, 1992).

Fay, John, ed., *Encyclopedia of Security Management: Techniques and Technology* (Butterworth–Heinemann, Stoneham, MA, 1993).

Ferrell, O. C., Gardiner, Gareth, ''Honesty may be the best policy but some days it's tough,'' *In Pursuit of Ethics: Tough Choices in the World of Work* (Smith Collins Company, Springfield, IL, 800/345-0096, 1991).

Geiger, Geoff, Craighead, Geoff, ''Minding the store: office security is big business'' (*Los Angeles Business Journal*, Los Angeles, July 1991).

Giambalvo, Thomas W., ''Old partners, new partnering'' (*Security Technology & Design*, Cumming, GA, November 1998).

Keating, Thomas K., ''Site supervisors—a critical link,'' *The Vigilant* (American Protective Services, Inc., Oakland, CA, December 1994).

Minion, Ronald R., *High Rise Building Security* (International Foundation for Protection Officers, Bellingham, WA, 1992).

NFPA 601, ''Security functions and duties,'' *Standard for Security Services in Fire Loss Prevention* (Used with permission of the National Fire Protection Association, Quincy, MA, Copyright 2000).

NFPA *Glossary of Terms* from the National Fire Code (National Fire Protection Association, Quincy, MA, 2001).

O'Hara, Charles E., and Gregory L. O'Hara, *Fundamentals of Criminal Investigation*, (Charles C. Thomas Publisher, Springfield, IL, 1994).

POA, ''Training,'' *Protection of Assets Manual*, vol. IV,10th printing. Timothy L. Williams, editor (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887, 2000. Original copyright from the Merritt Company, 1991). Merritt Company stated the Berman, Bennet H. quote was in the *Nation's Business*, January 1980, page 30B.

PPM 2000 Security Management Software InCase System (PPM 2000 Inc., Edmonton, Alberta, Canada, 1990–1993).

Roughton, Jim, ''Scanning the lines for security,'' *Security Management* (Arlington, VA, January 1989).

Sennewald, Charles A., ''Planning and budgeting,'' *Effective Security Management*, 3rd ed. (Butterworth–Heinemann, Woburn, MA, 1998).

Vail, Christopher L., ''What good supervisors are made of,'' ASIS Reprint Series (*Security Management*, Arlington, VA, 1993).

Vitch, Martin L., Nason, Randall, ''High-rise security issues,'' (*Security Technology & Design*, Cumming, GA, August 1995).

Webster's College Dictionary, 1992 Edition (From *Random House Webster's College Dictionary* by Random House, Inc. Copyright © 1995, 1992, 1991 by Random House, Inc. Reprinted by permission of Random House, Inc., New York, 1992).

Yoder, D., Heneman, H., eds., *American Society of Personnel Administrators' ''Handbook of Personnel and Industrial Relations''* (Bureau of National Affairs, Washington, D.C., 1979), as reported in ''Training,'' Part I, *Protection of Assets Manual*, vol. IV (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, 1991).

Additional Readings

Aggleton, David G., (POA Bulletins, April–October 2000), *System Implementation* and *System Procurement* (POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Copyright 2000). An explanation of the processes need to perform a major security system upgrade

McCrie, Robert D., *Security Operations Management* (Butterworth–Heinemann, Woburn, MA, 2001).

Sennewald, Charles A., *Effective Security Management*, 3rd ed. (Butterworth–Heinemann, Woburn, MA, 1998).

Appendix 8-1 NASCO Security Officer Code of Ethics

As a private security officer, I fulfill a vital function in the preservation and well-being of those whom I serve. In doing so, I pledge:

- To serve my employer and clients with loyalty and faithfulness, respecting the confidentiality of my job.
- To fulfill my duties in full compliance with the laws of the land.
- To conduct myself professionally at all times, and to perform my duties in a manner that reflects credit upon myself, my employer, and private security.
- To be fair and impartial in discharging my duties without prejudice or favoritism.
- To render reports that are complete, accurate, and honest.
- To remain alert to the interests of the client and the safety of those whom I serve.
- To earn the respect of my employer, clients, and fellow officers through my personal integrity and professionalism.
- To strive continually to improve my performance through training and education which will better prepare me for my private security duties.
- To recognize my role as that of a private security officer.

Reprinted with permission of the National Association of Security Companies (NASCO), 1995.

Appendix 8-2 Sample Security Officer Basic Training Test

NAME: ___________________________

POSITION/POST: LOBBY OFFICER ______________________

DATE: _________________________

1. What is the address of the building?

   ____

   ____

2. On what floor is the Office of the Building located?

   ____

   ____

3. What are the normal operating hours of the building? (Circle the correct one)
   - 6:00 A.M. to 7:00 P.M., Monday to Friday
   - 7:00 A.M. to 6:00 P.M., Monday to Friday.
4. What time do you secure the lobby doors?

   ____

   ____

5. When do building elevators go into the security mode?

   ____

   ____

6. If a visitor to the building asks an important question about the building operation that you cannot answer, what do you do? (Circle the correct one)
   - Tell the person you don't know the answer and you cannot help them
   - Tell the person that you do not know the answer but that you will call your supervisor to assist
   - Tell the person they have no business asking questions about the building
7. As a private security officer you have the same rights as a police officer. (Circle the correct one)
   - True
   - False
8. If a person enters the lobby and asks you how to get to the roof of the building, what do you do? (Circle the correct one)
   - Direct the person to the service elevator
   - Politely tell the person that under no circumstances is anyone permitted to travel to the roof
   - Direct the person to the Office of the Chief Engineer
9. If the person becomes upset, starts yelling obscenities, and refuses to comply with your wishes, what do you do? (Circle the correct one)
   - Try to calm the person. Call for the assistance of your supervisor
   - Yell back at the person.
10. If a person carrying a weapon enters the lobby, what do you? (Circle the correct one)
    - Inquire as to what floor they want to find
    - Carry out the procedures as outlined in your security instructions
    - Run screaming out of the lobby
11. In the situation just mentioned, describe what your first action would be.

    ____

    ____

12. If a delivery person enters the lobby with a cart, where do you direct this person to go?

____

____

13. If a fire alarm sounds in the lobby, whom do you immediately notify? (Circle the correct one)
    - The fire department
    - All occupants in the lobby
    - Building Management
14. If an earthquake occurs while you are in the lobby, what is your first action? (Circle the correct one)
    - Run out of the building lobby
    - Take an elevator to an upper floor
    - Move near an interior wall away from light fixtures, tuck your head to your knees, and cover your head with your arms to protect against falling objects
15. List six essential ingredients of any successful report of an incident.

___________________ ___________________

___________________ ___________________

___________________ ___________________

16. After normal business hours, if a building occupant exits the passenger elevator carrying a personal computer and several large boxes, what do you do? (Circle the correct one)
    - Ask if you can help carry the items to their vehicle
    - Tell the person they cannot remove anything from the building and request that they return the property to their office
    - Politely request a Building Property Removal Pass
17. If the person carrying the property has a Building Property Removal Pass but it is not filled out, what do you do? (Circle the correct one)
    - Take the pass and tell the occupant you will fill it out for them
    - Politely request that the occupant return to their office to have the pass completed before the property leaves the building
    - Let the person leave with the property and tell them to return the completed pass the next business day
18. What is the building policy for handling solicitors?

____

____

19. When the building is closed, a person dressed in coveralls asks to be allowed admittance to service a vending machine on a tenant floor. What do you do? (Circle the correct one)
    - Allow this person to do so on the understanding that they return to the lobby as soon as their work is completed
    - Request identification and allow the person to proceed to the tenant floor
    - Politely tell the person that the building is closed and that Building Management does not allow after hours work to be conducted without prior authorization
20. If there is a smell of burning material in the lobby, what do you do? (Circle the correct one)
    - Ignore this observation
    - Immediately notify the Security Control Center and the Building Fire Safety Director
    - Tell no one and leave your post to investigate the odor
21. If an occupant spills a soft drink on the lobby floor, what do you do? (Circle the correct one)
    - Go to the loading dock to get a cloth to clean up the spill
    - Leave it because it is a hot day and it will soon dry up
    - Cordon off the area and call for the assistance of a building janitor

Signature of the person being tested: _______________________________________

Signature of the supervisor conducting the test: ______________________________

Appendix 8-3 Sample Security Officer Training and Testing Log

NAME: ______________________

POSITION/POST: ______________________

Program/Procedure	Date(s) Trained				Date(s) Tested			
Employee Orientation								
Building Tour and Familiarization								
Inspect Building Security Systems and Equipment								
Review Building Security Program								
Review Security Instructions or Post Orders Standard Operating Procedures								
Inspect Building Fire Life Safety Systems and Equipment								
Review Building Fire Life Safety Program								
Review Building Emergency Procedures Manual								
Review Specific Post Duties and Responsibilities								
Specialized Training (CPR, First Aid, AED, etc.)								

Note: Each training and testing should be initialed by the Security Supervisor conducting the training.

9 *Investigations*

An *investigation* is an objective, fact-finding, systematic inquiry into particular incidents, conditions, subjects, or behavior with a specific, predetermined purpose in mind. A *fact* is an event that has actually occurred or is known to be true. The inquiry not only involves gathering relevant information, but also involves making assumptions and logical conclusions based on that evidence.

Evidence is anything that tends to prove a fact or support a conclusion. According to American Protective Services (1980, p. 14), there are three kinds of evidence:

1. Physical evidence—objects, materials, documents
2. Stated evidence—what people such as victims, witnesses, suspects, and technical experts say
3. Circumstantial evidence—facts that lead to a logical or at least likely conclusion

Owners and managers of high-rise office buildings may become involved in many types of investigations pertaining to security and fire life safety matters: analysis of specific events or certain conditions; examination of complaints about a particular building policy, a procedure, or a person; investigation of a crime, suspected crime, or some other infraction (criminal or civil actions); and physical or electronic surveillance of someone or something.

This chapter not only addresses the methodologies of conducting these specific investigations, but concentrates on the general principles involved in gathering, organizing, and evaluating information to properly establish the facts of an investigation. It does not address background investigations—pre-employment histories of job candidates or financial and lifestyle inquiries of present employees—or in-depth fire and explosion investigations.

Nature of Investigations

Tenants; building owners and managers; security staff; licensed private investigators; public law enforcement or the fire department; and various other municipal, state, and federal agencies may carry out investigations in high-rise buildings. These investigations may be informal or formal.

Informal Investigation

An informal or casual investigation involves something unusual or important being observed and then questions being asked or further observations made regarding the matter. For example, a member of building security staff, while patrolling a parking garage that has recently experienced thefts from several vehicles, encounters a person attempting to unlock an expensive automobile using a wire coat hanger. On questioning, it is discovered that the individual is the owner of the vehicle and locked his keys inside.

Formal Investigation

''A formal investigation may be conducted in response to a major incident or threat, or in response to a complaint. It is more organized than the casual investigation and proceeds through fairly well-defined stages'' (American Protective Services, 1980, p. 2). For example, an event that warranted such an investigation involved a fire that occured after normal business hours in the office of a building tenant. Analysis by a fire department arson investigator revealed that the fire was started by a lighted cigarette butt found in the wastepaper receptacle underneath a desk in the gutted office. A check of the building's after-hours access register revealed that the tenant whose office was involved had signed out of the building 20 minutes before a fire sprinkler alarm for the floor in question was received in the Fire Command Center. A subsequent interview of the tenant by an insurance investigator revealed that the tenant did in fact throw a lighted cigarette butt in the trash bin minutes before leaving the building on the night of the fire. Another example of a formal investigation involved the following:

> Several occupants from one tenant complained that over the past 2 months business items such as calculators, laptop and notebook computers, and personal belongings—cash, small mementos, and valuable pens—had been stolen from their offices. Building management, in conjunction with the tenant office manager, arranged for a covert surveillance camera to be placed in one of the areas where the thefts had occurred. This camera was connected to a video recorder. The recording from the third day showed a tenant employee who walked into the office at 7:00 PM, after most workers had left, and proceeded to rifle through desk drawers and place petty cash and an unsecured laptop in a briefcase and leave the area. The next day, the tenant's head of human resources conducted an interview with the employee. The employee, a trusted worker who had been with company for 10 years, admitted to the offenses and subsequently resigned.

The types of actual or suspected crimes that more commonly require investigation in commercial office buildings include petty theft or larceny, vandalism, trespass, burglary and unauthorized entry, and, less commonly, crimes of violence such as murder, manslaughter, robbery, assault, rape, and acts of arson and terrorism.

There are basic methods for conducting criminal investigations. Although it is not within the scope of this book to detail these methods, it is important to mention that the focus of these investigations will vary depending on whether they are conducted within the private sector or by a public agency.

Private Sector and Public Law Enforcement Investigations

The primary objective of a criminal investigation by public law enforcement is to serve the best interests of society by identifying and prosecuting offenders, whereas in the private sector the primary objective is to serve the best interests of the organization concerned. As Sennewald and Tsukayama explain,

> It is interesting to note that what serves the best interests of society may not necessarily serve the best interests of the organization, and vice versa. For example, the society's interests are protected when an embezzler is prosecuted and sentenced to prison. There are occasions, however, when the embezzler, having banked all his thefts, would be happy to return the stolen funds in order to avoid prosecution. Such an agreement would be unacceptable in the public sector. A seasoned private sector investigator, on the other hand, is not primarily concerned with prosecution and sentencing. Recovery of the loss might be a more important achievement, better serving the interests of the private organization. (2001, p. 12)

Other factors that influence whether an investigation is carried out in the private or public sector are the nature of the crime and the resources available to conduct the investigation. The Merritt Company (1991, pp. 16-69, 16-70) explains,

> Although the crime is of interest to law enforcement (and hence a matter for police investigation), there may be considerable preliminary effort required [by tenants, building owners or managers, the building security department, and private investigators] even to establish the existence of a crime. The police, generally overworked in criminal investigations, will not undertake preliminary inquiries in most situations unless there is a clear threat to public order or the general welfare.

An incident that illustrates this point occurred in a large California highrise building.

> Over a period of 6 months, a number of thefts of blank checks from the middle or back of tenants' checkbooks occurred throughout the building. These checks were subsequently filled out and cashed at a local bank with individual amounts ranging from $500 to $3000. Often the thefts were not discovered for months because tenants did not realize until then that the checks were missing. The bank, when notified of the fraud, refunded the full amount of each forged check to the tenant concerned. The tenants, after receiving full restitution, were unwilling to cooperate with building management by making police reports of the stolen checks. After 6 months, the money involved in these thefts amounted to $50,000! To compound the issue, local law enforcement was reluctant to begin an investigation because they were overwhelmed with work and no official police reports had been filed. Eventually building management hired a private investigator and a suspect was later identified. The case was then handed over to local law enforcement.

Rights of Public and Private Investigators

The authority of a public investigator is based on constitutional and statutory law, whereas the authority of a private investigator is similar to that of a private citizen. As a private citizen, the private investigator has no right to detain people against their will for questioning. The authority to conduct a private investigation and request cooperation from tenants and visitors of a high-rise building comes from the rights of a building owner or manager, and tenants within their own tenant areas, to maintain order on their property.

Private investigators do not have the same right of access as public investigators to information such as criminal records that are available at municipal, county, state, and federal levels. Also, charges of entrapment (solicitation by police officers for crimes to be committed) may be leveled against private investigators. Fischer and Green (1998, p. 155) caution,

> While entrapment does not generally apply to private citizens (the case of State v. Farns [542 P.2d 725 Kan. 1975] is frequently cited to prove that entrapment does not apply to private citizens), several states have passed legislation that extends entrapment statutes to cover private persons as well as police officers. Until the issue is resolved in the courts in the next few years, security officers [and private investigators] involved in undercover operations should be careful to avoid actions that might lead to entrapment charges.

''Whatever the capacity in which [an] investigator functions (public or private), it is important that the investigator be informed regarding all relevant legal restrictions, requirements, obligations, standards, and duties. Failure to do so could jeopardize the reliability of any investigation and could subject the investigator to civil liability or criminal prosecution'' (NFPA 921, 2001, p. 9). However, private investigators are more susceptible than public investigators to civil actions resulting from their work. The private investigator acting on behalf of a private company or an individual is a far more attractive target for a lawsuit than the public investigator acting on behalf of a government entity. It is therefore essential to fully evaluate any private investigator hired to conduct an investigation to ensure that he or she is professional, well trained, highly skilled, and trustworthy.

Skills of the Investigator

To effectively conduct an investigation, the investigator must possess certain qualities or attributes. Charles Sennewald outlines 21 characteristics an investigator should possess, in varying degrees, either as innate or learned qualities (Sennewald and Tsukayhama, 2001, pp. 21–32).

> He or she should be observant, resourceful, patient, people-oriented, understanding of human behavior, knowledgeable about legal implications of the work, a skilled communicator, receptive, possessed of a sense of well-being, dedicated to the work, a self-starter, skeptical, intuitive, energetic, a good actor, capable of good judgment, logical, intelligent, creatively imaginative, of good character, and professional.

It is essential to assign each case to an investigator who has the expertise to conduct it. For example, if the investigation involves computer fraud, it would be wise to use an investigator who has experience in this area. An investigator who is not trained in computer operations will require the technical assistance of a computer consultant to conduct the investigation.

In addition, an investigator must always be thorough. A thorough investigation is one in which all possible leads have been pursued; key leads have been rechecked several times to make sure the results are accurate; wherever possible, crucial evidence has been corroborated from more than one source; and the investigation has been continued until all information relevant to the case has been obtained.

To demonstrate why such thoroughness is critical to supplying managers with accurate information on which to base decisions, consider this example.

> One evening a concierge finished work at her desk located in the lobby of a high-rise office building. Before leaving, she locked the desk and placed the desk telephone handset beneath it. When she arrived at work the next morning, she discovered that the telephone was missing. She immediately notified building security. They began an investigation by reviewing videotape obtained from the building's closed-circuit television (CCTV) system (a camera located in the lobby directly viewed the desk). The tape was reviewed starting from the time the concierge reported that she left the desk. This review revealed a scene where a building janitor came up to the desk in question, went behind the desk, momentarily stooped down, and then walked away apparently concealing something under his arm. The ''something'' could not be clearly observed, even when video prints were taken from the tape and the image enhanced. Building security interviewed the janitor involved. He denied any wrongdoing and said that he had passed by the desk but had not gone behind it. Because of the apparent inconsistency in the janitor's story and his suspicious behavior as depicted on the tape, the janitorial contractor was shown the videotape and asked to remove the janitor from working at the building. This was done, despite the janitor's objections that he had done nothing wrong.
>
> For several weeks after the incident the janitor, through the contractor, continued to protest his innocence. Building security decided to further review the videotape of the incident. This showed that an hour after the janitor went behind the desk, the same janitor came up to the desk, momentarily looked at it, then turned and went away. It was then discovered that the janitor had in fact gone to the desk on two separate occasions but had failed to mention this in the interview. The second incident corresponded to the janitor's story about his actions near the desk. A subsequent interview with the janitor revealed that he had forgotten to mention that he had previously gone behind the desk to pick up a small trash bag from the bin located beneath the desk and had walked away with it tucked under his arm.
>
> Further review of the videotape showed a third incident relevant to the case—2 hours after the janitor walked past the desk an unidentified suspect walked up, went behind the desk, emerged with the telephone handset in his hand, and walked toward a nearby emergency exit. Building management, after being given this new information, made a full apology to the janitor and reinstated him.

Interviewing Techniques

''The most common way to get information and gather evidence, or at least identify it, is through people. Any time someone is spoken to for these purposes, an interview is conducted. Like the investigation itself, it can be casual or formal'' (American Protective Services, 1980, p. 17). The reason for conducting an interview is to obtain information or evidence relevant to the investigation.

The interviewing techniques in the following sections are taken (with minor modifications) from the *Protection Officer Training Manual* (Brennan, 1992, pp. 153–155, with assistance from Sgt. Steve Cloonan, Michigan State Police [Ret.]).

Preliminaries

It is important for the interviewer to go into an interview with a game plan in mind and with all the available facts ready at hand. The success or failure of an interview depends on many factors, some beyond the control of the interviewer. The more factors that can be controlled by the interviewer, the greater the chances are for a successful interview.

The first approach to the subject is very important. Many people will be emotionally upset, angry, hostile, physically injured, and so on. It may be necessary to tend to the subject's needs first before attempting to conduct a meaningful interview. Try to calm the subject, make him or her more comfortable, and enlist his or her active cooperation. Do not be rushed into an interview by the subject. Take your time, obtain all the facts, and get as much background information as possible before taking any action.

At times this approach will upset the subject, who feels that you should be taking swift action on his or her behalf; however, it is important to remember you are in charge and you are responsible for actions you take.

Make sure you have all the information before committing yourself to a course of action. If at all possible, the location of the interview should be chosen by the interviewer and should be free of distractions.

Conducting the Interview

Getting Acquainted

Your greeting should be cordial and sincere. Identify yourself, and if you are not in uniform, produce your identification. Your initial approach can be formal or informal, depending on the circumstances.

Attempt to set the subject at ease by entering into a general conversation with him or her before getting to the matter at hand. People like to talk about themselves and their interests and this is a useful tool in obtaining information about your subject and locating a common ground for communication. At this stage, allow the subject to become accustomed to your presence and to the surroundings by setting the pace.

Developing Rapport

Your immediate objective is to establish common ground on which you can communicate with the subject. By following the preliminaries, you should have a good idea of what the subject's educational background is and at what level it is best to talk with him or her. If you are dealing with a laborer, do not speak down to him or her or use terminology and words that he or she is not accustomed to hearing.

By the same token, you would not speak to an executive as you would a laborer. Find common ground and speak to the subject at his or her level. By finding areas of common interest, such as sports or hobbies, you can establish a rapport with the subject that will lead to easier communication.

In developing a rapport with another person, you must be able to put aside your personal feelings, respect the subject as a person, and show your understanding of the subject and the circumstances that have brought you together. If you are unable to establish a rapport with the subject, an unbridgeable gap will be created that may make further communication difficult, if not impossible.

Motivating the Subject

Most people you interview will be in a strange and stressed situation that makes them uncomfortable. It will be necessary for you to remove any fears they may have. Many people are afraid of ''authority'' as shown by a uniform; they also are afraid of appearing as witnesses, incriminating themselves or others, or may simply be unsure of what they are to do.

If you have developed a rapport with the subject, it will help to convince the subject of the need to tell the truth and to enlist his or her active cooperation.

Keeping the Subject Talking

Once rapport has been established and the subject is motivated, turn the conversation toward the topic you wish to discuss. Allow the subject to give a complete account of his or her involvement without interruptions, but be alert for inconsistencies or omissions.

At times, you may have to interrupt to guide the subject back in the direction you wish the conversation to go. You must control the conversation so that the subject keeps talking until you have all the information you require.

Listening to ''What Is Said'' and ''How It Is Said''

The interviewer must not only induce the subject to freely relate information she or he may possess, but must also evaluate the person and the conversation. In many instances, it is not what the subject says that is important, but the manner in which she or he says it or what a subject does not say.

The interviewer must be constantly alert for signals that indicate she or he is telling the truth, lying, or merely withholding information. Your interviewing abilities can be advanced considerably by learning how to interpret body language.

Repeat the Process

In most instances, the content of an incident will be covered in more than one conversation. The subject will be asked to repeat his or her story again to properly fill in gaps and correct previous statements. Again, it is important not to interrupt the subject during the initial stages and to allow the subject to recount his or her version in full.

After the initial story has been told, the interviewer may then ask the subject to repeat it, this time taking notes and stopping the subject from time to time to get the ''full'' story ''straight.'' Most people will never include all the details in the first attempt because they usually blurt out the information in rapid succession. After the initial telling, they will relax a bit, become more specific, and provide greater detail.

Obstacles to Conversation

Specific Questions

By asking specific questions, the interviewer diverts and limits the interview rather than letting the subject give a narrative of the whole or part of the story. Direct questions also may lead the subject into a false line of thinking as to what you consider to be important areas of the story; as a result, the subject may omit some details in an effort to supply the information he or she thinks you consider important.

Direct questions do have a place in an interview, but they should not be asked until the subject has given a complete narration. Direct questions can then be used to clear up various areas within the narrative. If the subject hits a block and stops talking, a direct question can be used to lead him or her back into the conversation.

Yes/No Questions

For the interviewer to obtain full and detailed facts, the subject must respond with an explanation detailing the events. If a question is asked that only requires a yes or no answer, the subject will normally respond with a yes or no, and information that may have been gained will be lost. By avoiding yes/no questions, you also reduce problems of subjects not understanding your question, agreeing or disagreeing based solely on what they perceive you want to hear, or what they want to tell you.

Leading Questions

Leading questions* have the same effect as yes/no questions. They may cause the subject to give false or misleading information to the interviewer. This may be done either mistakenly or on purpose.

*A leading question is defined by *Black's Law Dictionary* as ''one which instructs witnesses how to answer or puts into his [or her] mouth words to be echoed back'' (1990, p. 889).

Rapid-Fire Questions

Rapid-fire questions may seem appropriate to the inexperienced investigator, but they only lead to confusion, emotional tenseness, and resistance to the rapport that may have been developed. They also stop the cooperative witness from completing his or her statement, thereby possibly losing information.

Encouraging Conversation

Open-Ended Questions

By asking a series of questions in the early stages of an interview, you may be conditioning the subject to believe that if you want to know any information, he or she will be asked—that no spontaneous information is expected. On the other hand, asking relatively few questions leading into a conversation will give the subject the feeling that everything he or she tells has significance.

Typical open-ended questions are general queries: ''Tell me what you saw,'' ''Can you tell me more about that?'' or ''What happened next?'' These types of questions do not permit yes/no answers and allow for no misunderstanding of what the interviewer wants. The subject is forced to give a narrative to answer the question.

The Use of the Long Pause

Sometimes during an interview, the subject will stop talking and a silence will descend on the room. To the inexperienced interviewer, this can be unnerving and cause the interviewer to lose control of the interview and start talking. Pauses in conversation are normal and are never as long in duration as they seem to be. The subject is as ill at ease as you are during these silences, and the experienced interviewer will use them to advantage. Be patient and wait—many times the subject will resume talking and frequently will volunteer additional information just to break the silence.

Non-Directive Approach

The non-directive approach is a technique that turns the subject's statements into questions calling for more information. In using this method, simply repeat the subject's last phrase, but with a rising inflection on the last word so that it becomes a question.

During such an interview, control your emotions, do not register surprise or anxiety, but merely restate the subject's statement. The effect of this technique is that further information is drawn out without giving direction or restricting the thinking as in direct questioning.

Ending the Interview

No interview should be abruptly terminated with a curt dismissal of ''Thank you,'' ''O.K.,'' and so on. When it is apparent the interview is ending, close the conversation in a courteous and friendly manner. You may wish to summarize what has been said and ask the subject if there is anything else he or she wishes to add.

Let subjects know you appreciate what they have done, and that they have performed a valuable service. Thank subjects for their time and assistance. Treating subjects with concern and good manners will help ensure that, if you or another interviewer needs to speak with them in the future, they will be more cooperative and ready to assist instead of resist.

Interrogation

An interrogation is different from an interview in that it is ''an interview which focuses upon a person as a suspect. It is conducted after a substantial amount of information from other sources indicates guilt of an individual. Interrogations are not conversations with the purpose of acquiring information, but with the obtaining of a confession from the subject in mind'' (Hertig, 1992, p. 177).

Managing Investigations

If a high-rise building owner, manager, or tenant hires a private investigator to conduct an investigation, it is essential to clearly establish certain criteria before the investigation commences. They are as follows:

What is the exact purpose of the investigation and what do you expect from the investigator?
What is the scope of the investigation, and how far can the investigator go in conducting it? For example, are there certain individuals who are not to be approached? Are there certain areas that cannot be entered?
What are the time or financial limits on the investigation?
How frequently or under what circumstances should the investigator provide progress reports to the building owner, manager, or tenant?
Should the investigation necessitate calling in outside agencies, such as law enforcement? Will the building owner, manager, or tenant be notified when this is to occur?
How will the final investigative results be handled?

These considerations do not imply that the building owner, manager, or tenant is at liberty to interfere and try to conduct the investigation. If a professional, well-trained, highly skilled, and trustworthy investigator has been selected, that individual will ensure the investigation is properly controlled and managed. However, as Hertig (1992, p. 180) warns, ''If the investigative effort is not properly controlled, man-hours will be wasted, confidentiality may be compromised, and objectives will not be met.'' There also is the possibility that court action may ensue if the investigation is not properly conducted within the confines of the law and according to ethical principles. It is very important that a competent investigator be selected.

Guidelines for Investigator Selection

In selecting an investigator, it is imperative to follow guidelines such as the following:

1. Request the investigator's résumé and review his or her education, qualifications (including appropriate certifications), licensing, and professional experience and affiliations. Most states license investigators through a board, so the investigator's license can be verified. ''A state board can also tell a prospective client how long a firm has been in business, whether it has branch offices, who the company's principals are, whether complaints have been filed against the company, and the nature and disposition of those complaints'' (Kimmons, 1993, p. 60). Any potential conflict of interest the investigator may have should be examined at this point.
2. Ask how long the investigative company or individual has been in business. ''A firm should consider looking for agencies that have been in business for at least two years. It is best to work with a stable agency because a company may need testimony later or require an additional follow-up investigation on the case'' (Kimmons, 1993, p. 60).
3. Determine if the investigator has the necessary skills to carry out the particular investigation required. Request corporate references (business names, addresses, and telephone numbers) of clients for which similar investigations have been conducted. Call these businesses and ask them detailed questions about ''the quality of work performed by the investigator, timeliness, as well as confidentiality, results obtained, and the cost of the investigation. An organization should also ask references whether they received a full and detailed report of the agency's investigative efforts'' (Kimmons, 1993, p. 60).
4. Request a certificate of insurance to verify that the investigator's company has adequate liability insurance coverage. ''Most state boards require agencies to carry $3 million in liability coverage. However, many insurance carriers require that investigative companies carry $1 million in liability coverage with errors and omissions included'' (Kimmons, 1993, p. 60). The certificate of insurance should be requested directly from the insurance carrier.
5. Have the investigator submit a written proposal detailing the purpose of the investigation; how it is to be carried out (depending on the circumstances, a general statement may only be possible); assurance that the investigation will be conducted in an ethical manner within the boundaries of local, state, or federal laws; how long it is expected to take (if known); what form the final written report will take; and how fees for the project will be handled. A total fixed cost may be proposed for the project, or hourly or daily costs may be quoted; in addition, transportation, accommodation, and administrative costs may be separately billed. A retainer fee may be stipulated on acceptance of the proposal or commencement of the investigation, with additional regular payments scheduled during the investigation.
6. When the terms of the agreement are accepted by both parties, a written contract should be drawn up to include the proposal and incidental items such as a confidentiality agreement and acknowledgment that the results of the investigation are the property of the client and the investigator. Once the contract is fully executed, the investigation should commence as outlined in the agreement and all known facts be revealed to the investigator.

Sources of Private Investigators

A private sector investigator may be identified from a number of sources.

Local, county, and state law enforcement; municipal and county fire departments; and the local or state fire marshal's office often will be amenable to providing information and possible lists of investigators, consultants, and specialists.

In the security and fire life safety fields there are a number of professional associations—ASIS International, the National Fire Protection Association (NFPA), the Society of Fire Protection Engineers (SFPE), the International Association of Arson Investigators (IAAI), the International Association for Professional Security Consultants (IAPSC), the National Association of Certified Fraud Examiners, the Society of Certified Fraud Examiners (SCFE), the Society of Professional Investigators, the Association of Federal Investigators, the Council of International Investigators, the International Association of Computer Crime Investigators, the International Association of Credit Card Investigators, and the International Professional Security Association (IPSA)—incorporating the International Institute of Industrial Security. With the exception of the last one, which primarily serves security interests outside the United States, these associations can be contacted through local chapters. The ASIS *Security Industry Buyers Guide* provides a list of investigative services.

Finally, an investigator may be personally recommended by other security and life safety directors, risk managers, property or building managers, and insurance companies.

Summary

Investigations can be an invaluable tool in managing high-rise building security and fire life safety programs. They may be casual or formal in nature. Investigations carried out by tenants, building owners and managers, building security staff, or licensed private investigators differ from those conducted by public law enforcement agencies. The authority of a private investigator is very similar to that of a private citizen, whereas that of a public investigator is based on constitutional and statutory law. Investigators must possess certain qualities or attributes to successfully conduct effective and thorough investigations. For the building owner and manager or tenant, there are basic criteria to consider when selecting a private investigator.

References

American Protective Services, *Investigations and Reports: The Notebook Lesson Series for Security Officers* (American Protective Services, Inc., Oakland, CA, 1980).

ASIS *Security Industry Buyers Guide, 2002 Edition* (American Society for Industrial Security, 1625 Prince Street, Alexandria, VA 22314).

Black's Law Dictionary, 6th ed. (West Publishing, St. Paul, 1990).

Brennan, R. Lorne, ''Interviewing techniques,'' *The Protection Officer Training Manual*, 5th ed., International Foundation for Security Officers (Butterworth–Heinemann, Stoneham, MA, 1992).
Fischer, Robert J., and Gion Green, ''Security and the law,'' *Introduction to Security*, 6th ed. (Butterworth–Heinemann, Woburn, MA, 1998).
Hertig, Christopher A., ''Security investigations,'' *The Protection Officer Training Manual,* 5th ed., International Foundation for Protection Officers (Butterworth–Heinemann, Stoneham, MA, 1992).
Kimmons, Rob L., ''Investigate your investigator,'' (*Security Management*, Arlington, VA, December 1993).
NFPA 921, ''Legal Considerations,'' *Guide for Fire and Explosion Investigations 2001 Edition* (National Fire Protection Association, Quincy, MA, 2001).
Sennewald, Charles A., and John K. Tsukayama, *The Process of Investigation: Concepts and Strategies for Investigators in the Private Sector* (Butterworth–Heineman, Woburn, MA, 2001).
The Merritt Company, ''Incident type investigations,'' *Protection of Assets Manual*, Timothy L. Williams, editor (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, 1991).

Additional Reading

Criminal and Private Security Investigations

O'Hara, Charles E., and Gregory L. O'Hara, *Fundamentals of Criminal Investigation*, 6th ed. (Charles C. Thomas, Springfield, IL, 1994).
Sennewald, Charles A., and John K. Tsukayama, *The Process of Investigation: Concepts and Strategies for the Security Professional*, 2nd ed. (Butterworth–Heinemann, Woburn, MA, 2001).

Fire and Explosion Investigations

Custer, Richard L. P., ''Fire and Arson Investigation,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
DeHaan, John D., *Kirk's Fire Investigation*, 3rd ed., by Paul Leland Kirk, *Brady Fire Science Series* (Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1969, 1983, and 1991).
NFPA 921, *Guide for Fire and Explosion Investigations 2001 Edition* (National Fire Protection Association, Quincy, MA).

This Page Intentionally Left Blank

10 *Building Emergencies*

Modern technology has permitted us to build structures higher and higher. The more people in a high-rise, the greater the potential for ''something to happen'' and for a disaster to occur.

—CITY OF LOS ANGELES, EMERGENCY PREPAREDNESS UNIT

There are any numbers of emergencies that can occur in or affect a high-rise facility. The *New Webster Dictionary* defines an *emergency* as ''any event or combination of circumstances calling for immediate action.'' In the high-rise setting, an emergency poses a threat to both people and property, the people being occupants of the facility, including tenants or visitors, and the property including personal and business assets and the structure itself. The emergency may be caused by people or be a natural disaster. (Usually a disaster is a more widespread event that affects the surrounding community.)

The following sections describe emergency situations that might occur at high-rise buildings and possible ways that they can be handled. The emergencies are fires and fire alarms; workplace violence; hostage and barricade situations; medical emergencies; trip, slip, and falls; power failures; elevator malfunctions and entrapments; traffic accidents; labor disputes, demonstrations, riots, and civil disorder; bombs and bomb threats; hazardous materials, chemical and biological weapons, and nuclear attack; aircraft collisions; natural disasters (earthquakes, tsunamis, volcanoes, winter storms, tornadoes, hurricanes, high winds, cyclones, and floods); water leaks; and jumpers, protestors, and daredevils.

Most, if not all, of the foregoing emergencies have some impact on the security of a building depending on the nature of both the incident and the facility itself. The impact of an emergency on building operations will depend on factors such as the geographical and topographical location of the facility, its design and construction, its security and fire life safety systems and equipment, the location of the emergency within the facility, and the emergency preparedness of building emergency staff and occupants. If the emergency involves the commission of a crime, the crime scene should be preserved as much as possible.

Fires and Fire Alarms

Fire

The threat of fire is ever-present in high-rise office buildings. High-rise fires can be particularly dangerous to building occupants. ''The most critical risks in high-rise structures include fire, explosion and contamination of life-support systems such as air and potable water supply. These threats can be actualized accidentally or intentionally and because they propogate rapidly can quickly develop to catastrophic levels'' (POA, 2000, p. 19-98).

Despite the fact that fires are rare occurrences, if one does occur, everyone in a building must react quickly. In other emergencies, such as a winter storm or civil disturbance, the initial reaction to early warnings of this type of emergency will not necessarily determine its impact on the building. In a fire emergency, however, the first 3 to 4 minutes are critical. The timely handling of a fire emergency according to sound procedures can help stop the event from rapidly becoming a major problem.

Before proceeding, it is helpful to understand the makeup of fire and the behavior of occupants when it occurs.

Basics of Fire Science

Fire is the combustion of fuels (whether solids, liquids, or gases) by which heat and light are produced. Combustion is a chemical reaction between a substance and oxygen that needs three factors—fuel, oxygen, and heat—to occur. Removal of any one of these factors usually will result in the fire being extinguished.

Within a high-rise building there is an abundance of fuel; much equipment and furnishings are made of highly combustible synthetic materials. The centralized heating, ventilating, and air-conditioning (HVAC) systems ensure that there is a plentiful supply of oxygen within interior spaces. An accidental or deliberate application of heat to this scenario may have dire consequences for the life safety of occupants. When combustion occurs, heat can travel by moving from areas of high temperature to areas of lower temperature. This transfer is accomplished by means of conduction, convection, radiation, or direct contact with a flame (Figure 10.1).

Conduction is the movement of heat by direct contact of one piece of matter (whether solid, liquid, or gas, but most often a solid) with another. This heat transfer is crucial to the spread of a fire in a high-rise. For example, when heat is conducted from one end along a steel beam that passes through a fireproof barrier, the other end of the beam can ignite materials.

Convection involves the movement of heat when a liquid or gas is heated, expands, becomes less dense, rises, and is displaced by lower temperature and hence denser liquid or gas. This denser liquid or gas is then heated, and the process continues. The danger of heat transfer by circulating air is heightened in high-rise buildings because when a fire occurs, convection currents can carry hot gases produced by combustion upward through floor-to-floor air-conditioning systems, elevator shafts, open stairshafts, dumbwaiters, mail

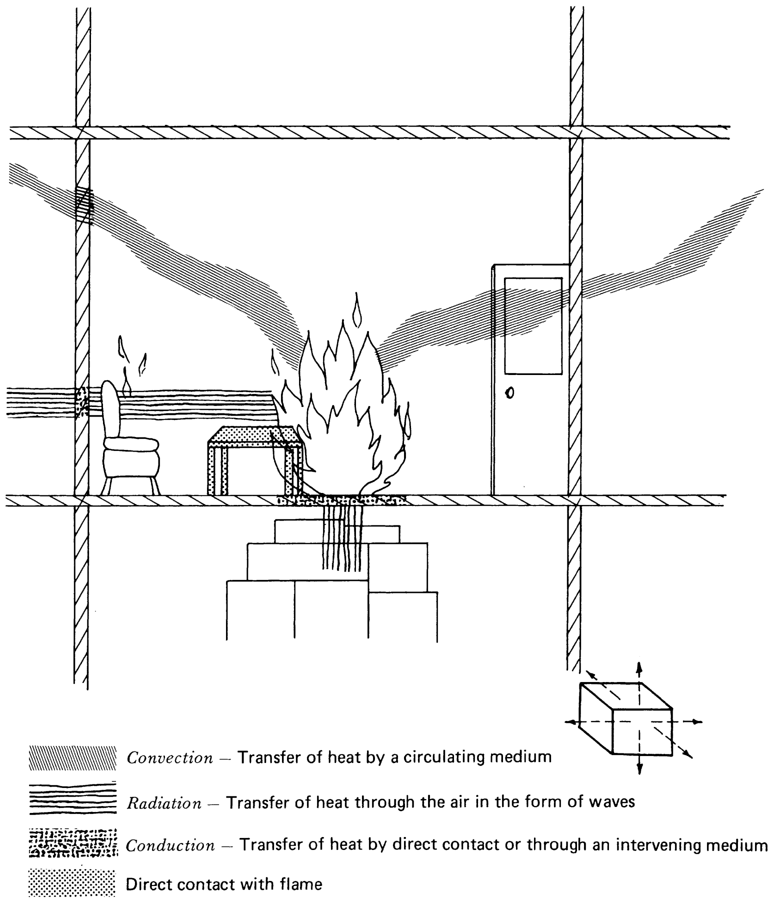


Figure 10.1 Various kinds of heat transfer. Courtesy of *Fire Problems in High-Rise Buildings* (Fire Protection Publications, Oklahoma State University, Stillwater, OK, 1976), p. 12.

chutes, unsealed poke-through construction, and in some high-rises, the exterior skin of a building, thereby spreading the fire to upper floors.* This phenomenon is known as stack effect (Figure 10.2). *Stack effect*, as described by Caldwell (1997, p. 9-18),

> results from the temperature differential between two areas, which creates a pressure differential that results in natural air movements within a building. In high-rise buildings, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke uncontrolled through the building.

---

* *Poke-through construction* occurs when holes are cut through concrete floors to allow the passage of conduit or ducts, primarily used for service utilities. Problems arise when the space between the conduit or duct and the surrounding floor is not then properly sealed with fire-resistant material.

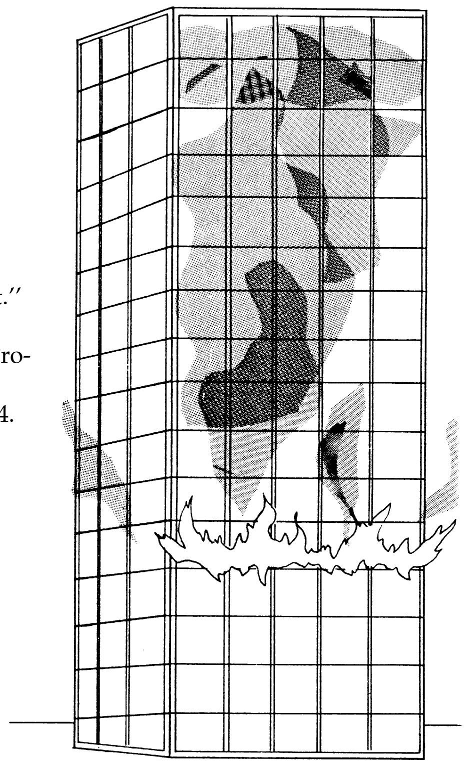


Figure 10.2 Diagram of ''stack effect.'' Reprinted with permission from *Fire Problems in High-Rise Buildings* (Fire Protection Publications, Oklahoma State University, Stillwater, OK, 1976), p. 24.

Radiation is the movement of heat across a space or through a material as waves. *Direct contact* is self-explanatory.

Principal Threat to Life Safety

Smoke is usually the principal threat* to building occupants' life safety and is the ''total airborne effluent from heating or burning a material'' (Clarke, 1997, p. 4-8). It may spread not only vertically between floors but also horizontally through a floor's corridors, open spaces, conduits and ducts, and HVAC systems. Smoke may also spread rapidly through the concealed space that extends throughout the entire floor area of many high-rises, especially if this space is used as a return plenum for the HVAC systems. Hartzell (1997, p. 4-10) states:

> The thermal decomposition or combustion of every combustible material or product produces a smoke atmosphere that is toxic. In sufficiently high concentrations, these smoke atmospheres present hazardous conditions to exposed humans. Predominant among the hazards are impaired vision due to eye irritation, narcosis

*In the September 11, 2001, World Trade Center incident, smoke was a tremendous threat to building occupants, particularly those trapped above the point of impact of each jetliner. Burning jet fuel was also a catastrophic hazard both to those occupants in proximity to the crash sites and to many traveling in elevators when burning fuel cascaded into elevator shafts.

from inhalation of asphyxiants, and irritation of the upper and/or lower respiratory tracts.

These effects, often occurring simultaneously in a fire, contribute to physical incapacitation, loss of motor coordination, faulty judgment, disorientation, restricted vision, and panic. The resulting delay or prevention of escape may lead to subsequent injury or death from further inhalation of toxic gases and/or the suffering of thermal burns. Survivors from a fire may also experience postexposure pulmonary (lung) complications that can lead to delayed death.

Behavior of Occupants

A common belief is that people tend to panic when fire occurs. The *New Webster Dictionary* defines panic as, ''sudden fear arising among people without visible cause; terror inspired by a trifling cause.'' ''Researchers who study human behavior in fires, however, believe that the experience of panic is rare'' (Keating and Loftus, 1981, p. 1). People tend to react in the way that they have been trained to do. If a person does panic, though, others should reassure the individual by exhibiting strong leadership and direction, dispelling rumors, and giving the person something constructive to do.

High-Rise Office Building Fires

Since 1988, several serious high-rise building fires[*] have occurred in the United States.

First Interstate Bank Building

May 4, 1988, Los Angeles, California—The First Interstate Bank Building fire resulted in the tragic death of a building engineer trapped in a service elevator that he used to travel to the initial fire floor to investigate the source of an automatic fire alarm, smoke inhalation suffered by many of the 40 people located inside the office building at the time of the fire, and a loss estimated by the National Fire Protection Association (NFPA) Fire Analysis and Research Division at $50 million (Figure 10.3). The fire started on the 12th floor of this 62-floor high-rise building. The Los Angeles Fire Department was first notified of it at 10:37 PM by a telephone call from outside the building. Using 64 fire companies and 383 fire fighters, it was extinguished 3 hours and 42 minutes later on the 16th floor. The cause of the fire was never positively determined.

[*]Details of the First Interstate Bank Building, the One Meridian Plaza, and the Los Angeles County Health Building fires were largely obtained from ''3 Major High-Rise Fires Reveal Protection Needs'' by Thomas J. Klem (*NFPA Journal*, National Fire Protection Association, Quincy, MA, September/October 1992). Details of the Peachtree 25th Building are from ''Five Die in High-Rise Office Building Fire'' by Michael S. Isner (*NFPA Journal*, National Fire Protection Association, Quincy, MA, July/August 1990).

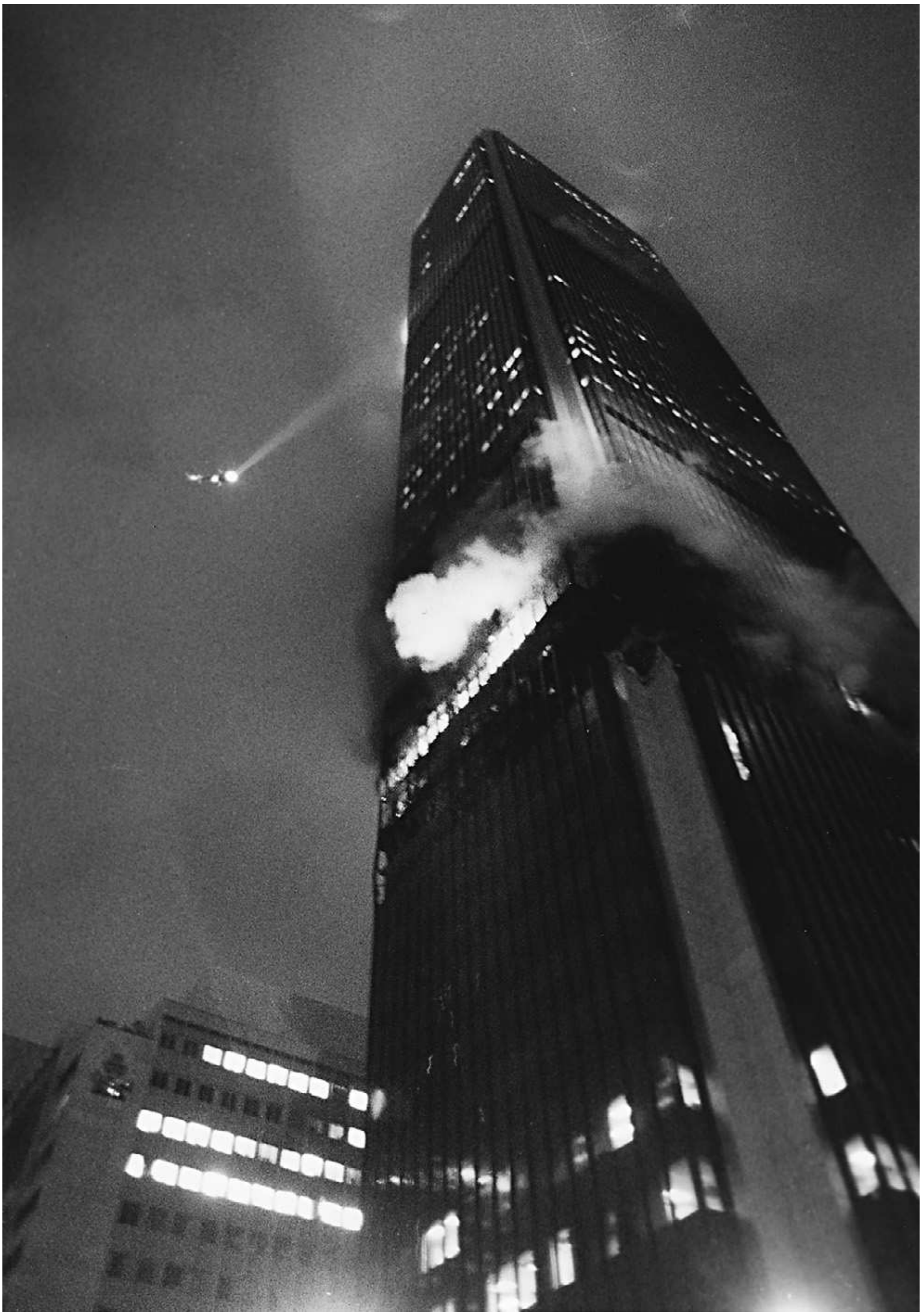


Figure 10.3 TOWERING INFERNO—A fire department helicopter, at left, hovering around First Interstate Bank Building early on Thursday morning, May 4, 1988, as flames shoot from the windows of the 62-story building. Fire officials described the 3½-hour blaze as the worst high-rise fire in the history of Los Angeles. Used with permission from AP/ WIDE WORLD PHOTOS.

According to the NFPA's analysis of the fire, ''the major factors that contributed to the loss of life and fire severity include:

- the lack of automatic fire sprinklers on the floor of fire origin;
- the delay in fire department notification following the internal automatic fire alarm*;
- the absence of compartmentation[,] typical of an open office floor plan, leading to rapid fire growth, development, and spread by means of combustible office furnishings;
- significant floor-to-floor fire extension by internal and external means; and
- significant floor-to-floor smoke spread by way of stairways, elevators, utility shafts and penetrations, and HVAC ducts'' (Klem, 1992, p. 61).

Unsafe Investigation of the Fire Alarm

The death of the building engineer investigating the source of the fire alarm was attributed to the fact that he took an elevator that directly penetrated the fire floor. He bypassed the building's fire life safety system and rode a service elevator to the fire floor to investigate the source of the fire alarm. On arrival at the 12th floor, the engineer began to open the metal elevator car doors but they buckled due to the intense heat of a fire that had intruded into the elevator vestibule. As a result, the doors could not be closed and he died crying out for help on his portable radio. Taking an elevator that can directly access the floor where a fire or fire alarm is occurring is extremely dangerous, particularly if done by non–fire department personnel who lack training and are not equipped with the breathing apparatus and forcible entry tools that fire fighters have when they respond to fire incidents.

Peachtree 25th Building

> *June 30, 1989, Atlanta, Georgia*—The Peachtree 25th Building fire resulted in the death of five occupants, including an electrician who apparently caused the fire, the injury of 20 building occupants and six fire fighters, and direct property damage estimated at over two million dollars. The fire began on the sixth floor of this 10-story office building at 10:30 AM on a Friday. ''Caused by improper repairs to an electrical distribution system, this fire was an extreme, sudden, and intense fire'' (Klem, 1992, p. 62). It was extinguished by the Atlanta City Fire Department only after it had caused heavy damage to the sixth floor and to electrical rooms on the fourth and fifth floors.

According to the NFPA's investigation of the fire, factors contributing to the loss of life and severity of the fire included:

- unsafe actions by an electrician replacing a fuse in the sixth-floor electrical room while the electrical power was on;
- ''The rapid development of a severe fire as a result of arcing in the electrical room'' (Isner, 1990, p. 59);

---

*A private security officer at a nearby building notified the fire department of the fire. On their arrival the delay in reporting the fire was confirmed by the extent of its development. ''The first responding chief fire officer reported that a significant portion of the 12th floor was involved in flames'' (Klem, 1992, p. 61).

- the ignition of wall- and floor-finish materials in the exit-access corridor directly outside the electrical room, the door of which was open;
- ''the absence of automatic sprinkler protection to control fire growth and spread in the exit-access corridor'' (Isner, 1990, p. 59);
- ''the immediate blockage of the egress path due to both the location of the room of fire origin and the rapid spread of fire in the corridor'' (Isner, 1990, p. 59); and
- ''Smoke apparently spread throughout the sixth floor in two ways. First, smoke from the fire in the room of origin quickly began to fill the corridor and advanced ahead of the flame front. The smoke entered the office spaces through doors that were left open, through cracks and openings around closed doors, and through other natural cracks and voids such as small openings between the top of interior partitions and the suspended ceiling assemblies. Second, the ceiling collapsed outside the room of fire origin, and pressurized smoke quickly filled the plenum space that extended over all of the office areas. This smoke then entered the offices through the ceiling vents used to collect return air and seeped through cracks and crevices in the ceiling assembly'' (Isner, 1990, p. 55).

One Meridian Plaza

February 23, 1991, Philadelphia, Pennsylvania—The One Meridian Plaza fire resulted in the tragic death of three fire fighters because of smoke inhalation and destroyed eight floors of this 38-story office building. The fire started on the 22nd floor at 8:23 PM. It was caused by ''spontaneous ignition of improperly stored linseed-soaked rags that were being used to restore and clean'' (Klem, 1992, pp. 58, 60). Eighteen and one-half hours later, the Philadelphia City Fire Department declared it under control on the 30th floor (the first floor above the fire floor that had an automatic sprinkler system).

According to the NFPA, ''the following significant factors affected the outcome of the fire:

- the lack of automatic sprinklers on the floor of fire origin;
- the effectiveness of automatic sprinklers on the 30th floor which, supplied by fire department pumpers, halted the fire's vertical spread;
- the lack of early detection of the incipient fire by automatic means;
- inadequate pressures for fire hoses because settings of pressure-reducing valves were too low for the specific application in this building;
- the improper storage and handling of hazardous materials, producing both the initial ignition and rapid early fire growth; and
- the early loss of the building's main electrical service and emergency power'' (Klem, 1992, p. 60).

Unsafe Investigation of the Fire Alarm

In this fire, when the first automatic fire alarm was received from the 22nd floor, a maintenance worker almost lost his life when he took an elevator to investigate the source of the alarm, leaving a security guard at the first-floor desk. ''When he reached that floor and the elevator doors opened, he encountered heat and dense smoke. The man dropped to the floor, notified the security guard of the fire by portable radio, and told the guard that he could not close the elevator doors. However, he was able to tell the guard how to override the elevator controls so the guard could return the elevator to the first floor. The guard gained control of the elevator, and the maintenance man returned safely to the ground level'' (Klem, 1992, p. 58).

Los Angeles County Health Building

> *February 15, 1992, Los Angeles, California*—At 10:06 AM on a Saturday morning, a fire occurred on the seventh floor of the 14-story, steel-frame, unsprinklered Los Angeles County Health Building. The fire was controlled within 80 minutes by 220 Los Angeles Fire Department fire fighters. Fire damage was restricted to the floor of origin, although there was ''smoke and heat damage on the floors above the floor of origin, and water damage on lower floors'' (Klem, 1992, p. 58). None of the 10 people in the building at the time of the incident were injured. According to the Los Angeles Fire Department, the probable cause was an arc/short of an undetermined electrical source.

According to the NFPA, ''significant factors that affected property loss in this incident included a lack of:

- automatic sprinklers to control the incipient fire and to prevent its spread;
- automatic fire detection equipment in the area of fire origin to provide early warning of an incipient fire;
- compartmentation to contain the fire in an area where suppression personnel could control it more easily;
- automatic shutdown features for the HVAC system'' (Klem, 1992, p. 58).

Mitigating Factor

The First Interstate Bank Building, the One Meridian Plaza, and the Los Angeles County Health Building fires occurred after normal business hours.

> Severe fires in occupied office buildings during business hours are very rare, in large part due to the awareness of people in the building to unusual conditions. Occupants of high-rise office buildings are mobile, awake, and alert, and they are effective early detectors if they are adequately trained to summon help. When such alerting occurs, fires usually are in their initial phase of growth, when they can be controlled more easily. This illustrates the importance of occupant training that includes emergency fire notification procedures. (Klem, 1992, p. 61)

During normal business hours in a fully occupied office building there usually are plenty of people in many areas of the facility. As a result, if a fire occurs, it is more likely that people as well as the building's automatic fire detection system will detect it quickly and cause notification of the fire department. Thus usually a fire will be suppressed before it has an opportunity to develop into a major conflagration. After hours, including weekends and holidays, the number of people present in a building is substantially reduced, so there is more dependence on the building's automatic fire detection and notification systems and security and engineering staff, if present.

Other Major High-Rise Office Building Fires

> *October 10, 1996, New York*—The Rockefeller Center Office Building, New York, NY, electrical fire that started at 4:00 AM on a Thursday morning led to the

> complete evacuation of an 11-story building in the complex. Due to the time, there were very few people in the building when the fire occurred. The lack of a fire sprinkler system on the upper stories of the building was a significant factor contributing to the loss (NFPA Fire Investigation Report by Edward Comeau, Mark C. Ode, and Robert F. Duval).

In addition, the *International Listing of Fatal High-Rise Structure Fires* (Hall, 2001, Appendix A) lists the March 26, 1991, Oakland, California, 18-story office building fire, involving one death, and the November 20, 1996, Hong Kong, 16-story office building fire, involving 40 deaths. (Although both the New York World Trade Center [WTC] February 26, 1993, and September 11, 2001, bombings involved fires, they are treated separately in this chapter under the ''Bombs and Bomb Threats'' and ''Aircraft Collisions'' sections, respectively.)

Word of Caution

Some fires can result from a seemingly innocuous action. An example illustrating this was a fire and explosion that occurred in a residential building, but could easily happen in any type of high-rise occupancy.

> *December 20, 2000, Westwood, California*—At 3:25 PM a fire and explosion on the 23rd floor of a residential high-rise burned five workman. The incident resulted from lacquer being sprayed in an elevator vestibule that had been screened off with clear plastic drapes. According to Los Angeles Fire Department spokesman Brian Humphrey, ''Someone, either entering or leaving the area, had pulled back the curtain, allowing the volatile vapor to come into contact with a halogen work lamp. . . . There was a flash fire, and then an explosion powerful enough to blow out a large window and shake the entire building (Sahagun, 2000, p. B7).

Such an incident highlights the need for strict supervision of all construction and maintenance work that is being conducted in a building.

Fire Alarms

Fire alarms are significant events in high-rise buildings. As Bryan (1982, p. 320) explains, ''The primary purpose of a fire detection system is to respond to a fire, and to transform this response into a visual-audible signal which should alert the building's occupants and the fire department that a fire has been initiated. The fire detection system is intended to respond to the initial signs, signals, or stimuli which indicates that a fire has begun.'' (See the section ''Manual Fire Alarm Stations'' in Chapter 6 for the sequence of events caused by fire alarms in modern high-rise buildings.)

Whenever a fire or a fire alarm occurs, all building occupants need to be alerted to the existence (or possible existence) of fire to initiate emergency procedures. All occupants should be evacuated in a prompt, safe, and orderly fashion according to procedures established in the Building Emergency Procedures Plan (discussed further in Chapter 11). According to NFPA 101, *Life Safety Code*, Section 4.5.3:

> Two means of egress, as a minimum, shall be provided in every building or structure, section, and area where size, occupancy, and arrangement endanger occupants attempting to use a single means of egress that is blocked by fire or smoke. The two means of egress shall be arranged to minimize the possibility that both might be rendered impassable by the same emergency condition.

Occupant Response to a Fire

When a fire occurs, occupants, floor wardens, and emergency staff have duties and responsibilities as outlined in the Building Emergency Procedures Plan. Occupants who discover a fire should know how to protect themselves, how to notify others who may be at risk, how to confine a fire, and how to notify those who will respond to the fire. The notification procedure may include telephoning the fire department and building management or security, and activating a manual fire alarm station on the floor where the fire is.

Occupant Actions

Generally, if occupants discover a fire they should:

1. Notify anyone in the immediate area of danger.
2. Close doors to confine the fire/smoke, but not lock them.
3. Activate or request that someone else activate a manual fire alarm station.
4. Call the fire department by dialing 911, if this service is available. If another number is required,[*] a sticker showing this number should be on all telephones. The following information should be given to the emergency service operator:
   – Building name and address
   – Nearest cross street
   – Location of fire in the building (floor number, suite/room number)
   – Known information about the fire/smoke
   – Caller's call-back telephone number
   The caller should not hang up until the emergency service operator does so.
5. If time allows, call the Building Management Office (or the Office of the Building) or security to notify them of the fire.
6. If time allows, contact floor wardens.
7. Operate a portable fire extinguisher if trained and it is safe to do so, making sure to keep an unobstructed escape route in case the fire enlarges.
8. Listen for announcements over the public address (PA) system.

To evacuate a floor, occupants should proceed immediately to the nearest safe stairwell, and go down at least five[†] floors before reentering the building.

---

[*]Some facilities request that tenants call building security first so that they can notify the fire department and tell them exactly where to respond. This is important, particularly in complex facilities and multi-building complexes, where it is crucial that the fire department arrive at a location that provides optimum access to the incident.

[†]The exact number of floors will be specified in the Building Emergency Procedures Plan and may vary from city to city. For example, the Los Angeles Fire Department specifies a "five-move-five" plan: five floors—including the fire floor, two floors above it (for safety purposes), and two floors below it (so that the second floor below the fire floor can be used as a staging area for the fire department)—are evacuated to five floors below, or out of the building. The NFPA 2002 *High-Rise Evacuation* video also recommends such a staged evacuation of occupants.

If the fire floor is less than six floors from ground level, some departments require occupants to evacuate the building entirely and proceed to a safe refuge area.

Use of Elevators

During a fire or fire alarm, evacuating occupants should never use an elevator whose shaft penetrates the fire/fire alarm floor.

The following reasons for not using such elevators are reported in *Feasibility and Design Considerations of Emergency Evacuation by Elevators* (1992, pp. 1–19), prepared for the General Services Administration (published by the U.S. Department of Commerce):

1. There are ''pressure disturbances caused by elevator car motion on smoke control'' (Klote and Tamura 1987, 1986; Klote 1988). Such piston effect is a concern, because it can pull smoke into a normally pressurized elevator lobby.
2. Elevator doors may jam because of pressure differences caused by building fires. (This phenomenon is known as the stack effect.)
3. Elevator doors may open into a fire.
4. Water from sprinklers and fire hoses can damage electronic, electrical, and mechanical components of an elevator evacuation system. This damage is most serious inside the elevator machinery room and inside the elevator shaft.

The *Fire Protection Handbook* (Donoghue, 1997, p. 8-56) states the following reasons why the use of elevators is unsafe in a fire:

1. Persons may push a corridor button and wait for an elevator that may never respond, losing valuable escape time.
2. Elevators do not prioritize car and corridor calls, and one of the calls may be at the fire floor.
3. Elevators cannot start until the car and hoistway doors close, and panic could lead to elevator overcrowding and door blockage, which would thus prevent closing.
4. Power can fail at any time during a fire, thus leading to entrapment.

The elevator can be delivered to the fire floor when:

1. An elevator passenger presses the car button at the fire floor.
2. One or both of the corridor call buttons is pushed on the fire floor.
3. Heat melts or deforms the corridor push button or its wiring at the fire floor.
4. The elevator functions normally at the fire floor, as in high or low call reversal.*

For many years, this issue has been a major concern of fire protection professionals. According to Charles Jennings, ''The latest and most advanced thought is now devoted to developing pressurization requirements for elevator shafts and lobbies. The objective of these current efforts is to make elevators a useful component of the building evacuation system during a fire'' (1995, p. 291).

---

*''High or low call reversal is basically a staging point for the elevators. In some hotels, for instance, when the elevators are not being extensively used, one of them may be programmed to wait on the concierge or other upper floor. That is an example of a high call reversal function. In other cases, the elevators may go to the lobby level to wait for passengers—that is an example of a low call reversal'' (Solomon, July 8, 2002).

Evacuation Guidelines

Evacuation is complicated by the tendency most people have to leave buildings by the same route they use to enter. Occupants should be taught the following evacuation guidelines:

- Try to stay as calm as possible.
- React immediately. Move quickly but do not run.
- Keep noise to a minimum and listen for instructions, particularly those over the PA system. Follow the directions of floor wardens.
- If there is smoke, crawl low, keeping the head above the floor. In its brochure ''Fire Safety on the Job'' (1993, p. 5), the NFPA recommends keeping the head 12 to 24 inches above the floor. The air near the floor is cleaner because heat and smoke rise. If necessary, place an article of clothing or a handkerchief over the mouth and nose to aid breathing. Do not wet the fabric, as heat may result in steam being breathed into the lungs.
- Do not smoke.
- Feel each door with the back of your hand to ensure the door is not hot because of a fire behind it. If it is hot, do not go through it. If the door is cool, open it slowly.
- Close doors behind you as you leave an area, but do not lock them. (If time permits, turn off electrical appliances, but leave lights on.)
- If trapped in a room, close all doors and seal the bottom of the door with clothing, or the like. If the telephone is working, notify building management or the fire department of your predicament. If you can reach an exterior window, try to signal for outside assistance by placing a sign against the window or waving with something brightly colored. Windows should not be broken unless breathing becomes difficult (breaking them may allow smoke or fire lapping up from floors below to enter). In a modern high-rise, if a window has to be broken out, try to choose one with a decal marked ''tempered'' because its glass will shatter when broken.
- Stop, drop, and roll if your clothing catches fire. Do not attempt to run through a fire.
- If you encounter smoke on entering a stairwell, proceed to an alternate stairwell.
- If smoke is coming up in the stairwells, evacuate upward and enter a safe floor that is located at least three floors above the fire floor, or proceed to the building roof. Move away from the stairwell exit and, if there is a helipad or heliport, proceed to the safe holding area's designated passenger pick up, and make room for a helicopter to land to execute a rescue. (Evacuation upward is most unusual in modern high-rise buildings because the stairwells are designed to keep smoke out—also, evacuating to the roof is not encouraged because only a limited number of people can be accommodated and removed from the building there, possibly by way of helicopter. The operation of helicopters in a fire situation is dangerous due to turbulent air currents exacerbated by the fire itself). If you have evacuated upward, try to notify building management, security, or the fire department of your actions.
- Always close stairwell doors after you enter them. (Occupants sometimes prop doors open, thereby allowing smoke to move into what should be a smoke-free zone.)
- Before entering the stairwell, remove high-heel or awkward shoes to avoid tripping injuries.

- Use the stairwell's continuous handrail and keep to one side in single file so that any responding building emergency staff or fire fighters are not obstructed.
- Do not use the stairwell to congregate with others.
- When you reach the relocation floor and before reentering the building from the stairwell, remember to feel the stairwell door with the back of your hand to ensure the door is not hot because of a fire behind it.
- When you exit the building, move away from it as soon as possible. Be careful of falling glass.
- To descend a fire escape face the rungs or steps, grasp both rails firmly, and look beneath your arms as you move down the escape. At the bottom there will be a ''drop ladder'' or ''swing ladder.'' Another person should be at this location to assist descending occupants.
- Dispel rumors and false information. (Refrain from using the word ''fire'' because it may cause some people to panic.)

Floor Warden Responsibilities

Building floor warden and alternate floor warden responsibilities include determining and coordinating emergency response actions for a particular floor or portion of a floor; ensuring that all occupants, including those with disabilities, are completely out of unsafe areas; making sure evacuees use stairwells and not building elevators; and keeping evacuated or relocated persons at the safe refuge area until building management or the fire department authorizes them to return to their workstations. For more information on floor wardens and the floor response personnel who assist them, see the ''Building Floor Wardens'' section in Chapter 11.

Building Emergency Staff Responsibilities

Responsibilities of building emergency staff—such as building management, the building Fire Safety Director, engineers, and security staff—include ensuring that the fire department has been notified immediately, all occupants have been notified and advised, any necessary evacuation or relocation procedures for affected occupants have begun, building fire life safety systems are operating under emergency conditions, any investigation of the source of the fire alarm or initial suppression of the fire is carried out, and that the fire department and other responding emergency personnel are met when they arrive at the facility.

Occupant Response to a Fire Alarm

When a fire alarm occurs, duties and responsibilities will be similar to those carried out in a fire emergency, but will vary from building to building and city to city, depending on the requirements of the authority having jurisdiction. For instance, some fire departments require occupants on the floor where the fire alarm is activated to proceed to the nearest safe stairwell and descend at least five floors below (see footnote in preceding section). Other fire departments require that when a fire alarm is activated the occupants on the floor in alarm proceed immediately to the nearest safe stairwell and wait there for further instructions from building management (usually over the PA system) or from floor wardens.

In a fire alarm situation, occupants should never use elevators to evacuate because, if there is an actual fire, they may malfunction because of heat and cause entrapment of passengers. This point is addressed in the preceding section.

Fire alarms always should be treated as though an actual fire was occurring. It has been the author's experience that the vast majority of building owners and managers do take fire alarms seriously. Unfortunately, there are others that do not. Some, especially if there is an existing problem with the fire detection system frequently causing false alarms, even request that fire alarms be immediately silenced on alarm floors when they occur. Such a practice is not only illegal but can have dire consequences for the life safety of building occupants. If there is a problem with the fire detection system, it should be treated as an engineering issue and appropriately addressed—it should not be allowed to jeopardize lives.

Workplace Violence

Violence in the workplace has become a very real and present danger in today's society. ''For the fourth year in a row, workplace violence, which affects 2 million American workers every year, is the number one security concern facing Fortune 1000 companies, according to an annual survey of corporate security professionals conducted by Pinkerton Consulting & Investigations* (''Fortune 1000 professionals list top security threats,'' 2002, p. 49).

The National Institute for Occupational Safety and Health (NIOSH web site, 2002) states:

> Violence is a substantial contributor to death and injury on the job. NIOSH data indicate homicide has become the second leading cause of occupational injury death, exceeded only by motor-vehicle-related deaths [Jenkins 1996]. Estimates of nonfatal workplace assaults vary dramatically, but a reasonable estimate from the National Crime Victimization Survey is that approximately one million people are assaulted while at work or on duty each year; this figure represents 15% of the acts of violence experienced by U.S. residents aged 12 or older [Bachman 1994].
>
> The circumstances of workplace violence differ significantly from those of all homicides. For example, 75% of all workplace homicides in 1993 were robbery-related; but in the general population, only 9% of homicides were robbery-related, and only 19% were committed in conjunction with any kind of felony (robbery, rape, arson, etc.) [FBI 1994)] Furthermore, 47% of all murder victims in 1993 were related to or acquainted with their assailants [FBI 1994], whereas the majority of

*''Pinkerton has been conducting its annual survey 'Top Security Threats and Management Issues Facing Corporate America' for nine years. . . . The survey's aim is to identify emerging trends related to perceived security threats, management challenges and operational issues. The 2002 survey drew nearly 200 responses. . . . For more information: *http://www.ci-pinkerton.com*'' (''Fortune 1000 professionals list top security threats,'' 2002, p. 49).

workplace homicides (because they are robbery-related) are believed to occur among persons not known to one another. Only 17% of female victims of workplace homicides were killed by a spouse or former spouse [Windau and Toscano 1994], whereas 29% of the female homicide victims in the general population were killed by a husband, ex-husband, boyfriend, or ex-boyfriend [FBI 1994].

Because statistics such as those compiled by NIOSH include all industries, this does not necessarily mean there is a high incidence of violence in high-rise office buildings. However, serious incidents such as the following have occurred in the high-rise setting.

July 1, 1993, San Francisco, California—A solitary, heavily armed, disgruntled individual entered a 48-story commercial office building in San Francisco's financial district at mid-afternoon, during the time the high-rise was open to the public for normal business. He rode an elevator up to the 34th floor where the offices of Pettit and Martin, a major international law firm, were located. In a 15-minute rampage, he roamed through four floors, shooting to death eight people and injuring six others. He was subsequently found dead in the building stairwell from apparent suicide.

July 29, 1999, Atlanta, Georgia—Mid-afternoon on a Friday, a frustrated day trader, evidently distressed over personal financial losses, entered the offices of brokerage firms each housed in close-by office buildings in Buckhead, Atlanta. Using several handguns, he shot to death nine people and injured 13 others. Later he was found dead from self-inflicted gunshot wounds (''The Atlanta massacre,'' August 9, 1999, p. 22).

Workplace Violence Profiles

The California Division of Occupational Safety and Health, in its *Guidelines for Workplace Security* (Cal/OSHA, 1994, pp. 7, 8), divides workplace violence scenarios (committed by a person called a ''hazardous agent'') into three major types:

1. The agent has no legitimate relationship to the workplace and usually enters it to commit a robbery or other violent act.
2. The agent is either the recipient or the object of a service provided by the workplace or the victim—for instance, the assailant is a current or former client, patient, customer, passenger, criminal suspect, or prisoner.
3. The agent has an employment-related involvement with the workplace—she or he currently works or formerly worked there (employee, supervisor, manager), is or was related in some way to an employee (spouse, [ex-spouse], lover, [ex-lover], relative, friend [former-friend]), or is any other person who has a dispute with someone who works there.

The last type includes domestic violence that can easily intrude into the workplace. In a personal relationship, each of the involved persons usually knows where the other one works. If a relationship has soured, unfortunately the aggressor knows exactly when and where to find the other party.

Bordes (1994, p. 20) summarizes some of the findings on the aforementioned hazardous agents:

> The violent person profile which has been developed through several studies indicates that the middle-aged white male is the most common perpetrator. Other factors which can be considered as major contributors to the development of the perpetrator include, but are not limited to:
>
> - Frustrated employees, who in many instances are simply shuffled between jobs requiring only menial tasks with very little advancement opportunity open to them.
> - Professionals who are experiencing personal frustration and cannot handle emotional deflations such as workforce cutbacks or layoffs.
> - Individuals who are simply bitter, dissatisfied people and are unable to ''shake'' their negativity toward everything.
> - People unable to accept personal blame for their own problems.
> - Individuals with uncontrollable pent-up rage who operate on a ''short fuse'' when it comes to getting upset or mad over anything.
> - Persons who have little or no support systems such as family, friends, neighbors, and who are unable to vent their rage by either confiding in someone or having some other avenue of relief in which they can ''blow off steam.''
> - People who are prone to use firearms and have access to weaponry of any kind.
> - Individuals suffering from depression and [those] who are potentially suicidal.

Alison Carper (1993) narrows the profile of the violent employee to: ''male, white, 35–50 years of age, identifies closely with his job, and has multiple outside pressures, such as marital problems'' (p. 5). The ideal solution would be to screen out, during the initial hiring process, those applicants who have an inclination for violence. However, this profile fits a large percentage of qualified individuals. Basic measures to take are to inquire about applicants' previous criminal convictions and to conduct a thorough background check with previous employers. Despite ethical questions and a degree of uncertainty about their predictive powers, psychological tests also are being used increasingly to screen prospective employees—and still it is often difficult to recognize potentially problematic employees.

The number of lawsuits related to the safety of employees in the workplace is growing as the frequency of these violent events continues to increase. ''The rising incidence of workplace violence is an alarming trend that the total security program must address. . . . With each incident comes the prospect of litigation for inadequate security from both outside and inside the institution'' (Chovanes, 1994, p. 215).

The onus is being placed on corporations, like those that often make up the tenant population in high-rise office buildings, to do something about the problem. Some believe that many of these violent acts against employees are preventable and, as a consequence, constitute possible violations of the ''General Duty'' clause of the Occupational Safety and Health Act of 1970. This clause summarizes the act and states that each employer ''shall furnish to each of his employees a place of employment free from recognized hazards that are causing or likely to cause death or serious physical harm to his employees'' (OSHA, 1974).

Tenant Prevention Measures

Tenant companies may take the following preventive measures, which have been adapted largely from the Cal/OSHA Guidelines for Workplace Security (1994), to address the problem:

- Control physical access through workplace design. This can include controlling access into and out of the workplace and freedom of movement within it, in addition to placing barriers between employees and those visiting. It may be appropriate, in certain situations, to use access cards or other locking devices, a receptionist who can unlatch a door, the installation of duress alarms as a back-up measure (in conjunction with a closed-circuit television [CCTV] camera system to monitor the duress alarm locations), or security personnel.
- Establish a clear anti-violence management policy and set boundaries as to what is considered acceptable behavior. Policies should be applied consistently and fairly to all employees, supervisors, and managers. Provide appropriate supervisory and employee training in workplace violence protection.
- Establish procedures for investigating occupational injury or illness arising from a workplace assault or threat of assault.
- Implement procedures to handle threats of violence by employees, including a policy on when to notify law enforcement agencies.
- Establish procedures to allow employees to confidentially report threats, and to protect them from physical retaliation for these reports.
- Provide training on how to recognize security hazards, how to prevent workplace assaults, and what to do when an assault occurs, including emergency action and post emergency procedures. Give employees instruction in crime awareness, assault and rape prevention, and hostile situation diffusion. For example, if you have employees working at night, encourage them to keep their doors locked and either to leave the building with a fellow employee or to call security for an escort to their vehicle if it is parked on-site.
- If a workplace assault occurs, reduce the short- and long-term physical and emotional effects of the incident by providing post event trauma counseling to those who desire such intervention.

Sound personnel practices, such as pre-employment screening and meaningful job performance evaluations, may help identify and screen out potential problem employees.

A large number of preventive measures can be accomplished without great expense to the employer. For example, if workforce reductions are anticipated, they should be thoroughly planned with dignity and respect afforded to the affected employees. Workers who will be laid off need as much advance notice as possible. Giving severance benefits and offering placement counseling and assistance will help outgoing employees cope with their situation and nurture a supportive work environment for the remaining employees. It has the added benefit of decreasing insurance premiums, because it may avoid triggering an incident of violence in the workplace and the expensive litigation that could result.

Emergency Actions of Security Staff

Despite prevention measures, a workplace violence incident may occur. Building security staff should be prepared ahead of time to deal with such a situation. For example, if an armed and dangerous person is in a high-rise building, either at the main lobby level or on an upper floor, security staff might take the following actions*:

1. Immediately notify local law enforcement, if it is safe to do so (using 911, if this service is available).
2. Notify building management.
3. Communicate with tenants, including floor wardens, over the building PA system, warning them of an emergency situation and directing them to seek a refuge area, lock doors to their offices (if possible), and stay put until further notice. Repeat the announcement periodically.
4. Restrict entry to parking areas, the building, and other areas as required.
5. Determine actions to confine the incident to a specific area. These may include:
   – Recall and shut down of building elevators to restrict the suspect's movement either from or to the main lobby. (Some security practitioners will disagree, stating that elevators should remain operating so as to provide a means of escape for fleeing occupants.)
   – Locking stairwell doors. (Panicked tenants may activate manual fire alarm stations in close proximity to the incident—in a modern high-rise building this activation will cause all stairwell doors to automatically unlock and thereby provide a possible route for the suspect to freely travel up or down between floors.)
6. Direct incoming emergency response agencies to a designated emergency operations center equipped with site maps, building floor plans, and communications equipment.
7. Assist any tenants evacuating the site and direct them to a safe area.
8. If injuries have occurred, provide an area for emergency medical personnel to set up operations.
9. If it is safe to do so, monitor the situation (using video surveillance systems, if possible) and keep law enforcement and emergency services updated.
10. Maintain a written log of events as they occur.
11. As soon as possible, contact families of the affected individuals.
12. Refer the media to a designated spokesperson for the building.

These are only suggestions; each set of circumstances is different, and nothing can be guaranteed to work in all incidents. However, site-specific general procedures approved by building management and local emergency agencies should be developed for each facility's emergency staff, occupants, and floor wardens, then thoroughly documented in the Building Emergency Procedures Manual (described in Chapter 11).

---

* The article ''Managing Violence in Office Buildings'' by Jeanne Arneson, Larry Legind, Jamey Puga, William L. Rinehart, and William V. Wenger that appeared in *Skylines* (September 1994), and Dave Dusenbury, American Protective Services, Inc., were instrumental in formulating these actions.

Hostage and Barricade Situations

In today's violent society, high-rise office buildings have been subject to several hostage-taking and barricade situations.

> *1982, First Interstate Bank Building, Los Angeles, California*—A man entered this 62-story high-rise, accosted the building's chief engineer in the main lobby, and demanded to be taken to the roof. On reaching it, he then tried to obtain publicity for a cause he was promoting—in this case, ''smoking is bad for your health.'' Building management immediately called the police department, and after a tense standoff, the individual eventually surrendered without anyone being injured.

> *March 2002, Rembrandt Tower, Amsterdam, Holland*—On a Monday morning, shortly after most businesses in the tallest building in the Dutch capital opened, a man armed with explosives and two guns took control of the 35-story office building. As many as 18 people were held hostage by the gunman in the building's main lobby and more than 200 people were trapped in their offices. After 7 hours, the gunman shot himself. All hostages were freed unharmed. Reportedly, the gunman was protesting the advertising practices of a major electronics firm that was previously headquartered in the high-rise.*

In most hostage situations, it is imperative to inform law enforcement as quickly as possible; these agencies have specialized training in handling such incidents. Before their arrival, the area where the incident is occurring must be contained to isolate the event from other individuals and, hopefully, to prevent the incident from moving beyond the area. Also, if it is safe to do so, anyone not involved in the incident should be evacuated from the location. Some tenant companies, depending on the nature of their business and their potential for such incidents, have crisis management teams established in case such an incident occurs. These companies will be prepared to make decisions and, in conjunction with law enforcement, take the necessary actions to handle the situation appropriately.

Medical Emergencies

Medical emergencies that can occur in high-rise office buildings range from choking to drug overdoses, from respiratory emergencies to seizures, and from serious injury to suicide. Because building populations are composed of people often working under pressure and stress, there is always the possibility of heart attacks or strokes.

When an occupant or visitor needs urgent medical attention, this must be quickly communicated to emergency medical services or a personal physician (usually located outside the building) and to building emergency staff so that they can prepare the building for medical responders' arrival. This is usually accomplished by dialing 911, if this service is available. If other numbers are

---

*As reported in the *Los Angeles Times* (Associated Press, March 12, 2002, p. A4).

required,* a sticker indicating the numbers to call should be on all telephones in the building. The following information should be given:

Building name and address	Nature of the medical emergency
Nearest cross-street	Victim's condition
Floor and room/suite number	Caller's call-back telephone number
Location and name of the victim	

The caller should not hang up until the emergency services operator does so. It is important to be sure that the operator has all the information to dispatch the right help to the scene without delay.

Someone (preferably not the one tending the victim or making the first call) should then call the Building Management Office or security staff and Floor Warden to notify them of the situation. Another individual should be assigned to wait at the freight/service elevator lobby on the floor where the incident is occurring to direct medical responders to the victim's location. Building management or security will put a freight/service elevator on independent service (or ''manual operation'') to transport the medical responders directly from the building loading dock lobby to the victim's floor. If a physician has been notified, the procedure may vary because such a person usually will not park near the loading dock, and will therefore not require a freight/service elevator to reach the victim. If time permits, a building staff member trained in first aid and/or cardiopulmonary resuscitation (CPR) or automated external defibrillators (AEDs) should be sent to assist the victim. Unless an injured person is in danger of additional, more serious injury, he or she should not be moved or assisted by anyone who is not trained to do so—moving the person could cause further damage or injury.

Tenants should be encouraged to maintain records of the names of employees who are trained in first aid and CPR. Also, telephone numbers of all their employees' next of kin should be kept on file.

Trip, Slip, and Falls

Due to the large numbers of tenants and visitors using high-rise buildings, trip, slip, and falls (whether a trip only; a slip only; a fall only; a trip and fall; a slip and fall; or a slip, trip, and fall) do occur. It is most important that these incidents are properly handled according to established procedures, particularly as these types of events can frequently lead to claims for compensation from the building owner, and sometimes litigation.

Building security staff should assist in handling the situation and thoroughly document their actions and the details of the incident, including taking photographs. (A digital camera is an invaluable tool for obtaining photographs that can later be imported into computerized incident reports.) Some buildings design special reports for such incidents. This helps ensure that basic details of these types of events are obtained.

---

* Some facilities request that tenants call building security first so that they can notify the emergency medical services and tell them exactly where to respond. This is important, particularly in complex facilities and multi-building complexes, where it is crucial that the responders arrive at a location that provides optimum access to the incident.

The following points should be kept in mind when handling trip, slip, and fall incidents:

- Immediately attend to the victim and ask them if they require medical attention. In assisting the person, do not move them if they are injured, unless they are in danger of further injury.
- As soon as possible, ask the victim for details of the accident and what they were actually doing immediately before it (were they in a hurry? was their attention distracted? were they carrying anything or pushing something that may have obstructed their view? etc.)
- Record details such as the date of the incident, time the incident occurred or was reported, name and contact details of the victim/injured person, name and contact details of any witnesses, and exactly where the incident occurred (if outside, describe the weather) and describe any contributing circumstances (foreign substance, debris, an obstacle, poor lighting) and the type of surface on which the incident occurred (carpet, cement, tile, marble, wood, other). If the incident occurred on stairs or a sloping surface, include whether the victim was ascending or descending, a description of the victim's shoes (business or casual, new or worn, type of sole, type of heel, whether tips are present on the sole), whether the victim complained of any pain or injury, the presence of any visible signs of injury, the time that medical assistance was requested, the time of arrival of medical personnel, identity of the medical personnel, whether the victim was transported to a hospital, the name of the hospital, etc.
- If possible, obtain a written and signed statement from the victim and witnesses. Take photographs of the area where the incident reportedly occurred and if possible, of the victim's injury and the soles of their shoes.
- As soon as possible, report the incident to building management and its insurance company.

The actual handling of trip, slip, and falls will vary according to the policy of the building and possibly its insurance carrier.

Power Failures

Failure of electrical power to a high-rise building will have a serious impact on its operations, particularly if the failure occurs during normal operating hours when the building is fully occupied. A power failure may be a brownout (a partial reduction in service) or a total blackout.

Power failure can be caused either by man-made or natural events. Man-made causes may include drivers who collide with utility poles or power transformers, human error in operating equipment within the building or outside it (such as at the utility company supplying the power), or malicious tampering. Natural events include storms, floods, and earthquakes.

> *November 9, 1965, Northeastern United States*—The Northeast power failure of 1965 vividly demonstrated the necessity for the emergency availability of electrical power separate from that supplied by public utilities. Otis Elevator Company reported that the area affected by the blackout contained approximately 20,000 elevators serviced by their company, and that a total of 355 passengers were detained in 161 elevators located in 107

buildings. Most passengers were removed in less than 1 hour. However, in a few cases, passengers were not removed for several hours when the cars were stalled in express hoistways (Otis Elevator Company, 5811, p. 1).

October 17, 1989, Loma Prieta, California—At 5:04 PM, the Oakland–San Francisco Bay Area was shaken by a 7.1-magnitude earthquake. The severe damage caused included fires, collapse of major freeways, and disruption of power and communications to many businesses that consequently, despite the relatively minor damage to buildings, could not reopen for a week.

Power failures also can cause computer memory loss and equipment damage. If the power loss is anticipated, computers and computer systems can be shut down before it occurs. If no prior notice is received, the equipment should still be turned off as quickly as possible to avoid potential serious damage to the electrical system from the sudden surge of power when it is first restored. Computer systems, particularly mainframes, often are equipped with an uninterruptible power supply (UPS); and personal computers often are equipped with surge protectors to reduce the chance of damage when power fluctuates, surges, or is lost.

High-rise buildings have emergency and standby power systems to provide safety and comfort to building occupants during interruptions in their normal power supply. See ''Emergency Power Systems'' and ''Standby Power Systems'' in Chapter 6 for a full description. These systems also provide power to operate building communication systems and to provide a minimum number of elevator functions, as described in the section ''Controls in Elevator Lobbies'' in Chapter 6. Both functions are critical to high-rise buildings during power failures. The following example illustrates this point.

One day during normal business hours, a worker was operating a backhoe in downtown Los Angeles when the machine severed an underground main power line. This resulted in the loss of electrical power to several high-rises, including the 62-story First Interstate Bank Building—at the time the tallest building west of the Mississippi River. The building was without primary power for several hours; this led to the evacuation of approximately 3000 occupants, using the building's stairwells and elevators.

Operating on emergency power, the 26 passenger elevators serving the tower were brought down, one by one, to the mezzanine level to release any passengers. This was completed in less than 30 minutes. After this, the building maintenance and security staffs operated one elevator in each bank, plus one freight/service elevator, to evacuate building occupants from upper floors down to the mezzanine level, starting at the highest floor each elevator bank served. The building's PA system, also operating on emergency power, was used to notify building occupants of building management's decision to evacuate the building and how it would be done.

Despite the fact that power failures are not a regular occurrence in high-rise buildings, occupants should be encouraged to keep a flashlight in their work area, and to make sure it is always in good working order. If a power failure occurs during the day, tenants should be encouraged to open window shades to let in daylight.

Elevator Malfunctions and Entrapments*

Elevators have proven to be a very safe form of transportation in modern high-rise buildings. ''According to the Elevator Escalator Safety Foundation, an estimated 85 billion people ride escalators and elevators every year. The fact that there is such a small number of injuries from elevator and escalator use is no accident'' (Plenzler, 1994, p. 27). Since the late 1970s, elevators have been developed with fully integrated, state-of-the-art microcomputer-based systems that analyze calls, set priorities, and dispatch cars on demand, enabling operators to control every aspect of elevator function. However, not all elevator systems located in high-rise office buildings are this modern and sophisticated. Sometimes, despite rigid continuing-maintenance schedules, they may malfunction or break down.

Elevator Problems

Common problems associated with the operation of elevators in high-rise buildings include elevator cars that do not correctly align with the floor when they arrive there, elevator doors that do not close, and elevator cars that ''slip'' while in motion (possibly caused by stretching of the elevator cables) or stall between floors, thereby entrapping occupants. If any of these conditions occurs, it must be reported promptly to management, engineering, or security staff, who in turn will notify the elevator company responsible for maintaining the equipment. The first three problems may result in temporary shutdown of the elevator for maintenance. Passenger entrapment, however, is a problem that requires immediate attention.

Elevator Entrapment

The passengers can summon assistance by pushing the EMERGENCY CALL, EMERGENCY ALARM, or EMERGENCY ONLY button on the elevator car's floor selection panel or by using the two-way emergency telephone that should be inside a compartment within the elevator car. (See ''Elevator Controls'' in Chapter 6 for a full explanation of these communication devices.)

A certified elevator mechanic may be available on-site; if not, one should be summoned immediately by those who receive the signal or call from the trapped passenger(s). This person will be familiar with the operation of the equipment and the hazards involved in removing passenger(s) from a stalled car. It may be possible to correct the problem that has disabled the elevator, restore normal operation, and release the passenger(s) right away. The passenger(s) may need to assist the process in some way; for instance, if they were instructed to push the EMERGENCY STOP button to the STOP position, they will need to be told to return it to the RUN position for service to be restored to the elevator.

---

*The information on elevator malfunctions was written with technical assistance from *How to Operate Elevators Under Emergency Situations* (Otis Elevator Company, 5811).

Importance of Constant Communication

Constant contact should be maintained with the trapped passengers to assure them that help is on its way. They should be told not to attempt to open the doors or do anything other than what they are instructed to do. If there is no direct communication system to the elevator car, it will be necessary to determine the position of the elevator in the hoistway, proceed to the nearest hoistway door, and speak to the passengers. Constant dialogue will help the passengers deal with the situation and reduce the chance of panic. If there is a delay in getting a trained mechanic to the site or if the problem cannot be corrected quickly, this communication will take on even greater importance.

Life-Threatening Situation

In a life-threatening situation, it may not be possible to wait for trained elevator personnel. ''Under such conditions, passenger evacuation must be performed by carefully selected and trained personnel. Planned and practiced procedures are needed to ensure the safety of rescued passengers and members of the rescue party. Any rescue party should be cautioned never to try to move an elevator from the machine room. Only trained elevator personnel should attempt this'' (Donoghue, 1997, p. 8-57).[*]

Authorized Personnel Only

Only trained elevator and fire department personnel should remove passengers from stalled elevators. Attempts to exit stalled elevators can have tragic consequences, as illustrated by the following incident.

> *October 24, 2000, Century City, California*—At about 4:00 PM on a Tuesday afternoon, a male courier completed a pick-up from an upper floor office of a high-rise building at 1840 Century Park East and boarded an elevator. While traveling down, the elevator became stuck between the eight and ninth floors. The courier notified building security of the problem and was told to wait until assistance arrived. When elevator maintenance personnel arrived, they found the elevator doors pried open but the man was nowhere to be seen. The elevator was repaired and placed back in service. At 10:00 AM the following day a maintenance worker, while routinely checking the elevator pit, found the body of the man.[†]
>
> Indications are that after forcing open the doors, the man, while trying to exit the elevator, fell down the open elevator shaft underneath the car.

[*]''ASME A 17.4, *Guide for Emergency Evacuation of Passengers from Stalled Elevator Cars* [ASME, Fairfield, NJ, 1991], details procedures to follow in performing a safe evacuation'' (Donoghue, 1997, p. 8-57).

[†]As reported in the *Los Angeles Times* (''Man falls to death from stalled elevator,'' October 26, 2000, p. B4).

Traffic Accidents

Motor vehicles such as cars, buses, vans, and trucks commonly enter the parking areas of high-rise buildings. As on public thoroughfares, traffic accidents sometimes occur. Although the incident may have occurred on private property, depending on its seriousness, immediate medical aid or public law enforcement assistance may need to be summoned. Also, building security staff should assist in handling the situation and thoroughly document their actions and details of the incident, including taking photographs. (A digital camera is an invaluable tool for obtaining photographs that can later be imported into computerized incident reports.) Some buildings design special reports for such incidents. This helps ensure that basic details of these types of events are obtained.

Labor Disputes, Demonstrations, Riots, and Civil Disorder

Events such as labor disputes, demonstrations, riots, and civil disorder can have a significant impact on the day-to-day operation of a high-rise building. Their effects will be influenced by the nature of the incident, the number of persons participating in it, the conduct of these participants, the response of building or tenant management and involved outside agencies, and the location of the incident in relation to the building.

Each type of activity needs to be handled on its own merits, but it must be remembered that building and tenant management have the right to conduct daily business activities without disruption by unlawful or unauthorized behavior. They also have the right to secure and protect their own property and assets. In particular, the owner or manager has the right to revoke permission for people to enter a building when it is open to the public (''Right to Pass by Permission. Permission Revocable at Any Time'' signs or plates should already be installed on sidewalks outside the building); irrespective of this, the tenant always has the right to refuse persons entry to their premises.

Labor Disputes

Labor disputes may be peaceful affairs if orderly groups of persons assemble outside the building, quietly display placards and signs to passing motorists, pass out leaflets explaining their cause, and present petitions to the parties involved. They can, however, be violent events if large groups of angry persons protesting a labor issue pertaining to the building, or one of its tenants, surround the building to prevent occupants and visitors from entering or leaving and forcibly try to enter the building, throwing rocks and various other objects at it.

Before a Labor Dispute

If the potential exists for such a situation, building management should take these steps:

- Designate a representative of management, preferably one experienced in handling such incidents, to assume control of the building's response to the situation. If necessary, obtain legal counsel.
- Initiate liaison with local law enforcement agencies at a senior level.
- Explain the situation to representatives of the various departments within the building (engineering, janitorial, security, parking, etc.) and keep them informed of the status of the incident. These persons in turn should brief their staffs as to their responsibilities and provide any required additional training. Instruct all building personnel to avoid contact (particularly any type of confrontation) with those involved in the dispute, and to immediately report problems and direct all inquiries about the dispute (particularly those from the media) to building management. Security personnel, amongst their other duties, will be responsible for documenting events, particularly by investigating incidents that involve unlawful conduct (noting the date, time, location, and possible identities of those involved, including any witnesses) and by photographing or video recording the events for possible later use as evidence. The overt use of a video or still camera can be an invaluable deterrent to illegal behavior—however, conducting surveillance on and recording lawful picketing activities may infringe on the legal rights of employees and the union. Legal advice should be sought regarding this matter.
- Examine the building security program, including insurance policies pertaining to such incidents, in light of the potential threat. If the present deployment of security staff, plus the expected commitment of local law enforcement, is not sufficient to handle a labor dispute, make arrangements for additional personnel from a professional contract security provider. If appropriate, consult major tenants as to the status of their security preparations.
- Establish a command center, including provisions for adequate radio communications with all building personnel involved in handling the incident; still and video cameras for recording events involving mass picketing, blocking of entrances and exits, and other unlawful behavior (the building's CCTV system could also be used for this, if applicable); and a means to maintain a chronological log of events.
- If the labor dispute involves unions, consider providing a separate entrance for workers involved in the dispute. Also, it may be necessary to consult other unions (including tenant unions), whose members work at the building but are not involved in the dispute, to ensure there is no disruption of their activities.
- Depending on the type of labor dispute and its expected impact on building operations, apprise all building tenants of the situation and instruct them to report problems to building management representatives or to the authorities.
- Make sure all oral and written communications regarding the event are cleared with building management and its legal counsel or designated representatives of building workers. Appoint one representative to handle media relations.

During labor disputes, it is essential for all management and staff to remain neutral. Confrontations will only interfere with management's role of providing for the safety of all building users, protecting the assets of the building and its occupants, and minimizing any disruption of building operations.

During a Labor Dispute

If the dispute occurs outside the building, there are basic steps that may need to be taken to handle the situation:

- Call local law enforcement agencies to respond if it is a serious problem and their assistance is definitely required.
- Lock exterior doors to the building. Provide escorts for persons entering or leaving.
- Have building security or law enforcement authorities establish a perimeter around the building or at entrances to it or to any parking structures.
- If the participants outside the building want to enter it for the purposes of handing a petition to a representative within the building, permit this under mutually accepted conditions. These may include an agreement that the delegation consist of no more than five persons, there will be an established time constraint on the visit, and that an escort will be provided at all times.
- Depending on the seriousness of the situation, notify occupants on lower levels to close their window drapes or blinds. If any occupants leave the building, they should avoid any confrontations with those involved in the situation.
- If the dispute occurs inside the building, the way to handle it will depend on the nature of the situation, the number of persons involved, and their behavior. If there is an attempt to unlawfully enter a tenant space, the tenant should call for the assistance of security staff and, if the situation warrants, local law enforcement. Further steps may need to be taken if the situation escalates. Participants in the dispute may be asked to leave if they are disrupting the authorized activities of the building; for example, if there are numerous protesters crowding lobbies, exits, and stairwell entrances, their presence may pose a life safety hazard to other building users. Elevators may be shut down to prevent access from the lobby to upper levels of the building. In addition, tenants may need to be notified of the situation and advised to lock doors to their offices.

Demonstrations

A demonstration is a gathering of people for the purposes of publicly displaying their attitude toward a particular cause, issue, or other matter. Such an activity, if carried out peacefully on public property, is permissible. However, such an activity may not obstruct, block, or in any way interfere with the ingress to and egress from private property such as a high-rise building. Prohibited interference includes any harassment or confrontation of building occupants and/or visitors. If demonstrators attempt to enter the building without permission, they may be arrested for trespassing.

As with a labor dispute, a demonstration may vary from a peaceful affair to a violent one (Figure 10.4). The preparation for and handling of a demonstration is similar to that just outlined for a labor dispute.

Riots and Civil Disorder

Over the past 130 years there have been a number of major civil disturbances in large U.S. cities—New York (draft riots of July 1863), Detroit (riots of July 1967), Newark (riots of July 1967), Miami (riots of 1982), and Los Angeles (Watts riots of 1965, and the 1992 riots).

> *April 29, 1992, Los Angeles, California*—The so-called ''Rodney King'' riots erupted on this date after ''not guilty'' verdicts were handed down in the trial

Figure 10.4 BATTLE AT THE BARRICADES. New York City Police used their clubs in an effort to keep angry demonstrators behind barricades set up outside the Sydenham Hospital on September 20, 1980. The demonstrators were protesting the closing of the facility. Used with permission from AP/ WIDE WORLD PHOTOS.

involving four white Los Angeles Police Department officers charged in the unlawful beating of a black civilian motorist named Rodney King. The 3-day riot and civil disorder was the most destructive disturbance in the United States since the Civil War. For a time, the community watched helplessly as a swathe of destruction swept through: 53 people died, more than 2400 were injured, and 862 buildings were set on fire, with a total fire loss of over $500 million.

December, 1999, Seattle, Washington—''Protesters from around the world came to speak out against the WTO [World Trade Organization], and its perceived wrongdoings. Among causes: animal rights, environmentalism, child labor, and human rights to name a few. Property damage, vandalism and looting took place'' (''WTO riot energizes new wave of domestic terrorism,'' January 2000, p. 7).

The basic steps in handling a riot and civil disorder are similar to those outlined for dealing with a labor dispute or demonstration. However, there are differences according to the nature of the riot, the behavior of the rioters, the area of the community affected by the riot, and the response of law enforcement in containing any civil disorder.

For example, the 1992 Los Angeles civil disturbance involved a large proportion of the community (many of whom were bent on committing criminal acts against people and property) and was widespread throughout Los Angeles County. It was initially met with passive resistance from the law enforcement agency primarily charged with maintaining law and order in the city. In fact, for much of the 3-day event, local law enforcement agencies were overwhelmed by the immense proportion of the disturbance and were unable to contain the full-scale looting and burning that was occurring. Likewise, fire agencies had tremendous demands for their services and were unable, in the early stages, to respond to certain locations without being accompanied by protective police escorts. During this period, many businesses were totally dependent on their own resources, including the utilization of private security staff, both proprietary and contract, to protect themselves and their assets.

Many high-rise office buildings in Los Angeles took the following steps:

- A representative of building management assumed control of the building's response to the disturbance. A command center was established to maintain good communication with all building personnel.
- A chronological log of events was maintained.
- Wherever possible, CCTV cameras were used to monitor external areas of the building.
- Security personnel equipped with portable radios and binoculars were posted on the roof or upper floors to observe activity outside.
- Exterior doors to the building and parking structures were locked. Escorts to parking areas were provided.
- Windows and shop fronts on lower levels were boarded up.
- Building management notified occupants, by telephone and announcements over the PA system, of the civil disturbance in the community. Some of these advisories recommended that tenants immediately leave the building or notify building management of their plans.
- HVAC systems and certain lighting were shut down.
- Fire hoses were attached to standpipes and made ready in the building lobby.
- Elevators were moved to upper floors and were taken out of service. A freight/service elevator remained at the ground floor lobby for the use of engineering and security personnel.
- A skeleton crew of building management, engineering, and security staff remained in the building; many worked 12-hour shifts and stayed even when not on duty.

Also, during this difficult period of civil unrest some high-rise office buildings contracted with civilians trained and certified to carry concealed weapons to supplement their unarmed security staffs. Fortunately, most office buildings were not subjected to the widespread looting that centered on retail businesses containing foodstuffs, liquor, cigarettes, electronic appliances, furniture, and clothing.

Bombs and Bomb Threats

Bombs and bomb threats are very real possibilities in today's world. The Bureau of Alcohol, Tobacco, and Firearms (ATF), Department of Treasury, reports that the number of bombings annually investigated within the United

States has been gradually increasing since the mid-1970s. Its web site contains statistics for explosives incidents by type and bombing incidents by target type.*

Bombings involve either *explosives* or *incendiary devices*. *Webster's College Dictionary* defines the former as ''devices designed to explode or expand with force and noise through rapid chemical change or decomposition;'' the latter are ''devices used or adapted for setting property on fire'' and can be activated by mechanical, electrical, or chemical means. Bombs and bomb threats may be acts of terrorism used by a person or group of persons attempting to control others through coercive intimidation or by those who want to promote their views by claiming direct responsibility or causing other targeted groups to be blamed for an incident. Terrorism also may include taking hostages and other criminal acts.†

1993 New York World Trade Center and 1995 Oklahoma City Bombings

The highly publicized 1993 international terrorist bombing of the New York World Trade Center, the world's second tallest building and a symbol of corporate America and technological achievement, and the 1995 domestic terrorist bombing of the Alfred P. Murrah Federal Building in Oklahoma City, sent shock waves throughout the U.S. high-rise building community.

1993 New York World Trade Center Bombing

February 26, 1993, New York City—At 12:18 PM on a snowy Friday afternoon, a bomb containing approximately 1200 pounds of urea nitrate fertilizer, located in a parked van, detonated and tore a ''five-story subgrade crater that measured 24-36 meters (80-120 feet) across on some levels'' (Hinman and Hammond, 1997, p. 3) in the subterranean parking garage of the 110-story New York WTC located in lower Manhattan (Figure 10.5).

Of the estimated 100,000-plus occupants and visitors of this seven–high-rise building complex, the explosion left six dead and 1042 injured (most suffered from smoke inhalation). According to the NFPA, the explosion caused $230 million in property damage (Hall, 2001, Appendix A). It severely damaged many of the complex's fire protection systems. For example, the fire alarm communication system for the Twin Towers of the Trade Center was incapacitated, and there was an interruption of primary and emergency power systems.

The bomb also resulted in a fire that rapidly disbursed thick, dark clouds of smoke to upper levels of the Twin Towers through horizontal openings—stairwell doors propped open while occupants were waiting to enter

*The data is derived from current National Repository data provided by the ATF, the Federal Bureau of Investigation's Bomb Data Center systems, and the United States Fire Administration's Fire Incident Reporting System.

†Although the September 11, 2001, destruction of the New York Trade Center involved hijacked aircraft which were in effect turned into bombs, the incident is treated later in the section ''Aircraft Collisions.''

Figure 10.5 DEVASTATION AT THE WORLD TRADE CENTER. Patient sifting through the debris of the severely damaged subterranean parking garage of the World Trade Center led investigators to the discovery of a vehicle identification number from the van that contained the explosives used in this horrific bombing on February 26, 1993. Courtesy of the Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms, Washington, D.C.

stairwells—and vertical openings—stairwells and elevator shafts. During this emergency, thousands of building occupants walked down darkened and smoke-filled stairwells to evacuate the building without the assistance of emergency lighting or advisory emergency instructions delivered over the PA system. (Generators supplying emergency power to these systems started up, but after 12 minutes they overheated and shut down because of damage from the explosion.) ''Many persons were needlessly exposed to smoke inhalation and stress in premature evacuation from a structure in which upper floors were safer and more hospitable than the escape routes'' (POA, 1995, p. 26-2).

According to the ATF, a vehicle identification number from the van, which had been rented but reported stolen the day before the explosion, was uncovered after the explosion. The ensuing investigation ultimately led to the identification and indictment of seven suspects, four of whom were convicted on conspiracy, assault, and various explosives charges. The evidence linked the defendants to the purchase of chemicals and hydrogen tanks used to manufacture the bomb, to the rental of the shed to warehouse the chemicals and later the bomb, and to the rental of the van that contained the bomb. Each of the four Muslim extremists found directly responsible for this incident was sentenced to life in prison.

Considerable information relating to this bombing was obtained from ATF and NFPA. After the incident, two ATF National Response Teams assisted the New York City Police Department and the FBI in their investigation. A thorough Fire Investigation Report on the WTC Explosion and Fire can be obtained from the NFPA (Isner and Klem, 1993).

According to an evacuation study conducted by NFPA and the National Research Council of Canada (NRCC), with funding provided by the National Institute of Standards and Technology (NIST), the evacuation of occupants from the Twin Towers ranged from minutes to hours and less than ten percent of the evacuees had previously participated in evacuation drills (Prouix and Fahy 2002).

1995 Oklahoma City Bombing

April 19, 1995, Oklahoma City—At 9:02 AM, when parents were dropping off their youngsters at the Alfred P. Murrah Federal Office Building's day-care center, a homemade bomb containing an ''estimated 4,800 pounds of ammonium nitrate [fertilizer] and fuel oil'' (Hinman and Hammond, 1997, p. 1), placed in a large rented truck parked in a no-parking, no-standing zone circular driveway outside the building, detonated and blew away the facade and nearly half of this nine-story reinforced concrete frame building located in downtown Oklahoma City (Figure 10.6).

The blast left a 30-foot-wide, 8-foot-deep crater and shot a fireball and thick black smoke and debris high into the atmosphere. Shards of glass were propelled in every direction across several city blocks, office windows were shattered, numerous nearby buildings suffered structural damage, and vehicles were damaged throughout the downtown business section.

Of the estimated 500-plus occupants and visitors of this structure, the explosion left 168 dead, including 19 children in the demolished day-care center. In addition, there were four fatalities at an adjacent building, one outside and one in a parked vehicle, while a nurse running to the scene was killed by a falling piece of concrete. Seven hundred eighty-two people were injured. According to the NFPA (Hall, 2001, Appendix A), the explosion caused almost $136 million in property damage. The building was demolished as a result of the incident.

Immediately following the explosion, the General Services Administration (GSA) placed over 1300 federal buildings throughout the United States on a security alert with building exterior patrols, inspection of packages, briefcases, and vehicles, and heightened surveillance for persons and objects, including vehicles, that were suspicious or looked out of place. Parking was restricted around some buildings and concrete barriers were erected in front of some structures to protect against this type of threat.

Timothy McVeigh was executed for this incident that was, up until September 11, 2001, the worst terrorist attack in U.S. history.

Figure 10.6 TERROR IN OKLAHOMA CITY. The Alfred P. Murrah Federal Building in downtown Oklahoma City sits in ruins after the April 19, 1995, devastating explosion that rocked the nation. Rescue workers using extension ladders work desperately to free survivors. Used with permission from AP/WIDE WORLD PHOTOS.

Vulnerability Assessment of Federal Facilities

Before the Oklahoma City bombing, there were no government-wide standards for security at federal facilities in the United States. After it, a security survey, entitled *Vulnerability Assessment of Federal Facilities* (June 28, 1995), was conducted by the U.S. Department of Justice, including the Federal Bureau of Investigation (FBI), and the U.S. Secret Service, the GSA, the State Department, the Social Security Administration, and the Department of Defense; the survey developed 52 recommended minimum security standards in light of the changed environment of heightened risk.

These standards apply to what GSA describes as a ''typical single- or multi-tenant federal office building'' and cover the subjects of perimeter, entry, and interior security and security planning. According to the Los Angeles Times, these standards, some of which are already in place, embody ''new parking restrictions within buildings and in adjacent areas, use of X-rays and metal detectors at entrances for visitors and packages, erection of physical barriers, deployment of roving patrols outside the buildings, closed-circuit television monitoring, installation of shatterproof glass on lower floors, better alarm systems, locating new buildings farther from streets, grouping agencies with similar security needs, and tougher standards for visitor and employee identification'' (Jackson, 1995, p. A23).

Bombs*

Bombs can be constructed to look like almost anything and can be placed or delivered in any number of ways. The probability of finding a stereotypical-looking bomb is almost nonexistent. The only common denominator among bombs is that they are designed to explode. Most bombs are homemade. Only the imagination of and the resources available to the bomber limit their design.† When searching for a bomb, suspect anything that looks unusual. Let the trained technician determine what is or is not a bomb.

Mail Bombs

Bombs can be received through the mail. The highly publicized ''Unabomber'' incidents involved the mail. This serial bomber was so-named by the FBI because the targets of these letter and package bombs sent in the United States since 1978 had previously been academics and executives at universities and airlines. After 16 bomb attacks, with three dead and 23 injured, the Unabomber, Ted Kaczynski, was finally arrested and convicted for these crimes.

Warning Signs

To enhance letter and package bomb recognition, remember there are possible warning signs. One must be discerning, because several of these characteristics

*Most of the information in the following sections pertaining to bombs, bomb threats, and security planning is taken with some adaptations and additions from the ATF publication, ''Bomb Threats and Physical Security Planning'' (ATF P 7550.2, 1987).

†Conventional explosives can also be encased in radioactive waste material. If detonated, these so-called radiological or ''dirty bombs'' are discussed in a later section, ''Nuclear Attack.''

(wrong addressee title, misspelling, etc.) apply to many letters from, for example, those applying for employment. The following general checklist was supplied by the ATF.

- Addressee unfamiliar with name and address of sender
- Package/letter has no return address
- Addressee is not expecting package/letter, or expects different size package
- Improper or incorrect title, address, or spelling of name of addressee
- Addressee title but no name given
- Wrong title with name
- Handwritten or poorly typed address
- Misspelling of common words
- Return address and postmark are not from same area
- Excessive postage or unusual stamps used versus metered postage
- Special handling instructions on package (SPECIAL DELIVERY, TO BE OPENED BY ADDRESSEE ONLY, FOREIGN MAIL, and AIR MAIL, etc.)
- Restrictive markings (PERSONAL, CONFIDENTIAL, etc.)
- Excessive securing material such as wrapping, tape, or string
- Oddly shaped or unevenly weighted packages
- Bulky, lumpy, or rigid envelopes
- Lopsided or uneven envelopes
- Oily stains or discoloration
- Strange odors
- Protruding wires or metal
- Visual distractions (drawings, statements, etc.)
- Mail arrives before or after a telephone call from an unknown person who asks whether the recipient has opened it or who requests that he or she opens it

This is only a general checklist. When an item is in question, the best protection is to make personal contact with the sender of the package or letter but not to open it.

Suicide Bombers

Walk-in suicide bombers with explosives attached to their body or contained in a suitcase, as demonstrated by such carnage in Israel, are virtually impossible to detect and could strike anywhere at any time. ''A major reason for the concern, as the Israeli government has learned, is that no amount of preparedness can stop such bombers—not swarms of police patrols, stepped-up border enforcement or increased intelligence-gathering missions. In most cases, one person armed with less than a handful of plastic explosives can walk into a public gathering, flick a detonation switch and kill dozens of people'' (Meyer, 2002, p. A18).

Bomb Threats

Bomb threats are delivered in a variety of ways. The majority are called in to the target. Occasionally these calls are through a third party. Sometimes a threat is communicated in writing, via e-mail, or by a recording. There is more than one reason for making or reporting a bomb threat. For instance, a caller who has definite knowledge or believes an explosive or incendiary bomb has been or will be placed may want to minimize personal injury or property damage. This caller could be the person who placed the device or someone who has become aware of such information. On the other hand, a caller may simply want to create an atmosphere of anxiety and panic, which will, in turn, result in a disruption of the normal activities at the facility where the device is purportedly placed. Whatever the reason for the report, there will certainly be a reaction to it. Through proper planning, the wide variety of potentially uncontrollable reactions can be greatly reduced.

Why Prepare?

Proper preparation can foil the bomber or threat maker by reducing the accessibility of a business or building and identifying areas that can be ''hardened'' against potential bombers. This will limit the amount of time lost to any searching determined necessary. If a bomb incident occurs, proper planning will demonstrate that those in charge do care and reduce the potential for personal injury and property loss.

Proper planning also can reduce the threat of panic, the most contagious of all human emotions. Panic is sudden, excessive, unreasoning terror that greatly increases the potential for injury and property damage. In the context of a bomb threat, panic is the ultimate goal of the caller.

How to Prepare

To cope with a bomb incident, it is necessary to develop two separate but interdependent plans. The bomb incident plan provides the detailed procedures to be implemented when a bombing attack is threatened or executed. A physical security plan, which is covered in detail in the next section, provides protection of property, personnel, facilities, and material against unauthorized entry, trespass, damage, sabotage, or other illegal or criminal acts. In most instances, some form of physical security is already in existence, although it may not necessarily be intended to prevent a bomb attack.

To carry out these plans, a definite chain of command must be established to instill confidence and avoid panic. This is easy if there is a simple office structure, or one business, in the building. However, in a multiple-tenant commercial office building a representative from each tenant should attend a planning conference. A leader—the Building or Property Manager, Fire Safety Director, or Director of Security—should be appointed and a clear line of succession delineated. This chain of command should be printed and circulated to all concerned parties. There should also be a command center to act as a focal point for telephone or radio communications. The management personnel assigned to operate the center should have the authority to decide what action is to be taken during the threat. Only those with assigned duties should be permitted in the center, and alternates need to be appointed in case someone is absent when a threat is received. In addition, an updated blueprint or floor plan of the building should be obtained and kept in the command center.

Contact the police department, fire department, or local government agencies to determine if any assistance is available for developing a physical security plan or bomb incident plan. If possible, have police or fire department representatives and building and tenant staff inspect the building for areas where explosives are likely to be concealed; make a checklist of these areas for inclusion in command center materials. Determine whether there is a bomb disposal unit available, how to contact the unit, and under what conditions it will respond. You must also ascertain whether the bomb disposal unit, in addition to disarming and removing the explosives, will assist in searching the building if a threat occurs.

Training is essential to deal properly with a bomb threat incident. Instruct all personnel, especially those at any telephone switchboards, in what to do if a bomb threat is received. Be absolutely certain that all personnel assigned to the command center are aware of their duties. The positive aspects of planning will be lost if leadership is not apparent.

If possible, the command center should be located near the focal point for telephone or radio communications. In any case, the search or evacuation teams must be able to keep the center informed of their progress at all times. In a large facility, if the teams go beyond the communications network, the command center must have the mobility to maintain contact and track search or evacuation efforts.

Security Against Bomb Threat Incidents

As mentioned previously, although most high-rise commercial structures already have security systems and measures in place (see Chapters 5 and 7 for details), the implementation of a specific physical security plan will prepare a facility against a potential bomb attack. Although there is no single security plan that is adaptable to all situations, the following recommendations are offered because they may help diminish vulnerability to bomb attacks.

The exterior configuration of a building or facility is very important. Unfortunately, in some instances, the architect has given little or no consideration to security, not to mention thwarting or discouraging a bomb attack. However, by adding physical barriers and lighting, by preventing vehicles from parking immediately adjacent to the building, and by controlling access, the vulnerability of a facility to a bomb attack can be reduced significantly.

Security Measures Against Vehicle Bombs

Bombs delivered by a vehicle or left in a vehicle are a grave reality. The destructive power of a vehicle bomb will depend on factors such as the location of the vehicle in relation to a building, the type and amount of explosives that it contains, and the structural strength of the facility to withstand the explosion.

Since the September 11, 2001, terrorist attacks, some major high-rise office buildings have instituted checking of passenger vehicles for suspected bombs as they enter (consisting either of security or parking personnel checking inside vehicles and trunks, or using a small mirror or CCTV camera attached to a 3–4-foot long metal pole to inspect under vehicles). Also, some high-security buildings restrict public parking and require vehicles,* particularly vans and trucks, to undergo on-street inspections, before they are permitted to enter under-building loading dock/shipping and receiving areas. Such inspections have even included performing x-rays† of entire vehicles and the use of bomb-sniffing dogs.

1993 New York World Trade Center Bombing

The 1993 WTC bombing was an example of the damage that explosives transported into an under-building parking garage can cause when detonated. According to Doug Karpiloff, the late Security and Life Safety Director for the WTC, ''Prior to the bombing, the WTC was an open building during the day, but closed at night. After the bombing, the Center was relegated to a closed facility, in which public parking was completely eliminated'' (''Security soars to new heights,'' September 1997, p. 21). As reported by *SECURITY* (''Never again!'' July 2000, pp. 19–20), security upgrades against the risk of vehicle bombs included the following measures:

- Forming a ring of 250 ten thousand-pound steel-reinforced planters surrounding the WTC complex, with a custom movable gate that permitted emergency vehicle access to the plaza. Then, according to Karpiloff, ''If the gate is opened, the CCTV cameras lock onto the gate and can't be moved until the gate is closed.'' Once the gate was closed, the cameras unlocked and resumed regular surveillance. [According to *Access Control & Security Systems* (''Towering team leader,'' September 2000, p. 42), bomb resistant trash containers were also provided as part of the perimeter protection system.]
- Providing total closed-circuit television (CCTV) coverage of the plaza and perimeter of the WTC.
- Restricting parking beneath the WTC to authorized tenants with special vehicle identification. [According to *Access Control & Security Systems* (''Towering team leader,'' September 2000, p. 42), the parking access control system utilized auto vehicle identification (AVI) tags on car windshields and driver's proximity cards to make sure that both the vehicle and the driver were authorized to enter the garage.]
- Equipping the underground parking garage with bullet-resistant guard booths, anti-ram barriers and bomb-sniffing dogs.
- Stopping trucks one block from the buildings for inspection (after being cleared to proceed to the truck dock, the drivers were photographed along with their driver's license, bill of lading and registration information for storage in the WTC main server).
- Installing a stopped vehicle detection system to sense cars stopping around the perimeter and within the WTC plaza. (When a stopped vehicle was sensed, the

*A sometimes overlooked but very simple security measure to restrict the size of vehicles entering parking areas is to install a vehicle header bar at the point of vehicle entry. The height at which the bar is positioned will depend on what type of vehicle is being allowed entry. Commonly, the height restriction is 6½ feet, or approximately 2 meters. Most buildings have such bars installed to warn drivers of oversize vehicles before damage is caused to the overhead structure and the vehicle.
†*MobileSearch*™ is a non-invasive inspection system that involves the use of an x-ray source mounted in a truck. It can be used to x-ray vehicles, including large trucks. Such a device can be very effective in screening for explosives and weapons before a vehicle is permitted entry to an under-building parking garage.

CCTV cameras locked onto that area, the WTC police were alerted and a video print of the vehicle could be taken. The cameras did not unlock until the vehicle was moved. This information was stored on the WTC server at the Security Command center.)

After the 1993 bombing, many high-rise office buildings in the United States installed CCTV systems at the entrance and exit points of under-building or subterranean parking garages. These cameras facilitated recording close-up images of the driver and license plate of every vehicle entering and the license plate of all vehicles exiting these areas. If there were an incident, this would help to identify vehicles that may have been involved.

1995 Oklahoma City Bombing

The 1995 Oklahoma City bombing was an example of the damage that explosives outside of a high-rise building can cause when detonated. One obvious security measure to reduce the impact of such an explosion would be to maintain a spatial separation of at least several hundred feet from the building of all vehicles prior to them being cleared for entry. However, this would be impractical in all but a few established buildings. Where practical and warranted according to the assessed risk to a particular building, a variety of security barriers such as perimeter landscaping, walls, fences, sidewalks, fountains, sculpture, boulders, planters, park benches, concrete barricades, and bollards might be deployed to restrict the proximity to buildings that vehicles can attain. Also, the establishment of restricted parking zones and the strict supervision of these no-stopping areas will reduce the risk of these types of incidents. In addition, the application of security window film on glass windows on lower floors and the structural hardening of a building by, for example, reinforcing exposed building columns in areas such as loading docks, will help reduce the effects of an explosion.

Other Security Measures to Reduce the Threat of Bombs

Controls should be established to positively identify personnel who have authorized access to critical areas and to deny access to unauthorized personnel. These controls should include inspection of all packages and materials being taken into critical areas, as well as the following:

- Security and maintenance personnel should be alert for people who act in a suspicious manner, as well as objects, items, or parcels that look out of place or suspicious. Surveillance should be established to include potential hiding places (e.g., stairwells, restrooms, and any vacant office space) for unwanted individuals. Designated patrols of such areas will assist in this endeavor.
- Doors or access ways to certain areas—mechanical rooms, mailrooms, computer rooms, data centers, switchboards, and elevator control rooms—should remain locked when not in use. It is important to establish a procedure to keep track of keys. If keys cannot be accounted for, locks should be changed.
- Good housekeeping also is vital. Trash or dumpster areas should remain free of debris. A bomb or device can easily be concealed in the trash. Combustible

materials should be properly disposed of, or protected if further use is anticipated.

- Mail boxes at buildings can constitute a security hazard. A bomb or device could be placed inside one and later detonated. Consideration should be given to using bomb-resistant mail boxes or to completely removing them.
- Detection devices may be installed at entrances to high-risk tenant areas, and CCTV should be used in areas identified as likely places where a bomb may be placed. This, coupled with posting signs indicating that such measures are in place, is a good deterrent.
- Perhaps entrances and exits can be modified with a minimal expenditure to channel all visitors through someone at a reception desk. Individuals entering a building after normal business hours would be required to sign a register indicating the name and suite or floor number of the person they wish to visit. Employees at these reception desks could contact the person to be visited and advise him or her that a visitor, by name, is in the lobby. The person to be visited may decide to come to the lobby to ascertain the purpose of the visit. A system for signing out when the individual departs could be integrated into this procedure, although this may result in complaints from the public. If the reception desk clerk explains to the visitor that these procedures were implemented for the visitor's own best interest and safety, complaints may be reduced. A sign also could be placed at the reception desk informing visitors of the need for safety.

Responding to Bomb Threats

Instruct all personnel, especially those at telephone switchboards, on what to do if a bomb threat call is received. It is always best if more than one person listens in on the call. To do this, a covert signaling system should be implemented, perhaps by using a predetermined signal to a second reception point.

A calm response to the bomb threat caller could result in obtaining additional information. This is especially true if the caller wishes to avoid injuries or deaths. If told that the building is occupied or cannot be evacuated in time, the bomber may be willing to give more specific information on the bomb's location, components, or method of initiation.

Vital Actions

The person making the threat is the best source of information about the bomb. When a bomb threat is called in, the person taking the call should do the following:

- Keep the caller on the line as long as possible. Ask him or her to repeat the message. Record every word spoken by the person. (Some building managers and individual tenants may provide audio recorders for this purpose; others by policy do not.)
- If the caller does not indicate the bomb's location or the time of possible detonation, ask for this information.
- Inform the caller that the building is occupied and that detonation of a bomb could result in death or serious injury to many innocent people.
- Pay particular attention to background noises such as motors running, music playing, and any other noise that may give a clue as to the location of the caller.

- Listen closely to the voice (male or female), voice quality (calm or excited), accent, and any speech impediment. Immediately after the caller hangs up, report the threat to the person(s) designated by management to receive such information.
- Report the information immediately to the police department, fire department, ATF, FBI, and other appropriate agencies. The sequence of notification should be established in the bomb incident plan.
- Remain available: Law enforcement personnel will want to interview you.

When a written threat is received, save all materials, including any envelope or container. Once the message is recognized as a bomb threat, further unnecessary handling should be avoided. Every possible effort must be made to retain evidence such as fingerprints, handwriting or typewriting, paper, and postal marks. These will prove essential in tracing the threat and identifying the writer. Although written messages usually are associated with generalized threats and extortion attempts, a written warning about a specific device may occasionally be received. It should never be ignored. A Bomb Threat Checklist developed by the ATF can be found in Appendix 11-1.

Decision Time

The most serious of all decisions to be made by management in the event of a bomb threat is whether to evacuate the entire building or only certain areas. In many cases, this decision may already have been made during the development of the bomb incident plan. Management may pronounce a carte blanche policy that, in the event of a bomb threat, all affected areas will be evacuated immediately. This decision circumvents the calculated risk; however, such a decision can result in costly loss of time and may not be the best approach.

A decision to evacuate an entire high-rise building would be a most unusual step to take. If an evacuation or relocation of occupants is chosen, it usually will involve only the floor where the threat was received and possibly, as a safety precaution, two floors above and two floors below the affected floor. Such partial evacuation is commonly referred to as staged evacuation. To totally evacuate a building takes considerable time and effort and is often an unnecessary step in handling this type of incident.

The responsibility for deciding whether to evacuate a tenant space usually resides with the tenant's senior officer. Sometimes, however, depending on the circumstances surrounding the threat and considerations for the general safety of all building occupants, the building owner or manager will make the decision.

To assess the credibility of a bomb threat, it is important to analyze the answers to the following questions:

1. What is the time of the threat?
2. How is the threat received (by telephone, by mail)?
3. How specific is the threat (type of bomb, place, time of explosion, etc)?
4. What is the history of the company involved with regard to threats? (Is it presently involved in a labor dispute with its employees? Does it produce a controversial product?)

5. What is the identity of the person making the threat (if the threat is over the telephone, is the person a child, young or old, drunk, claiming to be a terrorist, etc.)?
6. What is the possibility of someone obtaining access to plant the device?

Essentially, there are three alternatives when faced with a bomb threat: ignore the threat, evacuate immediately, or search and evacuate if warranted.

Ignore the Threat

Ignoring the threat completely can result in some serious problems. Although a statistical argument can be made that very few bomb threats are real, it cannot be overlooked that some bombs have been located in connection with threats. If employees learn that bomb threats have been received and ignored, it could result in morale problems and have a long-term adverse effect on business. Also, there is the possibility that if the bomb threat caller feels ignored, he or she may go beyond the threat and actually plant a bomb.

Evacuate Immediately

Evacuating immediately in response to every bomb threat is an alternative that on face value appears to be the preferred approach. However, the negative factors inherent in this approach must be considered. The obvious result of immediate evacuation is a disruptive effect on business and building operations. If the bomb threat caller knows that the building's policy is to evacuate each time a call is made, he or she can call continually and force tenants' business to come to a standstill. An employee who knows that the policy is to evacuate immediately may make a threat to get out of work. A student may use a bomb threat to avoid a class or miss a test. Also, a bomber wishing to cause personal injuries could place a bomb near an exit he or she knows is normally used to evacuate and then call in the threat.

Search and Evacuate if Warranted

Initiating a search after a threat is received and evacuating a portion of a building after a suspicious package or device is found is the third, and perhaps most desirable, approach. It is certainly not as disruptive as an immediate evacuation and will satisfy the requirement to do something when a threat is received. If a device is found, occupants can be evacuated expeditiously, avoiding the potential danger areas near the bomb.

Evacuation

An evacuation team consisting of building management, the building Fire Safety Director, security, floor wardens, and floor response personnel should be organized and trained. This should be coordinated with all building tenants and designed in conjunction with developing the bomb incident plan. The team will be trained in how to evacuate the building during a bomb threat. You should establish the order in which to evacuate—for instance, by floor level.

Evacuate the floor levels above and below the danger area to remove occupants from danger as quickly as possible. Training in such an evacuation usually is made available by building management, with advice supplied by local law enforcement and the fire department.

The evacuation team also may be trained in search techniques, or there may be a separate search team. Volunteers should be sought for this function; however, floor wardens, search monitors, and the like could be assigned to the task. To be proficient in searching the building, search personnel must be thoroughly familiar with all hallways, restrooms, false ceiling areas, and other locations in the building where an explosive or incendiary device could be concealed. When police officers or fire fighters arrive at the building, its contents and floor plan will be unfamiliar to them if they have not previously reconnoitered the facility. Thus it is extremely important for the evacuation or search team to be thoroughly trained and familiar with both the inside of the building and immediate outside areas. When a room or particular area has been searched, it should be marked or sealed with a piece of tape and reported as clear to the appropriate supervisor.

The team will be trained only in evacuation and search techniques and not in the techniques of neutralizing, removing, or otherwise having contact with the device. If a device is located, it should not be disturbed. However, its location should be well marked and the route to it noted.

Search Teams

It is advisable to use more than one individual to search any area or room, no matter how small. Supervisory personnel, area occupants, or trained explosive search teams can conduct searches. There are advantages and disadvantages to each method of staffing the search teams. Using supervisory personnel to search is a rapid approach and causes little disturbance. There will be little loss of employee working time, but a morale problem may develop if it is discovered later that a bomb threat was received and occupants were not informed. Using a supervisor to search usually will not be as thorough because of her or his unfamiliarity with many areas and a possible desire to get on with business.

Using occupants to search their own areas is the best method for a rapid search. Concerns for their own personal safety will contribute to a more thorough search. Furthermore, they are familiar with what does and does not belong in a particular place. Using occupants to search will result in a shorter loss of work time than if all were evacuated before a search by trained teams; it also can have a positive effect on morale if a good training program is provided to develop confidence. Of course, this would require training an entire work force and, ideally, performing several practical exercises. A drawback of this search method is the increased danger to unevacuated workers.

A search conducted by a trained team is the best option for safety, morale, and thoroughness, although it does result in a significant loss of productive time. It is a slow operation that requires comprehensive training and practice. The decision on search team personnel lies with senior management, and it should be considered with and incorporated into the bomb incident plan.

Use of Portable Radios

A common practice among security and law enforcement personnel involved in searching for a bomb is to maintain radio silence during the search out of concern that the radio transmissions of communication devices may cause a bomb device to accidentally detonate. The *Security Management Bulletin* reports that, ''the thinking of security professionals is shifting in regard to this rule . . . the new philosophy advocates sticking with the radios'' (Stratton, 1994, p. 1). The logic behind this is that:

1. Searchers need the mobility of portable communication devices such as cellular telephones and radios (using fixed-position phones is not practical).
2. The chances of detonation are low because the majority of bomb threats are hoaxes.
3. If there is a bomb, the bomber probably would not plant a device that is sensitive to radio waves. ''What bomber planting an explosive device is going to take a chance that a passing vehicle with a phone, CB [citizen's band radio], or other transmitting device could detonate the bomb with him [or her] standing next to it?'' (Stratton, 1994, p. 2).

A possible solution to this issue is that a radio should not be used in the immediate vicinity of a suspected device, but may be considered for use in the general search. Larry Cornelison, Group Manager of the ATF's Los Angeles Arson and Explosives Task Force, made a similar suggestion in a presentation before the Los Angeles Chapter of ASIS on November 22, 1994. At this stage no further information is available on the subject of whether to use radios (or mobile telephones) during searches.

Search Technique

Techniques for searching particular rooms vary in minor ways, but there are basic principles to be followed. (The procedures explained here are based on two-person search teams.) When the team enters the room to be searched, individuals should move to various parts of the room, stand quietly with eyes closed, and listen for a clockwork device (Figure 10.7). Frequently this mechanism can be detected quickly without using special equipment. Even if none is detected, the team is now aware of the background noise level within the room itself. Background noise or transferred sound is always disturbing during a building search. A ticking sound that is heard but cannot be located can be unnerving. The sound could come from an unbalanced air-conditioner fan several floors away or from a dripping sink down the hall. Sound will transfer through air-conditioning ducts, along water pipes, and through walls. A building that has steam or hot water heat is very difficult to search; it will constantly thump, crack, chatter, and tick because of the expansion and contraction of the pipes as steam or hot water moves through them. Background noise also may include outside traffic sounds, rain, and wind. The team's supervisor should look around the room and determine how to divide it for searching and to what height the first searching sweep should extend. This sweep usually covers all items resting on the floor up to the selected height. He or she determines the average height of most items, including table or desk

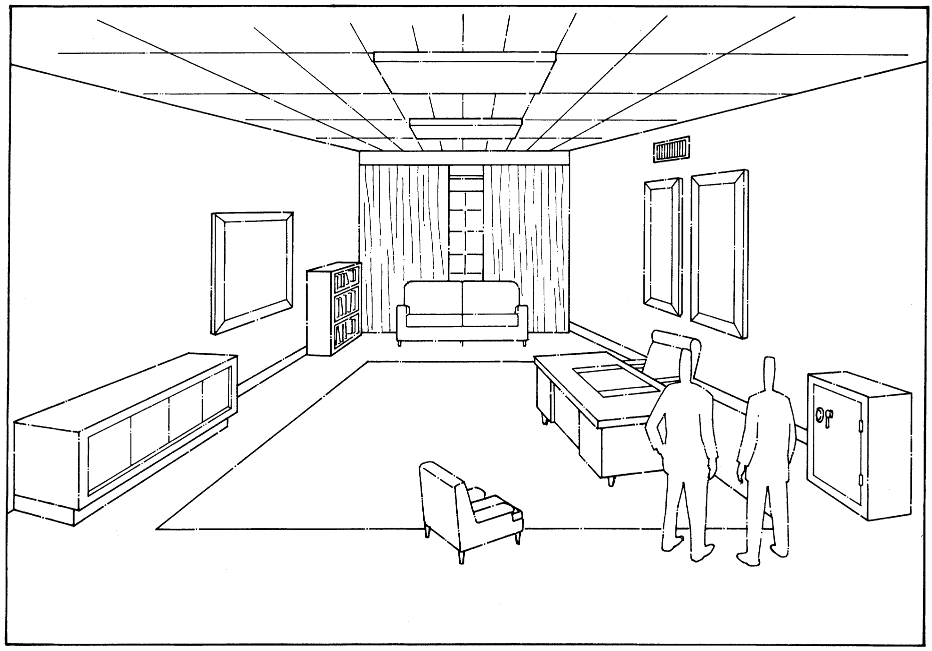


Figure 10.7 Room search—stop and listen. Reprinted with permission from Bomb Threats and Physical Security Planning (ATF P 7550.2, July 1987), U.S. Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms, Washington, D.C.

tops and chair backs, which is usually about waist level (Figure 10.8). Depending on its size, the room should be divided into two relatively equal parts, based on the number and type of objects to be searched and not on its floor area. An imaginary line is then drawn between two objects in the room; for example, from the edge of the window on the north wall to the floor lamp on the south wall.

First Room-Searching Sweep

After the room has been divided and a searching height, such as floor to waist level, has been selected, the two-team members go to one end of the room division line and begin from a back-to-back position. This is the starting point and will be used on each successive searching sweep. Each person now starts thoroughly searching the perimeter of the room, working toward the other person. When the two individuals meet, they will have completed a "wall sweep." They should then work together and check all items in the middle of the room up to the selected height, including the floor under any loose rugs. This first searching sweep also should include any items below this height that are mounted on or in the walls such as air-conditioning ducts, baseboard heaters, and built-in cupboards. This sweep usually takes the most time and effort.

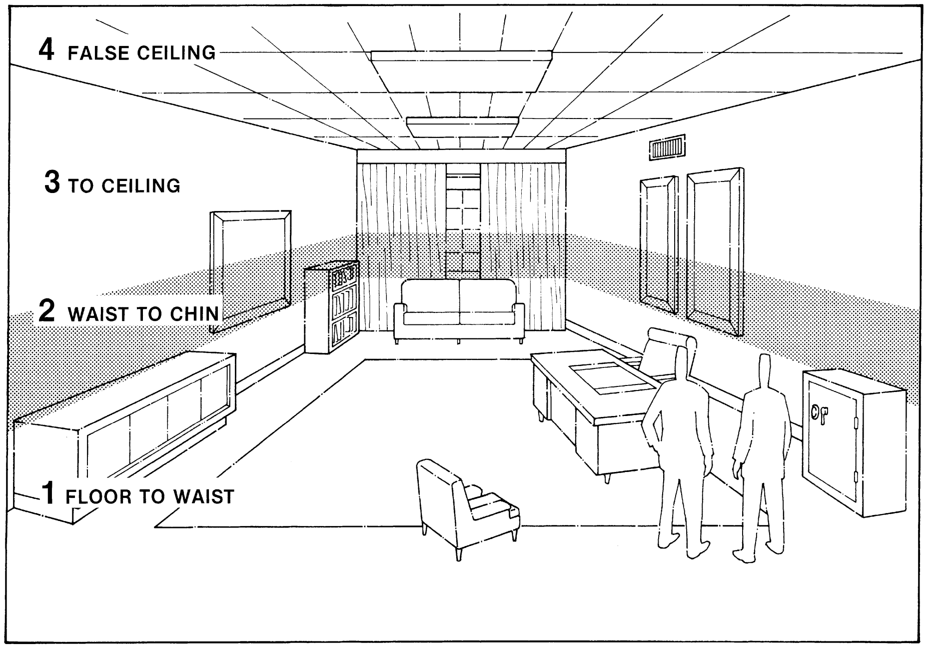


Figure 10.8 Divide room to search into sections by height. Reprinted with permission from Bomb Threats and Physical Security Planning (ATF P 7550.2, July 1987), U.S. Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms, Washington, D.C.

Second Room-Searching Sweep

The team leader again looks at the furniture or objects in the room and determines the height of the second searching sweep—usually from waist level to the chin or top of the head. The two persons return to the starting point and repeat the searching technique at the second height. This sweep usually covers pictures hanging on the walls, built-in bookcases, and tall table lamps.

Third Room-Searching Sweep

When the second searching sweep is completed, the person in charge again determines the next searching height, usually from the chin or the top of the head up to the ceiling. The third sweep is then made. This sweep usually covers high-mounted air-conditioning ducts and hanging light fixtures.

Fourth Room-Searching Sweep

If the room has a false or suspended ceiling, the fourth sweep involves investigation of this area. Check flush or ceiling-mounted light fixtures, air-conditioning or ventilation ducts, sound or speaker systems, electrical wiring, and structural frame members. Post a conspicuous sign or marker indicating "Search Completed" in the area after this sweep. Place a piece of colored tape or a sticker across the door and door jamb approximately two feet above floor level if using signs is not practical.

The room search technique can be expanded and applied to investigating any enclosed area. Encourage the use of common sense or logic in searching. If a guest speaker at a convention has been threatened, for instance, search the speaker platform and microphones first, but always return to the systematic searching technique. Do not rely on random or spot-checking of only logical target areas. The bomber may not be a logical person.

Summary of Search Steps

To summarize, the following steps should be taken to search a room:

1. Divide the area and select a search height
2. Start from the bottom and work up
3. Start back-to-back and work around the perimeter toward each other
4. Go around the walls and proceed toward the center of the room

Suspicious Object Located

It is imperative that personnel involved in a search be instructed that their only mission is to search for and report suspicious objects. Under no circumstances should anyone move, jar, or touch a suspicious object or anything attached to it. The removal or disarming of a bomb must be left to explosive ordinance disposal professionals. When a suspicious object is discovered, follow these procedures:

1. Report the location and an accurate description of the object to the appropriate warden. This information should be relayed immediately to the command center, from which the police and fire departments and bomb squad will be notified; they should be met and escorted to the scene.
2. If absolutely necessary, place sandbags, never metal shields, around the suspicious object. Do not attempt to cover the object.
3. Identify the danger area, and block it off with a clear zone of at least 300 feet, including floors below and above the object [the number of floors to be evacuated will depend on the nature of the device found, the history of these types of incidents, and building policy for handling such situations].
4. Check to see that all doors and windows are open (the latter will not be possible in modern high-rises) to minimize primary damage from blast and secondary damage from fragmentation.
5. Evacuate the building or selected floors as determined by the bomb incident plan.
6. Do not permit occupants to re-enter the building until the device has been removed/disarmed and the building is declared safe.

In planning, building owners and managers should also make arrangements to maintain offsite a supply of up-to-date building plans. These could be kept with the building architect, or even the commercial graphics firm that handles plan changes for the building.

Table 10.1 Bomb Incident Plan

1. Designate a chain of command.
2. Establish a command center based on the recommendations below.
3. Decide what primary and alternate communications will be used.
4. Clearly establish how and by whom a bomb threat will be evaluated.
5. Decide what procedures will be followed when a bomb threat is received or a device discovered.
6. Determine to what extent the available bomb squad will assist and at what point the squad will respond.
7. Provide an evacuation plan with enough flexibility to avoid a suspected danger area.
8. Designate search teams.
9. Designate areas to be searched.
10. Establish search techniques.
11. Establish a procedure to report and track the progress of the search and a method to lead qualified bomb technicians to a suspicious package.
12. Have a contingency plan available if a bomb should go off.
13. Establish a simple-to-follow procedure for the person receiving the bomb threat.
14. Review your physical security plan in conjunction with developing a bomb incident plan.

Command Center (or Emergency Operations Center) Recommendations

1. Designate a primary location and an alternate command center location.
2. Assign personnel and designate decision-making authority.
3. Establish a method for tracking search teams.
4. Maintain a list of likely target areas.
5. Maintain a blueprint of floor diagrams in the center.
6. Establish primary and alternate methods of communication.
7. Formulate a plan for establishing a command center if a threat is received after normal work hours.
8. Maintain a roster of all necessary telephone numbers.

Summary

Develop a bomb incident plan like the one shown in Table 10.1. Draw on any expertise available to you from police departments, government agencies, and security and safety specialists; the local police bomb squad and the local field offices of the ATF can be invaluable sources of information.

The preceding information, including that in Table 10.1, is intended only as a guide. Building management ultimately must determine how to handle a bomb threat situation and assist tenants' management with incidents in specific tenant areas.

Hazardous Materials, Chemical and Biological Weapons, and Nuclear Attack

There are many different names and definitions of the term *hazardous materials*, depending on the nature of the problem being considered. The U.S. Department of Transportation (DOT) and the NFPA use this term. The Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA) use the term *hazardous substances*, but their meaning is different. For our purposes, the NFPA's definition of a *hazardous material* will be used: ''a substance (solid, liquid, or gas) capable of creating harm to people, property, and the environment'' (NFPA *Glossary of Terms*, 2001). These substances may be corrosive, explosive, flammable, irritating, oxidizing, poisonous, radioactive, or toxic in effect. Hazardous materials may be chemical, biological, or nuclear in nature.

In the high-rise setting, hazardous materials may be in a building for legitimate operational purposes or be maliciously introduced into the building to harm people.

Hazardous Materials

In the United States, businesses, by law, must identify known hazardous materials and provide a Material Safety Data Sheet (MSDS) for each such chemical located on-site. As Fischer and Green (1998, p. 284) explain,

> Each MSDS contains seven sections:
>
> 1. Product identification and emergency notification instructions
> 2. Hazardous ingredients list and exposure limits
> 3. Physical and chemical characteristics
> 4. Physical hazards and how to handle them (that is, fire, explosion)
> 5. Reactivity—what the product may react with and whether it is stable
> 6. Health hazards—how the product can enter the body, signs and symptoms of problems, and emergency first-aid steps
> 7. Safe handling procedures
>
> The following hazardous materials, as mentioned in *Hazardous Materials in an Office Environment* (Bachman, 1992, p. 6), may be present within a high-rise office building:

- Photographic materials such as fixer solutions.
- Printing/reproduction/art materials such as inks, thinners, solvents, ammonia, and paint
- Liquid office materials such as cleaners and pesticides.
- Maintenance supplies and materials such as oils, engine fluids, transformer dielectrics, lead acid batteries, paints, thinners, solvents, and fluorescent light tubes.
- Janitorial and cleaning materials such as cleaners containing solvents, acids, caustics, chlorine compounds, pesticides, and polishes.
- Renovation and construction materials (such as varnishes, paints, coatings, glues, sealant, asbestos, and compressed gas).

All polychlorinated biphenyl (PCB)* transformers used in or near a commercial building are required by law to be registered with the building owner, who is responsible for maintaining records and adhering to reporting provisions.

Tenants should be made aware of the fact that they are required to notify building management of hazardous materials within their offices. Tenants should instruct employees who may come into contact with hazardous materials on the location of the MSDS manual, how to interpret the information on MSDS sheets and labels, and how they can obtain additional information regarding hazards. This training should be documented.

*After the World Trade Center's destruction on September 11, 2001, trace amounts of PCBs were found at the site of 7 WTC, the building that housed two electrical substations (''Collapsed 7 WTC contained toxic chemicals,'' January 20, 2002).

The presence of hazardous materials in a building can cause serious problems, particularly when a fire or explosion occurs. The following example illustrates this point.

February 15, 1992, Los Angeles, California—This fire occurred on the seventh floor of the 14-story County Health Building in downtown Los Angeles and was first reported at 10:06 AM. As a result of the fire, smoke and heat damage occurred on the floor of origin and the floors above it, and water damaged floors below it. The fire suppression efforts of the 220 Los Angeles Fire Department fire fighters assigned to this incident were hampered by (1) the fact that the building contained hazardous asbestos materials used in building construction, (2) a lack of automatic fire detection equipment near the origin of the fire to provide early warning, (3) a lack of automatic sprinklers to control the fire in its incipient stage, and (4) the failure of the building's HVAC system to automatically shut down when smoke was detected. Hence, the HVAC system distributed products of combustion to the eighth and ninth floors. The fire was controlled within 1 hour and 20 minutes of the initial alarm. According to the Los Angeles Fire Department, its origin was probably accidental, caused by an arc/short of an undetermined electrical source.

April 25, 2002, New York, New York—A late-morning explosion caused by volatile chemicals severely damaged the façade, hailing sheets of glass and debris onto the street, of a 10-story Manhattan commercial building. The blast, which originated in the basement, was possibly linked to shipments of 50-gallon drums of acetone used by a sign company. ''The explosion, which rocked the busy commercial neighborhood, triggered mass evacuations of surrounding buildings and caused widespread alarm in the area, witnesses said'' (Getlin, 2002, p. 814). Forty-two people were injured in the incident.*

The types of hazardous materials outside a high-rise office building may include PCBs (as already mentioned), radioactive substances in a nearby nuclear facility, potentially dangerous materials transported along an adjacent railway line, or flammable and potentially harmful chemicals contained in a nearby chemical manufacturing plant or oil refinery.

As previously mentioned, ''The most critical risks in high-rise structures include fire, explosion and contamination of life-support systems such as air and potable water supply. These threats can be actualized accidentally or intentionally and because they propogate rapidly can quickly develop to catastrophic levels'' (POA, 2000, p. 19-98). Therefore, to minimize or eliminate the hazards to people, property, or the environment, every hazardous material incident should be handled by building emergency staff according to standard operating procedures.

Procedures for Handling Incidents

Inside the Building

The type of hazardous material, the nature and scope of the incident, and the response specified by the appropriate MSDS will dictate the

*As reported in the *Los Angeles Times* (''N.Y. building blast injures 42,'' April 26, 2002, p. A14).

appropriate response. In addition, the following questions should be considered:

- What outside haz-mat (hazardous material) responding agencies should be immediately notified of the incident?
- Should the affected area be secured and entry to unauthorized persons denied?
- Should the floor involved be sealed and all elevators serving the floor shut down?
- What procedures are needed with regard to HVAC systems serving the floor where the incident has occurred?
- Is it necessary to evacuate occupants from the area or floor where the incident has occurred? Will they be allowed to do so using elevators as well as stairwells? To what area will they be evacuated? Is it necessary to evacuate other floors?
- After the incident has been handled, what agencies must be notified?
- What documentation of the incident is required?

There are a number of agencies and regulations that govern the way hazardous materials are handled and the response to incidents involving these substances. The Superfund Amendments and Reauthorization Act (SARA) of 1986 established controls and requirements for reporting incidents and for emergency response by both industry and public safety agencies. The EPA administers the section of the SARA legislation that requires industry to report releases of hazardous substances to government agencies and the public. In addition, the NFPA has developed many standards relating to hazardous materials such as NFPA 471, *Recommended Practice for Responding to Hazardous Materials Incidents;* NFPA 472, *Standard on Professional Competence of Responders to Hazardous Materials Incidents;* and NFPA 473, *Standard for Competencies for EMS Personnel Responding to Hazardous Materials Incidents*.

If building owners or managers use employees on-site to clean up hazardous materials they must be very careful to ensure compliance with the applicable OSHA regulation, or they could incur substantial penalties and fines. As Giordano (1995, p. 31) details,

> During clean-up operations, the employer must periodically monitor employees who may be exposed to hazardous substances in excess of OSHA's regulations. Once the presence and concentration of specific hazardous substances and health hazards have been established, employees involved in the clean-up operations must be informed of any risks associated with their work. Under certain circumstances, regular ongoing medical surveillance of employees by a licensed physician, and without cost to the employees, may be required.

Outside the Building

As just described, the type of hazardous material and the nature and scope of the incident will largely determine the appropriate response. However, there is one major consideration in handling such an incident: Are occupants to be evacuated from the building, or will they be able to remain in the building?

If they are to be evacuated, building management must decide when this will occur, whether evacuees will be allowed to use elevators as well as stairwells, and to what areas they will be moved. If occupants remain, it must be decided whether the building HVAC systems should continue to operate and whether doors and openings to the building should be sealed.

Chemical and Biological Weapons

The threat of chemical and biological weapons (CBW) has existed for some time in the modern world. However, over the past decade, the potential for the use of CBW against civilians has dramatically increased.

As early as 1995, European intelligence officials learned that chemical and biological warfare instructions disseminated from Al Qaeda sources in Pakistan and Afghanistan were circulating among Islamic terrorist cells. That year, Belgium police seized what turned out to be an 8000-page guerilla manual for jihad. One chapter, titled ''How to Kill,'' described how to prepare ''toxins, toxic gas and toxic drugs'' (Pyes and Rempel, 2001, p. A1).

The potential for deliberate contamination of buildings with toxic chemical substances, such as sarin gas or hydrogen cyanide, and dangerous biological material, such as anthrax (*Bacillus anthracis*), became of heightened concern due to the post-September 11, 2001, mailing of anthrax-tainted envelopes in the United States.

> *March 1995, Tokyo, Japan*—Sarin gas was deliberately released by a Japanese cult terrorist group on a Tokyo subway. It killed 13 people and led to 5000 more who sought medical attention. ''First responders had difficulty in identifying the odorless, colorless chemical and in knowing how to simultaneously protect themselves, handle mass casualties and stop the toxin from spreading in the subway system. Some of the deaths included subway maintenance workers who rushed to the scene and unknowingly touched, breathed in and further agitated the lethal nerve agent'' (''Sensors of chemical warfare agents make a mass-transit debut,'' July 14, 2000, p. 2).

> *September 2001, East Coast United States*—Five anthrax-contaminated letters were mailed to two liberal Democratic senators and news media (CBS, NBC, and the New York Post). These letters were received soon after the September 11, 2001, terrorist attacks on the New York World Trade Center and the Pentagon and led to the deaths of five people. According to Barbara Rosenberg, a molecular biologist, ''The anthrax discovered in the letters mailed to the two U.S. senators was so refined that it contained 1 trillion spores per gram, characteristic of the 'weaponized' anthrax made by U.S. defense labs'' (Neuman, 2002, p. A20) The suspected perpetrator(s) of these biological attacks range from a disgruntled scientist to accomplices of the September hijackers or to right-wing extremists.*

The difference between a chemical and biological attack is that ''a biological [and radiological] agent will almost never cause immediate symptoms; a chemical agent almost always will'' (Berkeley Lab, April 2002).

Law enforcement, fire, and emergency services are preparing for chemical and biological attacks within their communities. As new research becomes available, some of the recommended protocols for dealing with chemical and biological attacks will change. The following guidelines are given with that clear understanding.

*As reported in the *Los Angeles Times* (Neuman, April 21, 2002, p. A20).

*Pre-Event Advice for Safeguarding Buildings Against Airborne Chemical or Biological Attack**

- Identify building fresh air intakes and prevent unauthorized access [Figure 10.9 indicates ways to enclose vulnerable outdoor air intakes]. Also utilize security measures such as intrusion detection devices, security personnel, and CCTV to detect security breaches.
- Control access to building HVAC rooms and mechanical areas.
- Isolate mail room HVAC systems from building HVAC systems.†

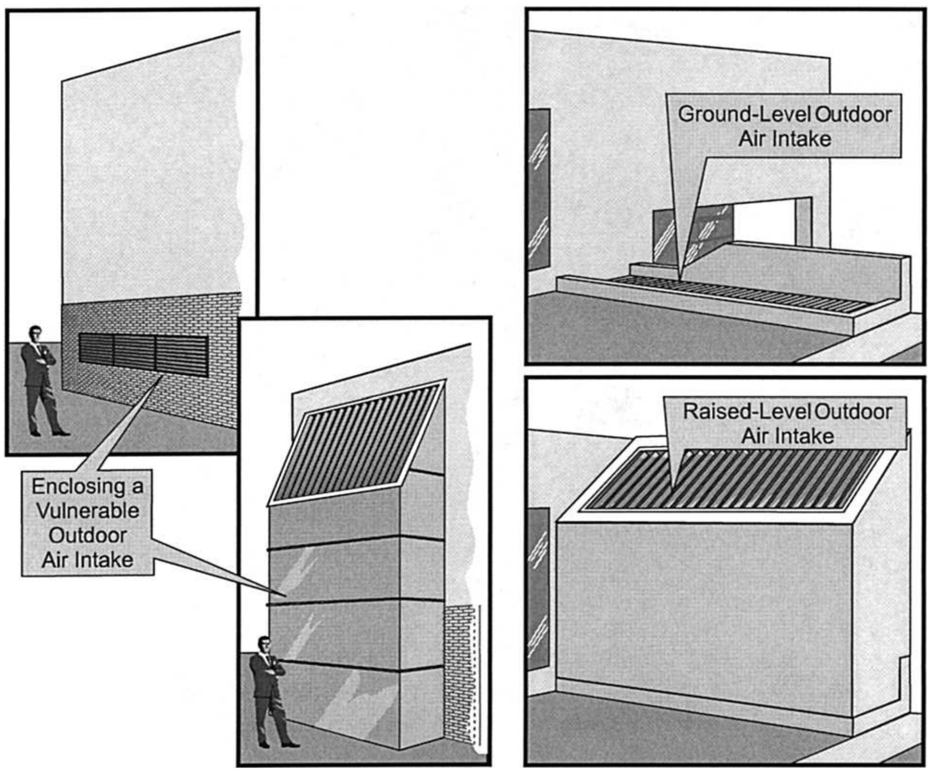


Figure 10.9 Ways to enclose vulnerable outdoor air intakes. Used with permission from NIOSH *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks* (Department of Health and Human Services, Centers for Disease Control and prevention, May 2002, p. 10).

*This information was primarily obtained from a web site (*http://securebuildings.lbl.gov*) developed by researchers of the U.S. Department of Energy's Lawrence Berkeley National Laboratory and is ''appropriate for small and medium sized releases [of chemical and biological agents] such as those that would be expected from a terrorist attack, not for industrial-scale releases. . . . The scientists plan to update the site as new research results on protecting buildings from chemical and biological attacks become available'' (Berkeley Lab, April 2002).

†Isolating a mailroom will involve sealing existing air vents and doors and installing a separate ventilation system. It may also require relocation of the mailroom itself to another area of the building or moving it outside of the building.

- Control distribution of building plans and the design of the building's HVAC system (and restrict dissemination of information pertaining to the operation of the building, including security and fire life safety systems, only to authorized personnel).
- Develop an emergency response plan, including ensuring that building personnel know how to operate building HVAC systems.
- Rehearse response procedures for inside-building and outside-building releases of chemical and biological agents.

Response to an Airborne Chemical or Biological Agent Release

The nature of the response to an airborne agent release will depend on whether a chemical or biological agent is involved, and whether the release has occurred inside or outside of a building. ''For a biological agent the goals are to reduce the total number of people exposed and to be sure that you can find everyone who was exposed. For a chemical release, the goal is to minimize the concentrations to which people are exposed'' (Berkeley Lab, April 2002).

Two critical decisions that will need to be made quickly relate to the operation of HVAC systems within a building, and whether building occupants need to be evacuated to a safe area. In a high-rise, the impact of the release of airborne chemical or biological agents is accentuated by the fact that a building's HVAC systems could provide a means for the rapid spread of contaminants throughout a building. This fact has caused considerable debate among industry experts as to what actions should be taken with regard to these complex systems, whose operations often vary from building to building and system to system.

If there is contamination of a building, it will need to be partially or completely closed and cleaned thoroughly.

ASHRAE Initial Report

The American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (ASHRAE), in an initial report issued in January 2002, *Risk Management Guidance for Health and Safety Under Extraordinary Incidents,* stated, ''Do not close outdoor air intake dampers or otherwise block ventilation paths; do not change the designed airflow patterns or quantities; and do not modify the fire protection and life safety systems without approval of the local fire marshal'' (Post, 2002, p. 12). Commenting in the *Engineering News-Record*, Nadine M. Post says that,

> Risk Management Guidance for Health and Safety Under Extraordinary Incidents also offers guidance on steps that can be taken to render buildings somewhat less vulnerable to bioterrorism and other attacks. But for the time being, unless the building is an obvious target, ASHRAE recommends operating buildings normally and, in every case, not making any changes without consulting a professional engineer or expert.
>
> The report, written by a 10-person committee, is not a ''definitive piece'' and not based on a specific building or HVAC system, said James E. Woods, committee

> chair and president of HP Woods Research Institute, Herndon, VA. It does advise owners to get to know their buildings before making changes and to develop a preparedness plan in case of an incident. It is important to look at the building operation as a whole and to avoid measures that can backfire, caution the authors. For instance, closing off air intake vents can decrease a system's ability to purge contaminants.
>
> Sensors and other warning devices are not available or are not reliable for many contaminants so they cannot be used as a control strategy, says the report. For protection against aerosol attacks from outside, openings ''must be capable of timely closure, located sufficiently remote from any launch site or the building must be equipped with adequate filtration.''
>
> Areas of refuge are not economically viable in many buildings. Consequently HVAC systems can be used to pressurize building egress paths and to isolate significant contamination to ''selected building volumes,'' says the report. Finally, enhanced air filtration alone is not sufficient to reduce airborne contamination. It should be coupled with pressurization of the interior relative to outdoors.

Post says that ASHRAE plans with the aid of a year-long exercise to develop more specific guidance and to coordinate its efforts with other engineering disciplines involved in similar studies.

Berkeley Laboratories Advice

The Berkeley Laboratories web site provides advice on handling a chemical or biological attack involving an indoor or outdoor release. Included among the supplied information is the statement that, ''for any indoor release, whether chemical or biological: if evacuation can be done safely, evacuate the building to a meeting point upwind of the building'' (Berkeley Lab, April 2002). For an open-air, outdoor release, they recommend, ''people should stay indoors, unless authorities give an evacuation order'' (Berkeley Lab, April 2002). Technical advice on whether to shut off or leave the HVAC system operating, whether to pressurize stairwells, or whether to put the building into ''smoke removal'' mode are discussed.

How Should a Building Prepare?

It is not within the scope of this book to detail exactly how a building should prepare for a chemical or biological attack. Each building owner and manager should analyze the potential for such an event to occur at their site, identify the vulnerabilities of the building to such an event, and design countermeasures to address those weaknesses. They should then, in conjunction with local emergency response agencies, and possibly ''a qualified HVAC professional that understands the ramifications of various HVAC operating modes on building operation and safety systems,'' (NIOSH, 2002, p. 15), develop an emergency response plan based specifically on the building's needs and the operating systems that exist within it.*

*There are a number of web sites providing up-to-date information on chemical and biological agents. These include the Federal Emergency Management Agency (FEMA), *http://www.fema.gov*; the Centers for Disease Control and Prevention (CDC), *http://www.cdc.gov*; the United States Postal

It must be realized that, ''no building can be fully protected from a determined individual who is intent on releasing a chemical, biological, or radiological (CBR) agent.... However, facility owners and managers can transform their buildings into less attractive targets by increasing the difficulty of introducing a CBR agent, by increasing the ability to detect terrorists before they carry out an intended release, and by incorporating plans and procedures to mitigate the effects of a CBR release'' (NIOSH, 2002, p. 2).

Nuclear Attack

As unlikely as a nuclear attack may be, the events of September 11, 2001, have brought the widespread realization that certain individuals in this world will stop at nothing to achieve their objectives. Therefore, a nuclear attack needs to be addressed as a possible threat faced by high-rise buildings situated in major urban centers with large populations.

The Institute of Real Estate Management (IREM, 1990, p. 165) states:

> The immediate effects of a nuclear attack are unmistakable: a flash of intense light followed by a blast of heat and radiation. Likewise, the secondary effect is [well] known... radioactive fallout. The degree of immediate and secondary effects will depend on the size and type of weapon, the terrain (hilly versus flat), the height of the explosion (e.g., near or far from the ground), the distance from the explosion, and weather conditions.
>
> People near the explosion most likely would be killed or seriously injured by the initial blast, heat, or radiation. Those several miles away from the explosion would be endangered by the initial blast, heat, and subsequent fires. Others probably would survive but would be affected by radioactive fallout. It is for these people that an emergency plan must be provided.
>
> The only precaution that a property manager can take to prevent loss due to a nuclear attack is to provide an emergency shelter for occupants, employees, and others at the property at the time of such an attack. Such a shelter could be a special building, underground bunker, or any space with walls and roof thick enough to absorb radioactive rays given off by fallout.

''There is also growing concern about so-called dirty bombs,* laced with radioactive material from a hospital, nuclear plant or manufacturing facility, for instance, that can contaminate the environment'' (Zimmerman, 2002, p. R7).

Service (USPS) with information on handling anthrax-contaminated mail, *http://www.usps.gov*; and the Occupational Safety and Health Administration (OSHA), *http://www.osha.org*. Also, the National Institute for Occupational Safety and Health (NIOSH), *http://cdc.gov/niosh*, has released *Guidance for Protecting Building Environments form Airborne Chemical, Biological, or Radiological Attacks*, Publication No. 2002-139. This document identifies actions that a building owner or manager can implement after an airborne chemical, biological, or radiological attack (CBR).

*Radiological or ''dirty bombs'' consist of conventional explosives encased in radioactive waste material. If detonated, this would disperse radioactive material over an area determined by the size of the explosion, the kind and amount of material, weather conditions, and the types of facilities in the vicinity (Willman and Munn, 2002, p. A16). After the detonation of a dirty bomb in a major urban area, as the level of radioactivity increased it could ''spark panic, overburdening the health-care system and perhaps forcing abandonment of many square blocks for decades'' (Willman and Munn, 2002, p. A16).

After the Attack

Emergency food and water supplies (public water supplies may not be safe for consumption due to radioactive contamination) will need to be provided for a time after the attack for people sheltering from the deadly fallout of radioactive particles.

> The advice is simple: Stay indoors for the first 24 hours after the initial explosion. This is the most dangerous period when radioactive fallout particles fall. Once they have hit the ground, these particles decay fairly rapidly. It probably would not be necessary to remain in the shelter more than one to two weeks, and more likely, people could leave the shelter for short periods of time after a few days. (IREM, 1990, p. 166)

Aircraft Collisions

Before discussing the September 11, 2001, destruction of the New York World Trade Center, it is appropriate to restate the text that appeared in the first edition of this book.

> A high-rise building, like any other, is vulnerable to the remote possibility that an aircraft flying off-course could collide with it. Obviously, the additional height, as compared with other structures, makes them more susceptible.
>
> *July 28, 1945, New York City*—At approximately 10:00 A.M. on a rainy, foggy Saturday, a U.S. Army Air Corps B-25 bomber crashed into the north wall of the 102-story Empire State Building (Figure 10.10). The impact tore a hole, approximately 20 feet by 18 feet, in the exterior wall of the building at the 78th and 79th floors, and a portion of the plane actually crossed one floor and exited through the south wall. The crash, along with several fires that resulted from flaming gasoline, resulted in the deaths of 3 crew members of the plane and 11 building occupants, injuries to 25 persons including several with severe burns, and property damage estimated at half a million dollars. A severed standpipe and damaged elevators caused by the crash restricted New York City Fire Department fire fighters' efforts; however, within an estimated 35 minutes they were able to control the fire. Despite the severity of the collision, the structural integrity of the building held.
>
> Because the majority of today's airplanes travel at higher speeds and are much larger, heavier, and carry far greater fuel loads than the B-25 that collided with the Empire State Building, a similar incident involving a modern high-rise building would have far more devastating consequences.
>
> The response to such an incident should be similar to that required for an explosion or fire. There would need to be an immediate call to the fire department to request assistance, and rapid evacuation of any building occupants from the affected area, including any injured persons, if remaining would subject them to more serious injury. Any fire would have to be contained and suppressed if safe to do so. Unauthorized persons would be restricted from entering the building or the actual incident scene, and a command center would be set up to oversee operations.

The author, like most people, never considered the possibility that such an incident would be deliberately planned and executed.

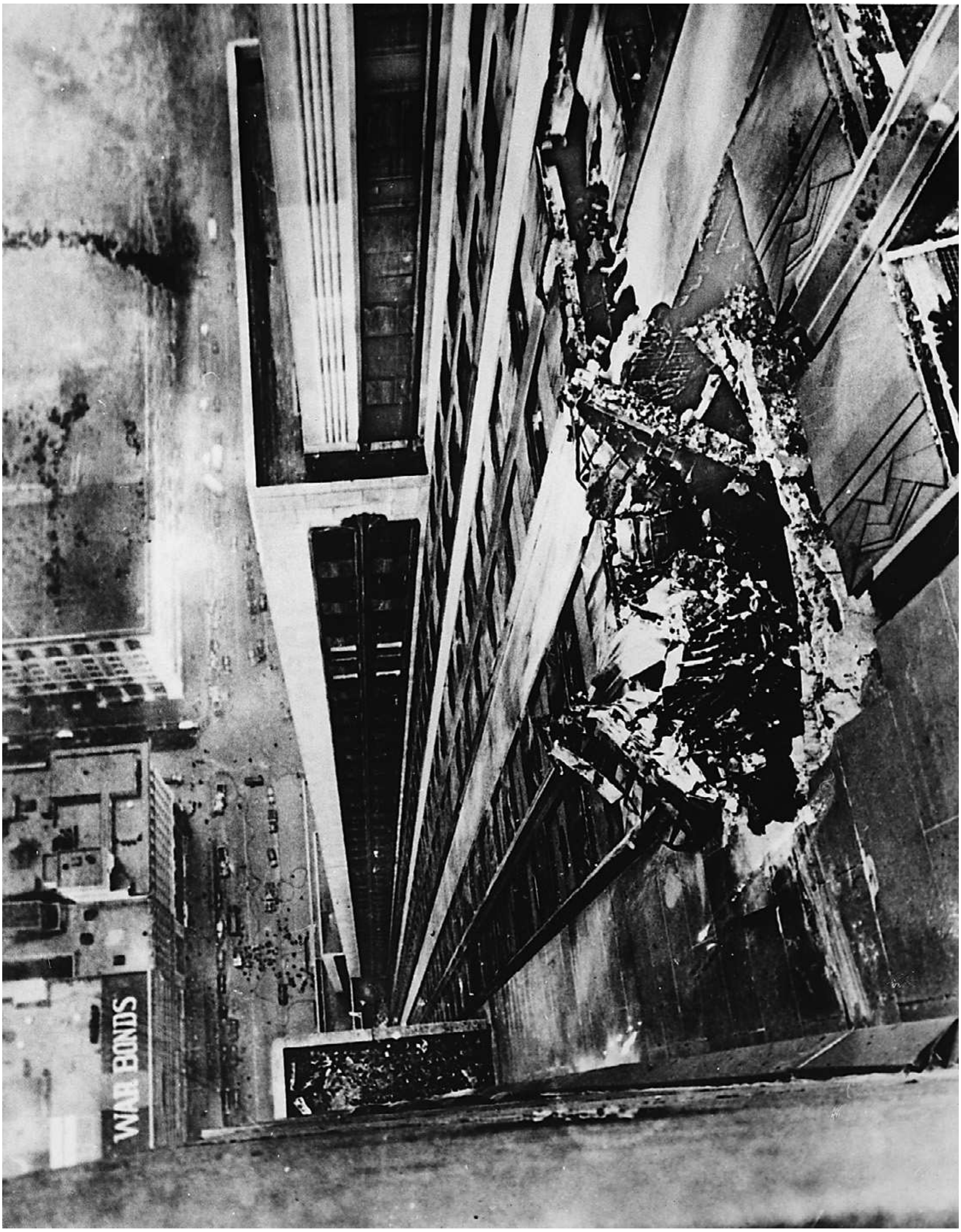


Figure 10.10 BOMBER STRIKES THE EMPIRE STATE BUILDING—A view from an upper floor of the building vividly shows the gaping hole at the 79th floor created by the impact of a B-25 bomber. Part of the wreckage of the plane, which crashed into the building on July 28, 1945, protrudes from the opening. Used with permission from AP/WIDE WORLD PHOTOS.

Before specifically addressing the World Trade Center, it is noteworthy that soon after September 11, 2001, there were two incidents involving light aircraft crashing into high-rise buildings.

> *January 5, 2002, Tampa, Florida*—Late on Saturday afternoon, a stolen Cessna 172 single-engine plane piloted by a 15-year-old boy crashed into the 28th floor of the 42-story Bank of America building. The single-engine plane appeared to have been deliberately flown into the building causing damage to an office and the death of the pilot. None of the six to eight people in the high-rise at the time of the incident were injured (Yanez, 2002, p. A1).

> *April 18, 2002, Milan, Italy*—At 5:50 PM, a small twin-engine aircraft piloted by an elderly businessman crashed into the 25th floor of 30-story Pirelli Tower, the tallest building in Milan, killing a cleaning woman, a government lawyer, and the pilot. At least 60 people were injured. The pilot reported mechanical trouble shortly before impact.*

The structural damage to both buildings was localized to the point of impact of the light aircraft.

New York World Trade Center September 11, 2001, Terrorist Attack

On the morning of September 11, 2001, within a 42-minute time frame, four commercial airliners fully loaded with fuel for transcontinental flights departed from Boston, Washington, D.C., and Newark airports. Within minutes of take-off, four- to five-man teams on board hijacked these planes. Two of these aircraft, each with a fuel-carrying capacity of 23,980 U.S. gallons (90,770 L) of aviation fuel and a maximum takeoff weight of 395,000 lbs. (179,170 kg) (FEMA, 2002, p. E-1), rammed into the Twin Towers of the World Trade Center in New York City. This soon resulted in the total collapse of both these 110-story buildings. One other plane smashed into the Pentagon in Washington. The fourth, reportedly bound for the White House, crashed in an open field in Pennsylvania after several of its passengers fought against the hijackers. These incidents constituted the most destructive terrorist acts ever committed against the United States. ''The events in New York City on September 11, 2001, were among the worst building disasters and loss of life from any single building event in the United States'' (FEMA, 2002, p. 1-1).

Sequence of Events

The events† on that fateful day were as follows:

> 8:46:26 AM—American Airlines Flight 11, a Boeing 767 airliner, with 81 passengers and 11 crew on board a scheduled flight from Boston to Los

*As reported in the *Los Angeles Times* (Boudreaux, 2002, p. A3).

†The exact times (Eastern Daylight Time) of the impact of the planes and the collapse of the twin towers were obtained by Columbia University scientists using a seismograph connected to an atomic clock. The plane that hit the north tower ''registered magnitude-0.9 on the seismograph, equal to a small earthquake'' (Cauchon, 2001, p. 3).

Angeles, crashed into the north side of the north tower (WTC 1) of the World Trade Center. The north tower was struck between the 94th and 98th floors. ''It wrecked the [three] stairwells on the 92nd floor'' (Cauchon, 2001, p. 3).

9:02:54 AM—United Airlines Flight 175, a Boeing 767 airliner, with 56 passengers and nine crew on board, also on a scheduled flight from Boston to Los Angeles, crashed into the south side of the south tower (WTC 2) of the World Trade Center and struck the 78th through 84th floors. ''One stairway [of the three] in the south tower remained open after the crash, but few used it to escape'' (Cauchon, 2001, p. 2).

Figure 10.11 depicts the approximate flight paths of the two aircraft. ''Each plane banked steeply as it was flown into the building, causing damage across multiple floors. According to Government sources, the speed of impact into the north tower was estimated to be 410 knots, or 470 miles per hour (mph), and the speed of impact into the south tower was estimated to be 510 knots, or 590 mph. As the two aircraft impacted the buildings, fireballs erupted. The term fireball is used to describe deflagration, or ignition, of a fuel vapor cloud'' (FEMA, 2002, p. 1-4). ''Remaining fuel flowed across the floors and down elevator and utility shafts, igniting intense fires throughout upper portions of the buildings. As these fires spread, they further weakened the steel-framed structures, eventually leading to total collapse'' (FEMA, 2002, p. ES-1). Figure 10.12 shows the areas where aircraft debris landed outside of the towers.

9:59:04 AM—56 minutes after it was hit, the top floors of the south tower collapsed, causing the entire building to fall down.

10:28:31 AM—1 hour and 43 minutes after it was struck, the north tower collapsed (Figure 10.13).

According to FEMA (2002, pp. ES-1, ES-8),

As the towers collapsed, massive debris clouds consisting of crushed and broken building components fell onto and blew into surrounding structures, causing extensive collateral damage and, in some cases, igniting fires and causing additional collapses. . . . Most of the fires went unattended as efforts were devoted to rescuing those trapped in the collapsed towers. The 22-story Marriott World Trade Center Hotel (WTC 3) was hit by a substantial amount of debris during both tower collapses. Portions of WTC 3 were severely damaged by debris from each tower collapse, but progressive collapse of the building did not occur. However, little of WTC 3 remained standing after the collapse of WTC 1. WTC 4, 5, and 6 had floor contents and furnishings burn completely and suffered significant partial collapses from debris impacts and from fire damage to their structural frames. WTC 7, a 47-story building that was part of the WTC complex, burned unattended for 7 hours before collapsing at 5:20 P.M. . . . In total, 10 major buildings experienced partial or total collapse and approximately 30 million square feet of commercial office space was removed from service, of which 12 million belonged to the WTC Complex. (Figure 10.14).

The Port Authority estimated that on September 11, 2001, the population of the WTC complex was 58,000 people, including those in the Port Authority Trans-Hudson and the Metropolitan Transit Authority subway stations and the

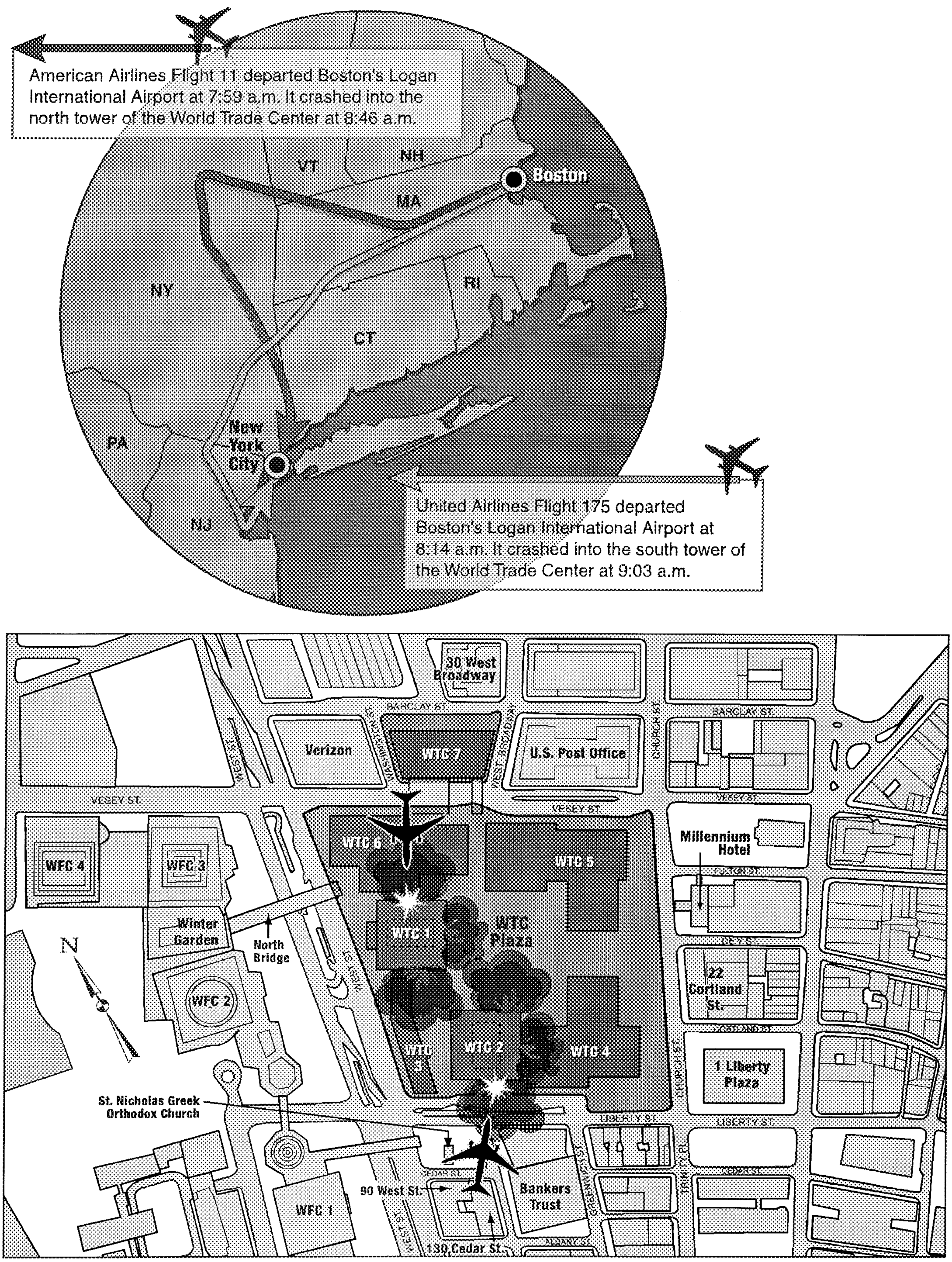


Figure 10.11 Approximate flight paths for the two aircraft. Used with permission of FEMA (World Trade Center Building Performance Study, FEMA 403, p. 1-5)

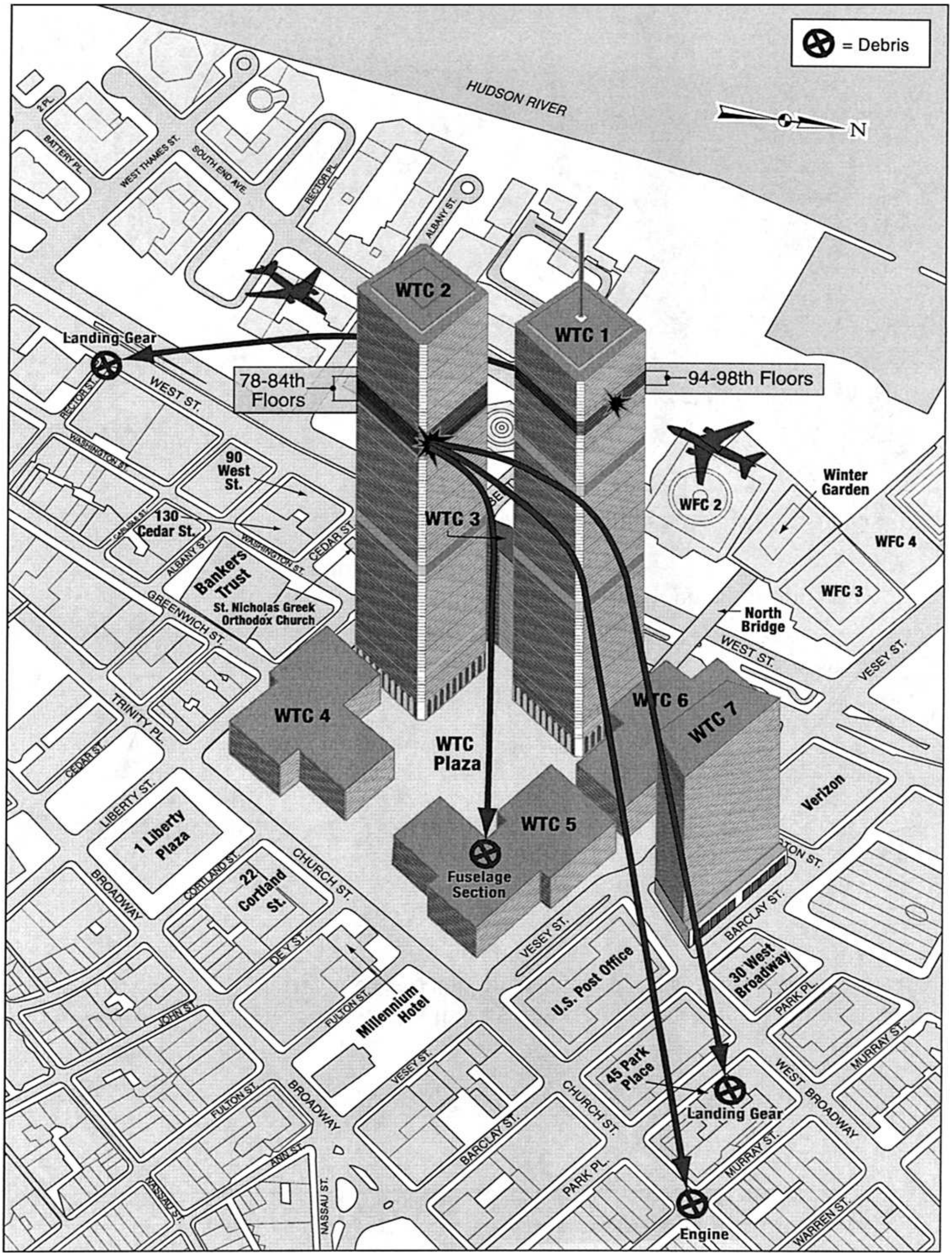


Figure 10.12 Areas of aircraft debris impact. Used with permission of FEMA (World Trade Center Building Performance Study, FEMA 403, p. 1-6).

Figure 10.13 UNBELIEVABLE HORROR. Plumes of smoke pour from the World Trade Center buildings in New York on Tuesday, September 11, 2001. Planes crashed into the upper floors of both World Trade Center towers 16 minutes and 28 seconds minutes apart in a horrific scene of explosions and fires that lead to the collapse of the 110-story buildings. The Empire State Building is seen in the foreground. Used with permission from AP/WIDE WORLD PHOTOS (AP Photograph/Patrick Sison).

Figure 10.14 UTTER DEVASTATION. The Woolworth Building rises behind the rubble of the collapsed World Trade Center buildings in New York on September 18, 2001. Used with permission from FEMA News Photo (Photograph by Michael Rieger).

Concourse areas (FEMA, 2002, p. 1-4). ''The buildings were half-empty when the jets struck.* *USA TODAY* estimates 5,000 to 7,000 people were in each tower when the attack began'' (Cauchon, 2001, p. 2). Of the estimated 10,000 to 14,000 people in the towers, plus the thousands using the underground complex, 2823† people perished and thousands were injured. ''Most of the dead were in the north tower, the first one hit and the second to collapse. *USA TODAY* documented 1,434 who died in the north tower versus 599 in the south tower. . . . Ten bystanders were killed outside by falling debris'' (Cauchon, 2001,

*The lower than usual population was attributed to the fact that some people were voting in New York City's mayoral primary election; some were taking their children for the first day of the school; due to Asia's financial recession many Asian investment firms had released employees or closed offices in the WTC; the 107th floor south tower observation deck was not scheduled to open until 9:30 AM; most retail stores under the complex were not yet open; and being 8:46 AM, a lot of workers were yet to arrive (Cauchon, 2001, p. 5).

†Estimated numbers of persons whose names were to be read at September 11, 2002, memorial observances in New York ('' 'Powerful' Sept. 11 observances set,'' August 7, 2002, p. A13).

pp 1, 3). Many were trapped in the 99 elevators in each tower. The death toll included 343 New York City firefighters, 23 New York City Police Officers, 37 Port Authority Police Officers, six members of ASIS, 13 private security officers who worked at the World Trade Center complex and one at a nearby building, and 157 people on the two planes. The total monetary loss from this disaster is estimated at between $40 and $70 billion.

World-Wide Impact

Shockwaves from these diabolical acts, and that simultaneously enacted upon the Pentagon in Washington, D.C., using an American Airlines Boeing 757 airliner, reverberated throughout the United States and the world. Within 22 minutes of the second plane hitting the World Trade Center, the Federal Aviation Administration grounded all U.S. domestic flights. Within hours, owners and managers of major U.S. high-rise office buildings, including the Sears Tower in Chicago, advised occupants to leave their buildings. *The Los Angeles Times* (Gold and Farley, 2001, p. A-10) reported that even in Europe, high-rise buildings were evacuated by authorities as a safety measure. U.S. markets closed and foreign stock markets plummeted. U.S. President George Bush declared the attacks in New York and Washington as ''Acts of War.'' In October 2001, a U.S.-led coalition began bombing Afghanistan, the country harboring the Al Qaeda terrorist organization, and its infamous leader, Osama Bin Ladin, who had been identified as the instigator of the attacks. The terrorist-supporting Taliban regime was ousted from power and a new government established.

Evacuation a Success

''*USA TODAY* spent two months finding out precisely what happened in the 1 hour, 42 minutes and 5 seconds from the first jet crash to the last building collapse. The newspaper identified where 95% of the victims worked or were located at the time of the attacks. In addition, it matched floor plans, architectural drawings and photographs to the accounts of survivors and victims'' (Cauchon, 2001, p. 2). Their findings indicated that, ''in each tower, 99% of the occupants below the crash site survived'' (Cauchon, 2001, p. 1).

The following is a brief summary, extrapolated from the *USA TODAY* article, of fatalities and injuries relative to the crash sites:

	WTC 1 NORTH TOWER*	WTC 2 SOUTH TOWER†
CRASH SITE AND ABOVE	1360 people died; none survived	595 people died
BELOW THE CRASH LINE	72 died and more than 4000 survived.	4 people died

*Floors could not be determined for two people who died in the north tower.
†Nobody who worked on the 58th floor or below is known to have died.

> Nearly everyone's fate inside the 110-story towers was sealed at the moment the jets hit. (Cauchon, 2001, p. 3)

''Almost everyone [i.e., the building occupants] in WTC 1 and WTC 2 who was below the impact areas was able to safely evacuate the buildings, due to the length of time between the impact and collapse of the individual towers'' (FEMA, 2002, p. 1-4).

The majority of occupants who died in the north tower (the first building struck and the second to collapse) were those on the crash floors or those trapped above the point of impact due to the fact that all three* of the building stairwells were severely damaged and could not be used as a means of escape.

The majority of occupants who died in the south tower were those on the crash floors or those trapped above the point of impact due to the fact that of the three building stairwells only ''one stairway† in the south tower remained open above the crash, but few used it to escape. Stairway A, one of the three, was unobstructed from top to bottom. . . . Others went up these stairs in search of a helicopter rescue that wasn't possible because of heavy smoke on the rooftop'' (Cauchon, 2001, p. 2). According to *USA TODAY*, 16 people from the 78th, 81st, and 84th floors went to safety down Stairway A (Cauchon and Moore, 2002).

Many people died entrapped in elevators.‡ ''An analysis shows that two thirds of south tower occupants evacuated the upper floors during the 16½ minutes between the attacks . . . The fate of more than 2,000 people on the south tower's upper floors was determined by what they did during that time. Most made the right decisions. They left soon after the first jet hit the north tower'' (Cauchon, 2001, pp. 2, 5).

Information obtained (Prouix and Fahy, 2002) from various media reports and a preliminary analysis of over 250 first-person accounts (NFPA and NRCC initiative) indicate that,

> In Tower 1, many reported leaving ''immediately.'' As many others reported ''routine'' activities, gathering belongings, or short delay. However, some delayed as long as 20 minutes or more before beginning evacuation.
>
> People on floors 90 and 91 [of Tower 1] evacuated in times as short as 45 minutes on September 11th. (In 1993, the median evacuation time from the 90th floor was 2½ hours. No one evacuated in less than 2 hours.)
>
> In Tower 2, most reported leaving right after Tower 1 was hit. . . . Once Tower 2 was hit, no one reported delaying their evacuation.
>
> Building occupants [of Tower 2] had less than one hour to evacuate before the collapse [56 minutes after the plane hit the tower, it collapsed].

---

*''The World Trade Center had an excellent stair system, much better than required by building codes—both when it was built 30 years ago and now. Each tower had three stairwells. New York City building codes require two. Stairways A and C, on opposite sides of the building's core, were 44 inches wide. In the center, Stairway B was 56 inches wide. The bigger the stairway, the faster an evacuation can proceed. In 44-inch stairways, a person must turn sideways to let another pass—for example, a rescuer heading up. In a 56-inch stairway, two people can pass comfortably'' (Cauchon, 2001, p. 4).

†''An elevator machine room on the 81st floor, where the jet's nose hit, helped protect one stairway in the south tower. Sixteen people used the stairway to escape. They were the only people in either tower to get out at the level of impact or above. . . . The elevator equipment room covered more than half the width of the 81st floor. Its size forced the tower's designers to route Stairway A around the machines. The detour moved Stairway A from the center of the building . . . (on most floors, the stairways were about 30 feet apart in the core) . . . toward the northwest corner—away from the path the hijacked jet would take (Cauchon and Moore, 2002, pp. 1–3).

‡''Eighty-three [elevator] mechanics from ACE Elevator of Palisades Park, N.J., left the buildings when the second jet hit. Dozens of people were trapped inside elevators at the time, according to the Port Authority. An elevator mechanic from another company rushed to the buildings from down the street and died trying to rescue people'' (Cauchon, 2001, p. 3).

> There were a number of evacuees with disabilities that included two blind men with guide dogs, two deaf people and several wheelchair users.

All indications are that the occupants who were able to evacuate did so in an orderly and competent manner. The World Trade Center had a comprehensive, well-executed fire life safety program and emergency plan that helped emergency staff and occupants to react appropriately to the catastrophic events that unfolded.

One clear message that applies to all high-rise buildings, whether they are evaluated to be at risk to a terrorist event or not, is that all occupants should be well trained in evacuation procedures.

What About Reports of Evacuating Occupants Returning to their Offices?

Some media reported that after the first plane hit, occupants evacuating the south tower were told* that their building was safe. Reportedly, some of these people returned to their floor and later perished when the south tower collapsed.

It must be realized that at the time the first plane hit the north tower, no one explicitly knew that this was a deliberate act of terrorism or that another aircraft was only 16 minutes and 28 seconds away from slamming into the south tower. After the first collision, there were large amounts of material from the crash site falling to the ground outside of the buildings. The first priority of the WTC emergency personnel would have been to take immediate actions to address the life safety of occupants in the north tower. Based on the information known at the time, it would not have been considered prudent to evacuate occupants from the south tower, because this may have involved placing those persons in considerable danger of falling debris. It was only after the second plane hit that an indication of the diabolical nature of the disaster was known.

World Trade Center Building Performance Study

The Federal Emergency Management Association (FEMA) and the American Society of Civil Engineers (ASCE), in association with New York City and several other federal agencies and professional organizations, formed a Building Performance Study (BPS) Team† of specialists in tall building design and engineering to evaluate the performance of buildings at the World Trade Center site (FEMA, 2002, p. 1-1). This team produced the *World Trade Center Building Performance Study: Data Collection, Preliminary Observations and Recommendations*.

---

*According to information obtained from various media reports ''announcement(s) in Tower 2 told occupants that the situation involved Tower 1. Beyond that, there is wide variety in reports of wording'' (Prouix and Fahy, 2002)

†Sometimes referred to as the Building Performance Assessment Team (BPAT), the team included personnel from the National Institute of Standards and Technology, the U.S. Fire Administration, the Worcester Polytechnic Institute, the Fire Department of New York, the New York City Office of Emergency Management, The Port Authority of New York and New Jersey, and the Structural Engineers Association of New York. Report reviewers included the American Institute of Steel Construction, various structural engineering groups, and the National Fire Protection Association.

Observations and Findings

The following observations and findings are from the *World Trade Center Building Performance Study* (FEMA, 2002, pp. ES-1–ES-3):

> The structural damage sustained by each of the two buildings [WTC 1 and WTC 2] as a result of the terrorist attacks was massive. The fact that the structures were able to sustain this level of damage and remain standing for an extended period of time is remarkable and is the reason that most building occupants were able to evacuate safely. Events of this type, resulting in such substantial damage, are generally not considered in building design, and the ability of these structures to successfully withstand such damage is noteworthy.
>
> Preliminary analyses of the damaged structures, together with the fact the structures remained standing for an extended period of time, suggest that, absent other severe loading events such as a windstorm or earthquake, the buildings could have remained standing in their damaged states until subjected to some significant additional load. However, the structures were subjected to a second, simultaneous severe loading event in the form of the fires caused by the aircraft impacts.
>
> The large quantity of jet fuel carried by each aircraft ignited upon impact into each building. A significant portion of this fuel was consumed immediately in the ensuing fireballs. The remaining fuel is believed either to have flowed down through the buildings or to have burned off within a few minutes of the aircraft impact. The heat produced by this burning jet fuel does not by itself appear to have been sufficient to initiate the structural collapses. However, as the burning jet fuel spread across several floors of the buildings, it ignited much of the buildings' contents, causing simultaneous fires across several floors of both buildings. The heat output from these fires is estimated to have been comparable to the power produced by a large commercial power generating station. Over a period of many minutes, this heat induced additional stresses into the damaged structural frames while simultaneously softening and weakening these frames. This additional loading and the resulting damage were sufficient to induce the collapse of both structures.
>
> The ability of the two towers to withstand aircraft impacts without immediate collapse was a direct function of their design and construction characteristics, as was the vulnerability of the two towers to collapse a result of the combined effects of the impacts and ensuing fires. Many buildings with other design and construction characteristics would have been more vulnerable to collapse in these events than the two towers, and few may have been less vulnerable. It was not the purpose of this study to assess the code-conformance of the building design and construction, or to judge the adequacy of these features. However, during the course of this study, the structural and fire protection features of the buildings were examined. The study did not reveal any specific structural features that would be regarded as substandard, and, in fact, many structural and fire protection features of the design and construction were found to be superior to the minimum code requirements.
>
> Several building design features have been identified as key to the buildings' ability to remain standing as long as they did and to allow the evacuation of most building occupants. These included the following:
>
> - robustness and redundancy of the steel framing system
> - adequate egress stairways that were well marked and lighted
> - conscientious implementation of emergency exiting training programs for building tenants

Similarly, several design features have been identified that may have played a role in allowing the buildings to collapse in the manner that they did and in the inability of victims at and above the impact floors to safely exit. These features should not be regarded either as design deficiencies or as features that should be prohibited in future building codes. Rather, these are features that should be subjected to more detailed evaluation, in order to understand their contribution to the performance of these buildings and how they may perform in other buildings. These include the following:

- the type of steel floor truss system present in these buildings and their structural robustness and redundancy when compared with other structural systems
- use of impact-resistant enclosures around egress paths
- resistance of passive fire protection to blasts and impacts in buildings designed to provide resistance to such hazards
- grouping emergency egress stairways in the central building core, as opposed to dispersing them throughout the structure

WTC 5, WTC 7, 90 West Street, the Bankers Trust building, the Verizon building, and World Financial Center 3 were impacted by large debris from the collapsing towers and suffered structural damage, but arrested collapse to localized areas. The performance of these buildings demonstrates the inherent ability of redundant steel-framed structures to withstand extensive damage from earthquakes, blasts, and other extreme events without progressive collapse.

What Future Changes May Result from the World Trade Center's Destruction?

The ensuing years will reveal the total impact of this disaster on society and the world of skyscrapers. Some changes will be determined by the findings of the *World Trade Center Building Performance Study* and future studies that are planned. The following comments are from the *World Trade Center Building Performance Study* (FEMA, 2002, pp. ES-3–ES-4):

> During the course of this study, the question of whether building codes should be changed in some way to make future buildings more resistant to such attacks was frequently explored. Depending on the size of the aircraft, it may not be technically feasible to develop design provisions that would enable all structures to be designed and constructed to resist the effects of impacts by rapidly moving aircraft, and the ensuing fires, without collapse. In addition, the cost of constructing such structures might be so large as to make this type of design intent practically infeasible.
>
> Although the attacks on the World Trade Center are a reason to question design philosophies, the BPS Team believes there are insufficient data to determine whether there is a reasonable threat of attacks on specific buildings to recommend inclusion of such requirements in building codes. Some believe the likelihood of such attacks on any specific building is deemed sufficiently low to not be considered at all. However, individual building developers may wish to consider design provisions for improving redundancy and robustness for such unforeseen events, particularly for structures that, by nature of their design or occupancy, may be especially susceptible to such incidents. Although some conceptual changes to the building codes that could make buildings more resistant to fire or impact damage or more conducive to occupant egress were identified in the course of this

study, the BPS Team felt that extensive technical, policy, and economic study of these concepts should be performed before any specific code change recommendations are developed. This report specifically recommends such additional studies. Future building code revisions may be considered after the technical details of the collapses and other building responses to damage are better understood.

The debris from the collapses of the WTC towers also initiated fires in surrounding buildings, including WTC 4, 5, 6, and 7; 90 West Street; and 130 Cedar Street. Many of the buildings suffered severe fire damage but remained standing. However, two steel-framed structures experienced fire-induced collapse. WTC 7 collapsed completely after burning unchecked for approximately 7 hours, and a partial collapse occurred in an interior section of WTC 5. Studies of WTC 7 indicate that the collapse began in the lower stories, either through failure of major load transfer members located above an electrical substation structure or in columns in the stories above the transfer structure. The collapse of WTC 7 caused damage to the Verizon building and 30 West Broadway. The partial collapse of WTC 5 was not initiated by debris and is possibly a result of fire-induced connection failures. The collapse of these structures is particularly significant in that, prior to these events, no protected steel-frame structure, the most common form of large commercial construction in the United States, had ever experienced a fire-induced collapse. Thus, these events may highlight new building vulnerabilities, not previously believed to exist.

Recommendations for Buildings Being Evaluated for Extreme Events[*]

In the study of the WTC towers and the surrounding buildings that were subsequently damaged by falling debris and fire, several issues were found to be critical to the observed building performance in one or more buildings. These issues fall into several broad topics that should be considered for buildings that are being evaluated or designed for extreme events. It may be that some of these issues should be considered for all buildings; however, additional studies are required before general recommendations, if any, can be made for all buildings. The issues identified from this study of damaged buildings in or near the WTC site have been summarized into the following points:

a) Structural framing systems need redundancy and/or robustness, so that alternative paths or additional capacity are available for transmitting loads when building damage occurs.
b) Fireproofing[†] needs to adhere under impact and fire conditions that deform steel members, so that the coatings remain on the steel and provide the intended protection.

[*]These recommendations are extracted directly from the *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations,* FEMA 403, Executive Summary, pp. 4–7 (Washington, DC, May 2002).

[†]There has been speculation that the spray-applied fire proofing on the WTC steel columns and trusses had been previously damaged due to wind or was dislodged as a result of the impact of the aircraft. ‘‘The fire performance of steel trusses with spray-applied fire protection, and with end

> One oft-mentioned issue is whether a separate, more rigorous set of codes and standards should apply to extremely tall buildings. . . . Robert Solomon of the National Fire Protection Association (NFPA) is one of the experts who recommends that architects and engineers consider categorizing high rises by height and perhaps tailor requirements accordingly. For example, 7- to 40-story buildings might be labeled ''tall buildings,'' buildings with 41 to 90 floors could be deemed ''high rises,'' and those 91 floors or more could be referred to as ''supertall'' structures.
>
> There is a recent precedent for code provisions to vary in high rises by building height. Recently, the NFPA adopted a change requiring that all buildings taller than 420 feet (roughly 40 stories) increase their fireproofing for structural members. Over the past 25 or so years, says Solomon, buildings over 40 stories required ''three-hour construction,'' meaning that structural members would have to be protected by fireproofing that lasted at least three hours. The change will bump that standard up to four hours. (Gips, September 2002, p. 48)

c) Connection performance under impact loads and during fire loads needs to be analytically understood and quantified for improved design capabilities and performance as critical components in structural frames.
d) Fire protection ratings that include the use of sprinklers in buildings require a reliable and redundant water supply. If the water supply is interrupted, the assumed fire protection is greatly reduced.
e) Egress systems currently in use should be evaluated for redundancy and robustness in providing egress when building damage occurs, including the issues of transfer floors, stair spacing and locations, and stairwell enclosure impact resistance.
f) Fire protection ratings and safety factors for structural transfer systems should be evaluated for their adequacy relative to the role of transfer systems in building stability.

The BPS Team has developed recommendations for specific issues, based on the study of the performance of the WTC towers and surrounding buildings in response to the impact and fire damage that occurred. These recommendations have a broader scope than the important issue of building concepts and design for mitigating damage from terrorist attacks, and also address the level at which resources should be expended for aircraft security, how the fire protection and structural engineering communities should increase their interaction in building design and construction, possible considerations for improved egress in damaged structures, the public understanding of typical building design capacities, issues related to the study process and future activities, and issues for communities to consider when they are developing emergency response plans that include engineering response.

---

restraint conditions similar to those present in the two towers, is not well understood, but is likely critical to the building collapse. Studies of the fire-performance of this structural system should be conducted. Observation of the debris generated by the collapse of the towers and of damaged adjacent structures suggests that spray-applied fireproofing may be vulnerable to mechanical damage from blasts and impacts. This vulnerability is not well understood. Tests of these materials should be conducted to understand how well they withstand such mechanical damage and to determine whether it is appropriate and feasible to improve their resistance to such damage'' (FEMA, 2002, p. 2-39).

[Regarding one of these aspects,] building evacuation, the following topics were not explicitly examined during this study, but are recognized as important aspects of designing buildings for impact and fire events. Recommendations for further study are to:

- Perform an analysis of occupant behavior during evacuation of the buildings at WTC to improve the design of fire alarm and egress systems* in high-rise buildings.
- Perform an analysis of the design basis of evacuation systems in high-rise buildings to assess the adequacy of the current design practice, which relies on phased evacuation.
- Evaluate the use of elevators† as part of the means of egress for mobility-impaired people as well as the general building population for the evacuation of high-rise buildings. In addition, the use of elevators for access by emergency personnel‡ needs to be evaluated.

[Regarding another of these aspects,] education of stakeholders (e.g., owners, operators, tenants, authorities, designers), [they] should be further educated about building codes, the minimum design loads typically addressed for building design, and the extreme events that are not addressed by building codes. Should stakeholders desire to address events not included in the building codes, they should understand the process of developing and implementing strategies to mitigate damage from extreme events.

Stakeholders should also be educated about the expected performance of their building when renovations, or changes in use or occupancy, occur and the building is subjected to different floor or fire loads. For instance, if the occupancy in a building changes to one with a higher fire hazard, stakeholders should have the fire protection systems reviewed to ensure there is adequate fire protection. Or, if the structural load is increased with a new occupancy, the structural support system should be reviewed to ensure it can carry the new load.

What Future Studies are Planned?

There are several future studies planned or already underway by the National Institute of Standards and Technology, the National Science Foundation, and the Council on Tall Buildings and Urban Habitat.

---

*''A code change relating to the width of stairwells is already in the works at the NFPA, though not because of 9-11, according to the NFPA's Solomon. Stairwells that must accommodate more than 2,000 occupants will soon be required to have 48 inches of width, up from the current 44'' (Gips, September 2002, p. 52).

†For some years this issue has been a major concern of fire protection professionals. Commenting on this subject, Charles Jennings, MS, MRP, of John Jay College stated that, ''The latest and most advanced thought is now devoted to developing pressurization requirements for elevator shafts and lobbies. The objective of these current efforts is to make elevators a useful component of the building evacuation system during a fire'' (1995, p. 291).

‡''Because of tragic 9/11 stories of doomed firefighters overburdened with gear and out of radio contact, Chicago and other cities are reviewing emergency communications and requiring or recommending that skyscrapers install lockers or closets with hoses, axes and oxygen tanks on upper floors so firefighters don't have to carry them'' (''High-rises remain vulnerable after 9/11,'' September 25, 2002, p. 3A).

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) will conduct a study of the World Trade Center. It is anticipated that this investigation will incorporate information from the *World Trade Center Building Performance Study.* The results of the study are expected to be available in 2004. According to Weiger and Nicholson (2002, p. 102),

> NIST Director Arden L. Bement, Jr., stated that ''The NIST study will focus on the Twin Towers, not only because their collapse triggered the damage done to the surrounding structures, but also because many of the towers' design features are still used by the construction industry. The NIST study will try to determine what measures are needed to give buildings the strength to resist abnormal loads, such as the impact of an airplane and an ensuing fire. Researchers will also study the effectiveness of fire protection and firefighting technologies and practices for tall buildings''. . . .
>
> While the NIST-led national building and fire safety investigation of the World Trade Center is being conducted, short-term and interim projects will be undertaken to provide facility owners, contractors, designers, and emergency personnel with guidance, tools, and technical assistance to prepare them better for future disasters. . . .
>
> The short-term studies NIST is undertaking will focus on fire, the buildings' progressive collapse, and threats to commercial and institutional buildings and facilities . . .
>
> Interim NIST studies will also examine progressive collapse, which refers to the spread of failure by a chain reaction that's disproportionate to the triggering event. According to Bement, current U.S. standards, codes, and practices don't address this type of collapse.
>
> Finally, NIST will investigate ways of reducing the vulnerability of commercial and institutional buildings to chemical, biological, and radiological attack.

National Science Foundation

Within weeks of the terrorist attacks, the National Science Foundation (NSF) provided grants for post-disaster studies. One grant was to Frederick Mowrer, associate professor in the Department of Fire Protection Engineering at the University of Maryland. ''Within the next year, Mowrer plans to compare the WTC incident to two other multi-floor burnouts in high-rise buildings, the 1988 First Interstate Bank building fire in Los Angeles, California, and the 1991 fire at One Meridian Plaza in Philadelphia, Pennsylvania. Neither of these buildings[*] collapsed, despite fire on multiple floors'' (Weiger and Nicholson, 2002, p. 103).

Council on Tall Buildings and Urban Habitat

The Council on Tall Buildings and Urban Habitat (CTBUH) has formed a task force consisting of leaders in architecture, engineering, building security, and fire protection to explore options ''to further increase the level of safety in tall

[*]Both the First Interstate Bank Building and the One Meridian Plaza fires are discussed earlier in this chapter.

buildings including the establishment of guidelines to better educate building management on safety procedures and decision-making and communication during an emergency'' (CTBUH, 2001, p. 1).

How to Prepare a Building for an Aircraft Collision*

In 1991 the 62-story John Hancock Tower in Boston, Massachusetts, conducted an emergency preparedness exercise to organize the response of building and emergency forces to a scenario of a small aircraft losing control and crashing into the 54th floor of this high-rise office building. In designing the scenario, the point of impact was stipulated and the number of occupants killed and injured was specified, including the actual locations of injured persons. As detailed in the *NFPA Journal* (Johnson and Matthews, 1993, p. 36),

> John Hancock's overall objectives for this drill were to exercise and evaluate its communications and incident command systems and to observe how its unified command interfaced with that of outside emergency forces. . . . When developing its preparedness plan, the company brought together all the agencies that would play a major role in mitigating such an incident in a well-planned test of their emergency response effectiveness. In addition to John Hancock's emergency preparedness organization, the participants included the Boston Fire Department, Boston Emergency Medical Services, the Boston Police Department, and the American Red Cross, which were prestaged. Area hospitals also participated to test their own disaster plans.
>
> It is important to point out that the exercise was to be a tool for learning, and there were to be no surprises. The scenario was fully disclosed at the planning meetings, and each participating agency was encouraged to develop its own response to the simulated emergency.
>
> Although the disaster was simulated, the participants postulated the many ways in which this type of aircraft accident would affect the tower and its building systems.

John Hancock's planning and preparation took 11 months and included members of the building's emergency preparedness organization as well as outside agencies. Topics covered included ''safety, communications, elevator use, site security, property preservation during the drill, public relations, observers of the exercise, and most important, the roles and responsibilities of the participating organizations. John Hancock hired a consultant who specialized in emergency preparedness and response training and development to help plan the drill'' (Johnson and Matthews, 1993, p. 37). This planning culminated in a 2½-hour exercise that was conducted with observers documenting and evaluating errors or omissions by the building's emergency preparedness organization. Evaluation meetings were held after the exercise to learn lessons from the event and make needed corrections to emergency response procedures.

---

*Information in this section was obtained from ''Disaster Plan Simulates Plane Crash into High-Rise Building'' by William H. Johnson and Warren R. Matthews (*NFPA Journal*, November/December 1993).

Natural Disasters

Each natural disaster (earthquake, tsunami, volcano, winter storm, tornado, hurricane, or flood) requires a separate life safety approach and should be independently covered in the Building Emergency Procedures Manual (see Chapter 11).

Earthquakes

> The foundations of the earth shake.
> The earth is broken asunder,
> The earth is split through,
> The earth is shaken violently.
> —Isaiah 24:18–19

During the time that high-rise buildings have been in existence in the United States, it is primarily the West Coast and Alaska that have been subjected to numerous earthquakes ranging from an almost indiscernible tremble of the ground to the violent shaking of a major quake. This shaking is sometimes side-to-side and other times up-and-down; it can last for a few seconds or for several minutes.

A map indicating where earthquakes have occurred in the United States shows that only a few areas are considered low-risk for quakes (Figure 10.15).

The reason that California, particularly, is such an active earthquake zone is that it lies on the boundary—marked by the infamous 800-mile-long San Andreas Fault—between two tectonic plates, the Pacific and the North American Plates. These two gigantic sections of the earth's crust float above a very thick layer of hot rocks called the mantle, which in turn floats atop the earth's core of molten rock. The Pacific Plate, to which Los Angeles is attached, is gradually inching its way north and west, past the North American Plate to its east, which is moving in the opposite direction. At most points, and at most times, these two plates obstruct each other's advancement, resulting in the buildup of intense pressure. An earthquake will occur at certain times when the blockage at a specific point along the fault line releases (faults are fractures in the earth's crust), the plates slide past one another, and the ground suddenly shifts. When earthquakes occur, the strength and duration of the shaking largely determines the potential for damage. Some earthquakes are preceded by smaller quakes called foreshocks, some occur suddenly with no forewarning, some occur in groups of approximately the same magnitude (called swarms or clusters), and some are followed by smaller quakes called aftershocks. Earthquake strength, or magnitude, can be measured on the Richter scale—a logarithmic scale of increasing magnitude from 1 to 10 that was developed in 1935. ''Scientists prefer to describe earthquakes greater than 7.0 on the moment magnitude scale. The moment magnitude scale measures more of the ground movements produced by an earthquake. Thus, it describes large earthquakes more accurately than does the Richter scale'' (McNally, 2002, p. 6).

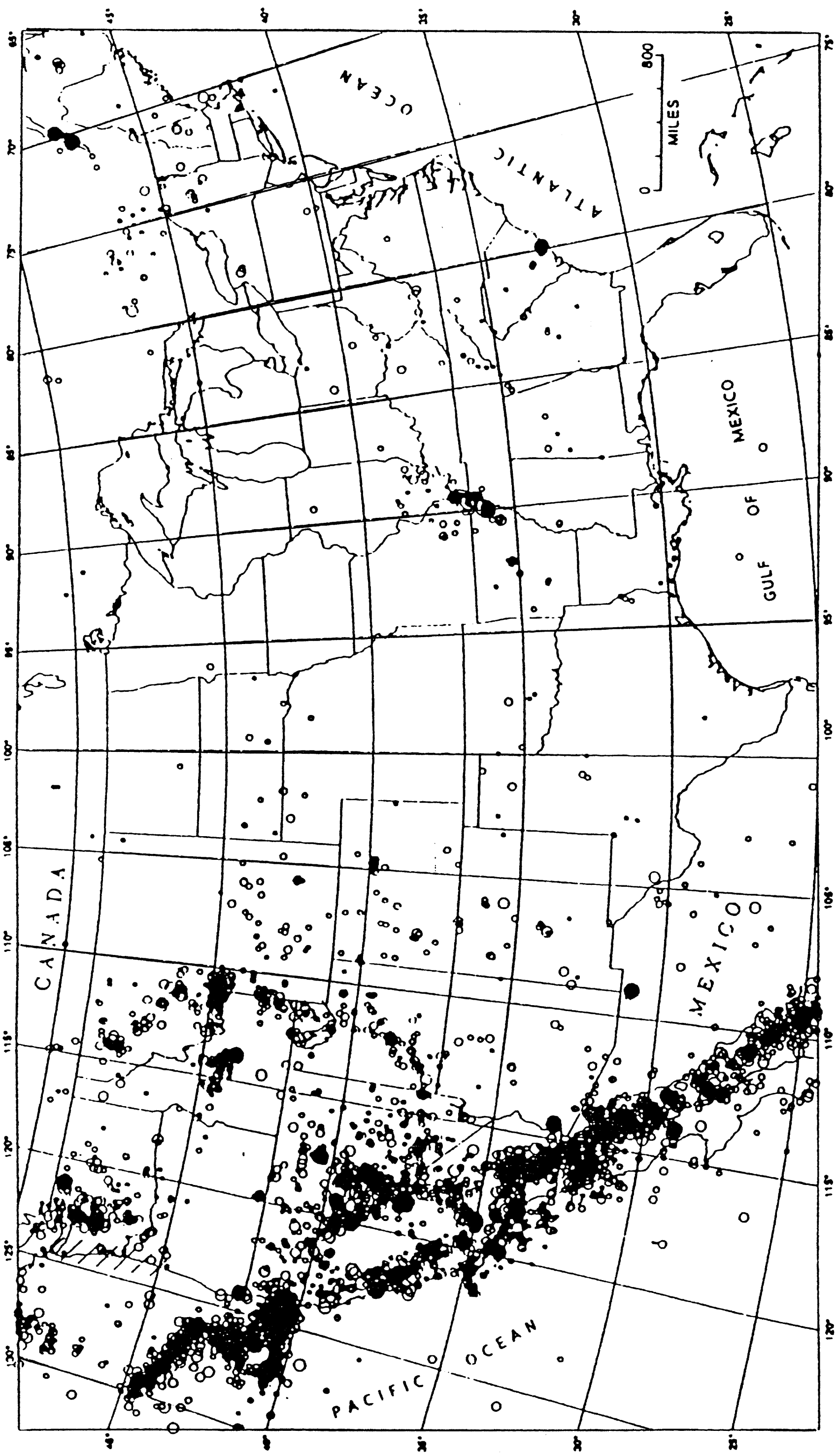


Figure 10.15 Earthquakes occur throughout the United States. Courtesy of U.S. Geological Survey (National Earthquake Information Center, Denver, CO, 1990).

Earthquake Preparedness

Earthquake preparedness can be approached in three distinct phases—before, during, and after the earthquake.

Before the Earthquake

Modern high-rise buildings in areas subject to earthquake activity have been constructed in accordance with strict building codes. Older buildings erected before seismic design considerations were mandated may be required to perform structural retrofits to bring the structures up to code.

The effect of earthquakes on a high-rise building depends on factors such as the building's location in relation to the quake's epicenter, type of soil or rock beneath the structure, magnitude of the quake, duration of the shaking, type of motion the structure is subjected to, and the building's design and quality of construction. The shaking of an earthquake may cause no structural damage, or it may cause destruction so severe that the building collapses. In areas like California, modern high-rise buildings are seismically designed to withstand certain magnitude earthquakes. ''The idea of earthquake-proof construction is unrealistic, unless exceptionally expensive measures are taken. Any building will collapse if the ground under it shakes hard enough or becomes permanently deformed. But structures can be designed and constructed to incorporate a high degree of earthquake resistance'' (Kimball, 1988, p. 42).

As Dames and Moore/URS Corporation (1994) explain, ''To resist seismic forces, steel buildings are either constructed with braced frames (such as X-bracing) or moment frames (rigid beam-column assembly)'' (p. 21). Many structures, particularly seismically designed steel-framed buildings, have been constructed to flex and move without breaking. Lower floors may shake more rapidly, but movement of the building from side to side is greatest on uppermost floors. ''To dissipate the force of the ground shaking through a tall structure, the building is designed to sway[*] as a unit in a side-to-side motion'' (Kimball, 1988, p. 106).

Northridge Earthquake

> *January 17, 1994, Northridge, California*—At 4:31 AM an earthquake of magnitude 6.7 rocked the heavily populated San Fernando Valley. It severely impaired the public transportation network and residential community; 72 people were killed and 11,846 people were treated for earthquake-related injuries: ''30 of the 72 Northridge deaths were attributed to heart attacks'' (Reich, 1995, p. A1). Thousands were left homeless in the wake of this disaster that had an insured loss of $12,500,000,000.[†]

[*]Most high-rise buildings are designed to sway in a gentle wind but not so much that occupants on upper floors experience motion sickness. The object is to ''make [the building] stiff enough that people wouldn't get sick, but not so rigid that it could snap if it got too big a load. . . . Big buildings are designed to be stiff enough that the period to go one way and back the other way is 15 to 20 seconds, or even 30 seconds'' (Eagar, 2002, pp. 2, 3).

[†]Insured loss provided by the Insurance Information Institute, ''Insurance Issues Update,'' August 1998, as stated in *Risk Analysis and the Security Survey*, 2nd ed., by James F. Broder (Butterworth-Heinemann, 2000, p. xi).

The January 17, 1994, Northridge earthquake raised some serious safety concerns about the degree of earthquake resistance that high-rise buildings, in particular steel moment frame structures, afford. Unlike braced frames, these moment frames feature larger beams and columns, with additional welding or bolting of the connections. Before this earthquake, this structural system was thought to be among the safest seismically. As John Hall (1994, pp. 1, 2), an associate professor of civil engineering at the California Institute of Technology, points out:

> During the 1994 Northridge earthquake, many modern steel buildings suffered unexpected fractures in welded beam-to-column connections. Although none of these buildings collapsed, fractured connections are a serious matter since they reduce the lateral strength of the structure, and, thereby, increase the risk of collapse. The problem is apparently widespread and, at this point, one must assume that any welded steel moment-frame is susceptible to this type of connection failure.

The following comments regarding this situation were written shortly after the quake in *The Northridge Earthquake, January 17, 1994, A Special Report* by Dames and Moore/URS Corporation (1994, p. 21):

> Steel moment frame buildings have generally been considered very effective in resisting seismic forces. However, the high intensity of the Northridge earthquake pushed even steel moment frame buildings to their seismic limits, causing damage not experienced before. More than 50 relatively new 2- to 10-story structures that sustained brittle structural damage have been identified at the time of writing this report. Such damage raises troubling questions about the seismic resistance of this type of construction. Damage took the form of cracks in welds and rupture of steel sections at connections of beams to columns and columns to the base plate—both areas are critical for stability of the structure. Steel-framed buildings are designed to absorb energy by bending without breaking. However, the failure of welded connections would not allow the level of bending assumed in design and can cause brittle failures. Steel members in existing buildings are covered with fireproofing and are not readily available for inspection. Thus, damage caused by the quake may go unnoticed unless a detailed and costly inspection program is undertaken. The damage to steel moment frame buildings has potentially the highest structural significance of the Northridge earthquake and will probably result in substantial research and associated design code changes.

After this disaster, the City of Los Angeles by ordinance required that owners of steel moment frame buildings inspect for damage, and FEMA subsequently prepared guidelines to address this potential hazard.

Even though issues about weld cracks in steel-framed construction were the most startling results of the quake, the failures of concrete-framed parking structures were among the most dramatic (Figure 10.16). As the *Engineering News Record* (January 16, 1995, pp. 28–33) reported, ''In response to such collapses, federal officials anticipate a new treatment of parking structures in the National Earthquake Hazard Reduction Program's 1997 provisions, to serve as a basis for model codes.''

During a severe earthquake, occupants and building contents will be shaken. Items not properly secured may fall; desks and furniture may slide; filing cabinets and bookcases may topple; ceiling tiles may be dislodged;

Figure 10.16 TOTAL DESTRUCTION. Severe shaking during the 1994 Northridge earthquake led to the collapse of this recently constructed, precast four-level concrete parking structure at California State University. Courtesy of Los Angeles Fire Department, Disaster Preparedness Division.

windows may crack or shatter; sprinkler heads may shear off and result in water discharge; seismic devices may cause building elevators to go to the nearest floor in the direction of travel, stop, automatically open elevator car doors, and then cease operation; the automatic fire detection and reporting equipment may produce multiple false alarms; electrical power may be disrupted; lights may go off; the telephone system may be damaged, or shortly after the shaking has stopped, be deluged with calls. Falling objects will often cause injuries (Figure 10.17).

Therefore, in earthquake-prone areas it is wise to anchor computer systems, attach unsecured bookcases and cabinets to walls, and place objects that may break close to the floor or in cabinets with latching doors. Do not store heavy objects on top of cabinets, credenzas, and bookcases, or place chairs with rollers close to floor-to-ceiling windows. The last precaution was the subject of a story once told by an emergency planner who worked in San Francisco.

> The individual was visiting his boss on the 50th floor of a major high-rise. The boss was sitting on a chair with recently lubricated rollers when suddenly a

Figure 10.17 During the 1994 Northridge earthquake these tall, caster-mounted computer cabinets rolled across the floor of a second-story room without overturning. Unfortunately, the newly installed ceiling and lighting fixtures did not fare as well. Courtesy of Dames and Moore/URS Corporation, *A Special Report on the January 17, 1994, Northridge Earthquake*.

severe earthquake hit. The building swayed so violently that the boss started rolling rapidly toward the nearby window. The subordinate reached out and caught the chair before it went crashing into the window. The emergency planner said that this incident certainly did not hurt his career!

Occupants should also identify safe areas in their office where they may take shelter if an earthquake hits; store items such as a flashlight, portable radio, extra batteries, walking shoes, food items, necessary medications, contact lens solution, and so on in a desk drawer; know ahead of time the location of emergency exits and stairwells; and have out-of-state telephone numbers for contacting family members. In a severe earthquake, regular telephone service may be disrupted. Public pay telephones often are the first services to be restored and can be used by family members to dial out-of-state and leave messages for each other.

Building management or individual tenants also may provide occupants with earthquake preparedness supplies, including bottled water, canned and dry food, first aid kits, sleeping bags, and other items detailed in the ‘‘Emergency Operations Center (EOC)’’ section in Chapter 11. All perishable items should be replaced every 6 months, or as needed, to ensure quality.

If a major earthquake occurs, occupants may have to remain in their building for several days because of the disruption of public transportation and communication systems or widespread damage in the community.

In California, emergency planners predict that after a severe earthquake, such as the magnitude 8.0 predicted along the San Andreas Fault, occupants may be without the assistance of outside emergency services for 72 hours or more.

During the Earthquake

An earthquake usually occurs without any warning other than possibly a roaring sound like a fast-approaching locomotive or airplane. Thus occupants and building staff alike have only a few moments to act. During an earthquake, most actions of those inside a high-rise building are geared toward self-preservation, particularly on upper floors where the swaying may be the most extreme. The following are basic guidelines for these moments:

- Do not panic (easier said than done).
- If on an upper floor, do not attempt to rush for stairwells. If on the ground or street level, do not run outside. Occupants running out of high-rise buildings may be hit by falling glass and other materials or by vehicles. If outside the building, do not attempt to re-enter the building but move, if possible, to an open area that is a safe distance away from the building, utility poles, fallen electrical power lines, street light fixtures, trees, and objects that may be a hazard.
- If inside an elevator, remember that in earthquake-susceptible areas most building elevators are equipped with the seismic devices described in the previous section on ''Elevator Malfunctions and Entrapments,'' which will take you to the nearest floor in the direction you were traveling, stop, and automatically open the doors. If the elevator stalls, do not attempt to force open the doors. Summon assistance by pushing the EMERGENCY CALL, EMERGENCY ALARM, or EMERGENCY ONLY button on the elevator car's floor selection panel. Then carry out the instructions of responding staff. Remember that power failures are commonly associated with severe earthquakes, and there may be some delay in freeing all passengers trapped in building elevators.
- If inside an office area, move away from exterior glass windows, interior temporary or glass partitions, hanging objects, freestanding bookcases or cabinets, and other objects that may fall. Get under a strong table or desk and hold onto it—it may move during a severe shaker.
- If in crowded interior areas such as conference rooms or auditoriums, try to keep others calm and take the same actions as for an office area.
- If in building corridors or lobbies, move to an interior wall away from light fixtures, tuck your head to your knees, and cover your head with your arms to protect against falling objects such as ceiling tiles. Do not attempt to use elevators.
- If inside a restroom, remain there and cover your head with your arms to protect yourself from falling objects.
- If in the parking area and it is safe to remain, tuck your head to your knees, and cover your head with your arms. In a severe earthquake, there may be out-of-control vehicles.
- Stay in your protective position, unless it becomes unsafe to do so, until the shaking has ceased and it appears safe to move.

- Do not smoke or use a lighter or matches; if the building has gas lines, there may be leaks.

After the Earthquake

If the earthquake has caused damage, assist floor wardens and building emergency staff by checking for injured persons and providing assistance if you are trained to do so. If not, locate someone who is trained to assist. Do not attempt to move injured persons unless it is imperative or there is the risk of more severe injury occurring if they are not moved. If there are many injured occupants, it may be necessary to set up a triage (triage is the process of classifying victims according to medical treatment needs) and first aid area on each floor. There may be fatalities during a severe earthquake. One cause of death may be heart attacks suffered during such a traumatic event. Next, check your immediate area for damage and potential hazards if aftershocks should occur. Open doors cautiously because objects may fall. Check for telephone handsets that have been knocked off the hook. Use telephones for emergency communications only.

During this time, listen for announcements and instructions over the PA communication system if it is still operational. Follow the directions of building staff members, floor wardens, and responding public agencies. You could also listen to portable radios for public safety messages. Do not pass on anything to others that could be misinformation. Remain on your floor and do not use elevators until you are authorized to do so. Above all, *be prepared for aftershocks*. Depending on the severity of the event, building management will notify occupants if it is safe to return to work, if evacuation of the building or relocation within the building is required, or if occupants are to remain on their floor and await further instructions.

Soil liquefaction, landslides, and fires are common results of major earthquakes. *Liquefaction* occurs in areas where loose soils with a high water table are present. ''As the earthquake causes water to percolate up through the loose soil, it creates quicksand. Heavy objects such as buildings and other structures may sink or tilt into the liquefied soil'' (Kimball, 1988, pp. 17–18). Fires can result from fuel spillage, rupturing of gas lines, and the many ignition sources available in urban areas. If the earthquake is a major one, public fire fighting capabilities will be severely strained because of extraordinary demands for service, difficulties in transporting equipment along damaged or blocked roadways and freeways, and possible disruption of the public water supply.

An earthquake may cause such serious damage to a building that for a time tenants cannot enter it at all, or can enter only under certain conditions. The building should be secured and a recorded message informing tenants of the situation placed on building management's voice-mail system or on a special toll-free number. Tenants should be aware that such communications are provided for them to obtain information about building operations, particularly during emergency situations.

Tsunamis

In coastal areas, vertical motion of the seabed—which could be caused by an earthquake—may result in a tsunami or tidal wave. On July 17, 1998, Papua New Guinea suffered a massive tsunami that caused the death of some 2000 people.* Japan has a history of tsunamis following major earthquakes; its government has developed a tsunami warning system similar to the U.S. Emergency Broadcast System, which broadcasts warnings over television and radio networks.

Tsunamis can occur at any point along the U.S. coastline and lead to waves over 50-foot high pounding the shores. ''The most destructive tsunamis have occurred along the coasts of California, Oregon, Washington, Alaska, and Hawaii'' (BOMA, 1994, p. 66).

If a tsunami warning is issued, television and radio networks should be monitored for information and instructions. If the building owner or manager deems it necessary to evacuate the building, it should be accomplished in an orderly fashion. Building elevators should be used, starting first with upper floors in each elevator bank.

Volcanoes

A *volcano* is defined as ''an opening in the earth's crust through which steam, gases, ashes, rocks, and frequently streams of molten material are or have been periodically ejected'' (*Reader's Digest*, 1979). If a volcano erupts and the volcanic ash travels to a high-rise building, all external doors should be kept closed and the HVAC system should be shut down, or outside air intakes closed off, to avoid contamination within the building. Occupants should be instructed to stay within the building while the ash is falling. Such an event is unlikely in the United States, but nonetheless possible, because there are active volcanoes in the Pacific Northwest, Alaska, and Hawaii.

Winter Storms

There are many types of storms (freezing rain, sleet, hail, snowstorms, and blizzards) that may occur between autumn and spring. Depending on their severity, storms may hamper public transportation, cause power failures, and freeze building equipment. Critical high-rise building systems should be closely monitored, particularly equipment that is subject to freezing and is located in unheated areas or areas that during a power failure would no longer be heated. Building staff also should be alert to the condition of exterior areas to ensure that pathways for building occupants and visitors are safe to use.

All building occupants should be kept informed, possibly by way of the building PA system, about the development of severe weather conditions that may affect their departure from the building. They should be advised to heed storm warnings issued by the National Weather Service (NWS). The NWS is a

*As reported in the *Los Angeles Times* (''Official death toll of tsunami at 2000,'' July 28, 1998, p. A4).

public service agency that aims to protect life and property from natural disasters such as flash floods, tornadoes, and severe thunderstorms. It is made up of a network of Weather Service Forecast Offices (WSFOs) and Weather Service Offices (WSOs).

Tornadoes

Tornadoes ''can occur in all fifty states, but the Midwest and Southeast parts of the country are the most vulnerable. Tornadoes can also strike at any time of the year, but occur most frequently during April, May, and June'' (BOMA, 1994, p. 66). A *tornado* is defined as ''a violent storm, usually with heavy rain, in which wind rotates or constantly changes direction, especially in the Mississippi region of the United States'' (*Reader's Digest*, 1979). A tornado is usually characterized by a funnel-shaped waterspout.

> *March 28, 2000, Fort Worth, Texas*—A tornado that killed four people and injured at least 36 others raced through downtown Fort Worth. The twister overturned vehicles, uprooted trees and shattered windows in high-rise buildings, causing evacuation of one 35-story structure.*

If a threat of tornadoes is reported, tornado watch or tornado warning advisories may be issued by the NWS. A *tornado watch* means that tornadoes are possible; a *tornado warning* means that tornadoes actually have been sighted in the area.

Tornado Preparedness

Tornado preparedness, like that for earthquakes, can be approached in three distinct phases—before, during, and after the event. The following preventive measures were developed using *Before Disaster Strikes: Developing an Emergency Procedures Manual* by the Institute of Real Estate Management (IREM) as a resource.

Before the Tornado

National Weather Service advisories regarding the tornado should be monitored not only by tenants and their employees, but by building management, which may communicate updates of the situation over the building PA system or by telephone calls to office managers or other key tenant representatives. Preparations for the possibility of an incoming tornado may include the following:

- Ensure that workers on outside building scaffolding and window washing appliances immediately stop work, secure their equipment if there is time, and take shelter inside the building.
- Secure or move outdoor objects such as trash containers, dumpsters, planters, signs, furniture, and vehicles that may blow away or cause damage to people or property.

*As reported in the *Los Angeles Times* (''Tornado rips downtown Fort Worth,'' March 29, 2000, p. A18).

- Prune trees of branches that may cause damage to the building, if time allows.
- Have occupants clear all objects from desks and working areas. All exposed paperwork should be stored in closed cabinets and other containers. Valuable equipment and documents should be moved from outer offices to interior rooms.
- To protect them from possible power surges, all office equipment, including computers, and appliances should be switched off and unplugged.
- All doors should be closed.
- Curtains and blinds should be shut.
- Personal possessions should be made ready in case of evacuation.
- Food, bottled water, and other supplies should be made ready in case they are needed.

The extent of preparation will depend on the time of day and day of the week that warning of the impending tornado is received. For example, if the warning is received after normal business hours when the majority of tenants have left the building, preparations within tenant space may not be possible or may be carried out on a restricted basis only. The extent of preparation also may be impacted by the behavior of the tornado. For example, if there is an abrupt change in the direction of the storm, preparatory actions may be curtailed substantially. Depending on the expected nature of the tornado, building management may have engineering or janitorial staff board up or tape building windows, glass doors, and shop fronts on lower levels to reduce the possibility of pieces of broken glass becoming deadly missiles. Building engineering and security may be assigned to lock off building elevators at a level that is considered safe, or shut down HVAC systems and certain lighting. Walkthroughs of the building may be conducted (perhaps by floor wardens) to ensure that appropriate precautions are underway. It may be necessary to advise occupants to evacuate the building or relocate to lower levels, including subterranean parking or under-building garages. If the building is evacuated, certain members of the building staff (usually engineering and security personnel) will often remain behind.

During the Tornado

Most actions of those inside a high-rise building are geared toward self-preservation during a tornado. The following are basic guidelines for this time:

- Do not panic.
- Seek cover in interior areas or designated shelter areas. Interior areas may include building corridors that are well away from exterior glass windows, interior temporary or glass partitions, hanging objects, freestanding bookcases or cabinets, or other objects that may fall. Depending on the severity of the tornado, protect your head and face with your arms and get under a strong table or desk or shelter in areas such as interior offices or restrooms.
- Stay in your protective position, unless it becomes unsafe to do so, until it appears safe to move.

- Do not attempt to use elevators because power may fail and passengers may become trapped.
- Do not attempt to leave the building.

After the Tornado

If there has been damage caused by the tornado, you can be most helpful by assisting building staff in the same ways as you would after an earthquake. Damage caused by a tornado may also cause disruptions to building operations similar to the situation following an earthquake. (See ''After the Earthquake'' section earlier in this chapter.) The damage may not be finished either: In coastal areas, a tornado can be the forerunner of a hurricane.

Hurricanes

''Every Atlantic and Gulf coast area of the United States as well as the coastal areas of Hawaii and the Caribbean islands are threatened by hurricanes. Hurricane season extends from the beginning of June through November'' (BOMA, 1994, p. 67). A *hurricane*, which is also referred to as a *typhoon*, is defined as ''a violent windstorm . . . with air moving rapidly (up to 130 m.p.h.) around a central calm space, which with the whole system advances in a straight or curved track. Wind of 73 M.P.H. or more (force of 12 in the Beaufort Scale)'' (*Reader's Digest*, 1979). In addition to high winds, heavy rains characterize hurricanes. Although the winds can cause serious damage, the majority of damage is a result of flooding during and after the hurricane. Remember when weathering this type of storm that it has a central eye. When the hurricane passes over an area, the winds and rains will abate for a time that may vary from a few minutes to half an hour or more. After this eye has passed, the storm will return, with the full fury of its winds now gusting in the opposite direction. Hurricanes also may lead to the development of tornadoes.

> *1960, New York City*—''During Hurricane Donna, occupants of high-rise buildings were justifiably frightened when large glass panels of the curtain walls were blown into their offices by the wind pressure. They were probably even more frightened and amazed when the leeward wind action sucked the window panels out of their offices. These leeward panels fell into the street, creating an additional hazard to passersby. . . . The total wind force is the sum of the windward pressure and the leeward suction, but each of these two forces has its own local effects'' (Salvadori, 1980, pp. 50, 51).

> *August 24, 1992, South Florida*—In the predawn hours, Hurricane Andrew swept through southern Florida, leaving behind a 30-mile-wide swath of destruction. Houses and buildings were destroyed, thousands were left homeless, roads were blocked, telephone lines were downed, power failures occurred, and insured loss was $15,500,000,000.*

*Insured loss provided by the Insurance Information Institute, ''Insurance Issues Update,'' August 1998, as stated in *Risk Analysis and the Security Survey*, 2nd ed., by James F. Broder (Butterworth–Heinemann, 2000, p. xi).

If there is a threat of this kind of storm, hurricane-watch or hurricane-warning advisories may be issued by the NWS. A *hurricane watch* means that hurricane conditions constitute a threat to a coastal area; a *hurricane warning* means that sustained winds of 74 mph or higher are expected within 24 hours in a specific coastal area.

Hurricane Preparedness

Preparing for hurricanes requires similar methods to those used in preparing for tornadoes, except that the flooding that often results from the heavy rains associated with them needs to be prepared for.

Before the Hurricane

National Weather Service advisories regarding the hurricane should be monitored in the same way as tornado advisories. Preparations for an incoming hurricane may include the following:

- Ensure that workers on outside building scaffolding and window washing appliances immediately stop work, secure equipment if there is time, and take shelter inside the building.
- Secure or move outdoor objects such as trash containers, dumpsters, planters, signs, furniture, and vehicles that may blow away or cause damage to people or property.
- Prune trees of branches that may cause damage to the building, if time allows.
- Have occupants clear all objects from desks and working areas. All exposed paperwork should be stored in closed cabinets and other containers. Valuable equipment and documents should be moved from outer offices to interior rooms. Heavy plastic can be used as a covering to lessen the chance of water damage.
- Valuable and water-sensitive equipment may be moved to upper levels to reduce the chance of damage by the flooding of lower levels.
- All doors should be closed.
- Curtains and blinds should be shut.
- To prepare for possible evacuation, personal possessions should be made ready.
- Food, bottled water, and other supplies should be made ready in case they are needed.
- Building management, engineering or security staff, or floor wardens may conduct walkthroughs of the building to ensure that appropriate precautions are being undertaken.

The extent of preparation will depend on whether the hurricane is predicted to occur during business hours. ''Because a hurricane's path is often tracked for days, there usually is time for preparation and preventive measures to be taken. At the minimum, a property manager should have at least one day's notice, inasmuch as hurricane watches will be upgraded to hurricane warnings when the hurricane is expected to strike an area within 24 hours'' (IREM 1990, p. 138).

Depending on the expected nature of the hurricane, building management may have engineering, security, and janitorial staffs take the following actions:

- Board up or tape building windows, glass doors, and shop fronts that are located on lower levels to reduce the possibility of pieces of broken glass becoming deadly missiles.
- Lock off building elevators at an upper level that is considered safe from possible flooding.
- Shut down building HVAC systems and certain lighting.
- Lay down sandbags if flooding is expected.
- Advise occupants to evacuate the building or relocate to lower levels of the building—but not subterranean areas, because of the potential for flooding. If the building is evacuated, certain members of the building staff (usually engineering and security personnel) will often remain behind.

During the Hurricane

During a hurricane, horizontal swaying of the top of a high-rise may be caused by strong winds. Salvadori (1980, p. 51) reports that:

> Under a strong wind the tops of the World Trade Center towers swing left and right of their vertical position by as much as three feet, and a hurricane can produce swings of six to seven feet on each side of the vertical. These horizontal swings are not structurally dangerous, but may be inconvenient for those who work at such great heights: occupants may become airsick.

Most actions of those inside a high-rise building are geared toward self-preservation during a hurricane. Follow the same basic guidelines as for during tornadoes.

After the Hurricane

If there has been damage caused by the hurricane, assist building staff in the same ways as you would after an earthquake. Damage caused by a hurricane also may cause disruptions to building operations similar to the situation following an earthquake. (See ''After the Earthquake'' section earlier in this chapter.)

High Winds and Cyclones

High winds or cyclones occur in certain areas. A *cyclone* is defined as, ''a system of winds rotating around a region of low barometric pressure (in the Northern hemisphere anti-clockwise, in the Southern hemisphere clockwise)'' (*Reader's Digest*, 1979). High winds and cyclones are handled in a similar manner to a hurricane, except that flooding is usually not an anticipated problem.

Floods

Torrential rain, melting snow, a tsunami, or a hurricane may produce too much water for land, rivers, and flood control channels to handle and therefore result in serious flooding that will impact an entire area, including high-rise buildings. Floods also can occur as a result of a public water main breaking or a reservoir failing.

February 10, 1992, Los Angeles—Within 2 hours, 8 inches of rain fell in the northwest portion of Los Angeles County and a torrent of rain entered the Los Angeles flood channel system. Storm water drains in several cities became clogged and could not handle the inundation of water. As a result, without warning, several subterranean parking facilities located beneath high-rise buildings became flooded with water up to 2 feet deep. Substantial damage was caused to elevator systems because of water cascading into elevator shafts. Vehicles also sustained water damage, and a substantial cleanup of affected areas was required. The loss of elevator service for several days caused considerable inconvenience to building tenants who were forced to use stairwells to reach their place of work.

April 13, 1992, Chicago—Floods of water inundated subterranean tunnels located beneath the downtown high-rise community. Almost 300 buildings were affected and many employees were unable to return to their place of work the next day. Some buildings reopened, but a massive cleanup of the impacted areas was required before business operations could fully return to normal.

If a *flash flood* occurs, there usually will not be time for a building to prepare for the deluge. The first priority should be to provide for the safety of building occupants and visitors. Then efforts should concentrate on alleviating damage to the building and its contents. If advance warning of the flood is received, certain preparations can be taken, as the Building Owners and Managers Association (1994, p. 64) explains:

> Building contents can be removed or relocated to floor levels above the predicted flood level. Electricity can be turned off in areas likely to be flooded. Pumps and hoses can be readied. Sandbags or other protective devices can be put in place based on anticipated flood depths. If deep flooding is predicted, it may be advisable to allow floodwaters to enter basement areas or even to flood the basement intentionally in advance of the flood waters. This can reduce potential structural damage by lowering the hydrostatic [liquid] pressure on basement walls. Similarly, buried storage tanks may be flooded with clean water to prevent them from being crushed or pushed out of the ground by hydrostatic pressure.

The building owner or manager can decide whether to evacuate building occupants, depending on the expected seriousness of the flood and its time of arrival.

Water Leaks

A water leak in a high-rise building can result in considerable damage to the structure and its contents. Leaks may be from a broken water pipe, a severed fire system sprinkler head, seepage through subterranean walls, overflow of a toilet receptacle, a backed-up sewer line, a blocked drain, failure of a sump pump, or a malfunctioning fountain. Someone deliberately leaving a water tap running in an area such as a public restroom also may cause it. The worst time for such an event to occur is after normal business operating hours when the number of building staff and occupants is greatly reduced, and when such a leak may go undetected for an extended time.

When a water leak is discovered, the first priority is to locate its source and attempt to shut off or control it as soon as possible. If there is difficulty in determining the exact location of the leak, it may be possible to shut down the entire system that is supplying water to the area. For safety reasons, electrical power to the affected area should be shut down or electrical equipment turned off. This should be done before attempting to resolve the problem if the electricity poses any danger. If possible, any building contents at risk of being damaged or subjected to further damage should be removed to a safe area or covered with plastic sheeting. Hand mopping or mechanical pumping can then be used to remove excess water. If not discovered quickly, serious water leaks—particularly those on upper floors of a high-rise—can have devastating effects. Water may drain down through multiple floors via stairwells, elevator shafts, and poke-through construction. This can lead to water in concealed ceiling spaces, soaked acoustical ceiling tiles that may fall from their own weight, water-soaked walls, and malfunction and possible failure of electrical systems if water comes in contact with them.

Jumpers, Protestors, and Daredevils

Because of their height, over the years that high-rises have been in existence there have been numerous people who have gone to a building's roof and, tragically, jumped over the side. (In the late 1990s, in a major Los Angeles downtown high-rise, a distraught businessman even used a chair to smash a window in his upper floor office and jump to his death.)

In addition, protestors have attempted to drape large banners promoting their raison d'être over the front of a building, and daredevils have used high-rises as their own personal stages to perform outlandish feats to gain attention or simply to prove that they can do it.

The way to stop jumpers and protestors from reaching a building's roof is to strictly control access to that area. Whether or not the door(s) leading to the roof can be locked depends on local city ordinances. Some jurisdictions permit it under special circumstances (such as requiring the door[s] to automatically unlock or fail-safe when a fire alarm occurs). If permitted, an intercom and CCTV camera, both constantly monitored in the Security Command Center, can be installed at the door. A person (other than those who carry a key or card to unlock the door) can request access via the intercom, and can be seen by the security staff via the camera. If the person is permitted to go onto the roof, the security staff can then remotely unlock the door.

Daring Acts

In the 1970s, the newly constructed Twin Towers of the New York World Trade Center were the scenes of three daring acts by a tightrope walker, a parachutist, and a climber. The following details of these incidents were obtained from *Twin Towers* by Angus Kress Gillespie (1999, pp. 141–146).

April 7, 1974, New York City—Starting at 7:15 AM, 24-year-old French tightrope walker, Philippe Petit, walked back and forth seven or eight times on a tightrope cable stretched between the roofs of the 1350-foot high Twin Towers. Three days before this heart-stopping display, Petit and three companions, all disguised as construction workers, used a freight elevator to transport cables and other equipment to the roof. On the night before the walk, they positioned themselves on each roof and used a 5-foot crossbow to shoot an arrow, with a nylon fishing line attached, across from the north to the south Tower. Using the line, they then strung across a 131-foot cable and secured it in place.

The next morning, Petit nonchalantly walked back and forth between the towers for nearly 75 minutes, stopping at times to sit down, lie down, and even hang from his feet. So many spectators gathered to watch that it caused a giant traffic jam on the streets below. Eventually, Petit was persuaded by a Port Authority police sergeant to come to the safety of the roof.

July 22, 1975, New York City—A skydiver parachuted from the north tower roof to the plaza 1350 feet below. *A New York Times* reporter, Lee Dembart, described how it was accomplished: ''With his white parachute concealed in a green bag, 34-year-old Owen J. Quinn, of 30–42 23rd Street, Astoria, eluded security guards on the 78th floor of the north tower, walked to the roof above the 110th floor, jumped off at 4:45 PM, and landed less than two minutes later on the raised ceremonial plaza between the buildings'' (Dembart, July 23, 1975). Apart from some cuts and bruises on his leg caused by the wind blowing him into the side of the building, he landed safely. Quinn, who said that he was trying to draw attention to the plight of the poor, was booked on charges of criminal trespass and reckless endangerment.

May 27, 1977, New York City—Starting at 6:30 AM, George W. Willig, a 27-year-old amateur mountain climber, using special equipment that he designed to fit the window-washing equipment tracks, in 3½ hours climbed the outside of one of the Twin Towers. The spectacle was watched by thousands of onlookers on the ground and millions of viewers on television. When he safely reached the roof he was greeted by two police officers. Later, the city of New York sued him for a quarter of a million dollars to cover the costs of police overtime and the police helicopters that were dispatched to the scene to stop news helicopters from flying too close to the towers. The lawsuit was later dropped and Willig paid a $1.10 fine, which equated to a penny a floor.

An essential element in preventing the first two types of these acts is controlling access to building roofs. In the last type, it is important for a building's perimeter to be controlled using security personnel and video surveillance, or a combination of both.

BASE Jumping

BASE is an acronym for Building, Antenna, Span (bridges) and Earth (cliffs). BASE jumping is a practice by which parachutists leap off high fixed objects.

Sometimes, high-rise building owners permit these jumps, particularly where a special film permit or sporting competition is being staged. For example, the Los Angeles Times reported that Petronas Towers, presently the world's tallest two buildings, was the site of the 2001 Malaysia International Extreme Skydiving Championships in Kuala Lumpur. However, in many jurisdictions these jumps violate trespassing and reckless endangerment laws.

> In private, some veterans tell of concocting elaborate ruses involving forged employee passes, paying off security guards and removing air-conditioning grates, all to pull off a stealth building jump. In 2001, BASE jumpers were arrested or cited for parachuting off buildings in cities including Minneapolis, New York and Paris. (Tawa, 2002, p. E3)

"In a bid for credibility—and more legal jump sites—veteran jumpers are offering training sessions and camps that stress safety, and selling gear made especially for their sport" (Tawa, 2002, p. E1). According to Jean Potvin, a skydiver and physics professor, "The new BASE-specific gear is reliable, and the sport can be practiced safely by experienced jumpers if all goes well. But the ante is upped for those who want to jump off buildings, he said. Odd winds that swirl around high-rises could slam a parachutist into a window. Vision becomes tricky on a nighttime jump from a high-rise, when the backdrop is darkness and not sky blue. Jumpers must be able to steer their chutes away from power lines, telephone poles and other obstacles. All in a matter of seconds" (Tawa, 2002, p. E3).

Strictly controlling access to the roof is the way to stop BASE jumpers.

Jumpers, protestors and daredevils can also be a serious problem when a building is being constructed. Strict access control to the construction site is the key to preventing such incidents.

Preserving a Crime Scene

Some of the preceding emergencies may have involved the commission of a crime. Arson, explosions, deliberate release of harmful chemical and biological agents, as well as workplace violence, robbery, rape, and homicide, are but a few examples. When a crime has occurred, its reconstruction largely depends on the collection, preservation, and analysis of physical evidence. Therefore, it is critical for any crime scene to be preserved as much as possible. Although the preservation of a crime scene will depend largely on the type of incident, the following are guidelines for security staff to observe:

1. Remove all persons from the crime scene and cordon off the area to prevent further entry.
2. Restrict entry to the crime scene to authorized individuals such as law enforcement, fire department, and emergency services personnel.
3. Prevent removal of any physical items from the crime scene.

In some situations, it may be critical for security staff to detain witnesses to a crime until the arrival of law enforcement. For example, in the September 23, 1997, fatal shooting on the observation deck of the Empire State Building, building security staff's actions in holding all of the witnesses to the incident considerably aided the New York Police Department's homicide investigation.

Impact of Building Emergencies on Security

Depending on the nature of the incident, most of the foregoing emergencies have some impact on the security of a high-rise building. By assessing these emergencies and their potential impact on a building's operations, preventive measures can be designed to reduce either their likelihood or their anticipated effects. Yet, as the Merritt Company (1991, p. 19-119) states:

> Some of the life-safety requirements [in a high-rise structure] actually pose unique security difficulties. The code provision which insists upon unimpeded exit during a building emergency means that if such an emergency can be faked, egress may be possible under little or no surveillance. Even if the emergency is genuine, it may occur at a time when the security forces are unprepared for the joint demands of emergency response and heightened security attention.

When a Building Emergency Is Faked

Once, in a high-rise office building, an individual set off a fire alarm by activating a manual fire alarm station on a tenant floor. This resulted in the evacuation of occupants from that floor and also two floors above and below it. An accomplice waiting on one of the evacuated floors, after all occupants had left, quickly roamed unchallenged through tenant offices and stole items from handbags and billfolds in coats that had been left behind in the hurry to evacuate. The thief then entered a stairwell, descended to the ground level, and walked undetected out of the building.

Such an event could similarly be staged by two individuals to gain unauthorized access to a floor that is normally always secured (i.e., the elevators only proceed to the floor if an authorized access card is used). One person could activate a manual fire alarm station on one floor, thereby causing the stairwell door locks to unlock automatically (if this feature is provided). An accomplice waiting in a stairwell on the targeted floor could then proceed into the tenant space (sometimes stairwells lead directly into tenant areas rather than into common corridors) and gain entry to commit a crime. The thief could then board a passenger elevator—because during fire alarm situations in many high-rise buildings, the elevators remain in service unless an elevator lobby smoke detector has been activated—or re-enter the stairwell and proceed down to the ground level to exit the building. Some facilities have security staff manually recall all elevators serving floors in alarm to prevent occupants from using them during fire and fire alarm situations. This practice has the added advantage of securing the floor from unauthorized access by someone using the elevators.

The following measures can be used to maintain a moderate level of building security during a fire or fire alarm emergency:

- If stairwells lead directly into tenant areas, consider redesigning the area to remove this security hazard.

- Train building occupants to always take personal valuables with them during evacuation and, if such actions do not place them in danger, to quickly secure other items.
- Position CCTV cameras with alarm-activated recording devices in tenant high-risk areas (particularly where valuables such as cash are found) to at least obtain a record of an incident.
- Install CCTV cameras with motion detectors in building stairwells close to the ground-level exit.

When an Emergency Overwhelms Security Staff

It is possible that a building emergency may be of such magnitude that security personnel are unprepared to handle both the emergency itself and the heightened security demands created by the incident. This may occur especially with fires (particularly if multiple ones simultaneously occur), explosions, workplace violence, civil disturbances, and some natural disasters.

The 1993 World Trade Center (WTC) bombing in New York (described earlier in this chapter) illustrated this point. After the explosion, WTC security staff were involved in caring for the injured, assisting hundreds of fire fighters (at that time, the number of which constituted the greatest single response to a fire in New York City Fire Department's history) and other emergency services in occupant evacuation, and helping other agencies—the Port Authority Police and New York Transit Police among others—to control access to the complex. Because of the enormity of the incident, the thousands of people affected, and the disastrous effects the explosion had on the towers' fire life safety systems, building security personnel were inundated with demands for their services and were strained to the breaking point. Of course, the tragic 2001 terrorist incident placed an almost indescribable burden on all involved, including those who lost their lives while helping others.

Summary

There are many emergency situations that can develop in high-rise office buildings. They include fires and fire alarms; workplace violence; hostage and barricade situations; medical emergencies; trip, slip, and falls; power failures; elevator malfunctions and entrapments; traffic accidents; labor disputes, demonstrations, riots, and civil disorder; bombs and bomb threats; hazardous materials, chemical and biological weapons, and nuclear attack; aircraft collisions; natural disasters (earthquakes, tsunamis, volcanoes, winter storms, tornadoes, hurricanes, high winds, cyclones, and floods); water leaks; and jumpers, protestors, and daredevils. Each one must be properly handled according to preplanned procedures.

The impact of such an emergency on building operations, including security, will depend on such factors as the geographical and topographical location of the facility, its design and construction, its security and fire life safety systems and equipment, the location of the emergency within the facility, and the emergency preparedness of building emergency staff and occupants. Also, if the emergency involves the commission of a crime, the crime scene should be preserved as much as possible.

References

Arneson, Jeanne, Larry Legind, Jamey Puga, William L. Rinehart, and William V. Wenger, ''Managing Violence in Office Buildings,'' (*Skylines*, Building Owners and Managers Association, September 1994).

Associated Press, ''Dutchman in product dispute takes hostages, kills himself'' from Associated Press (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, March 12, 2002).

ATF, *Bomb Threats and Physical Security Planning*, (Bureau of Alcohol, Tobacco and Firearms, Department of the Treasury, ATF P 7550.2, Washington, D.C., July 1987).

ATF, *1993 Explosives Incidents Reports*, (Bureau of Alcohol, Tobacco and Firearms, Department of the Treasury, Washington, D.C., 1993). Includes data from the Federal Bureau of Investigation, the United States Postal Service, and the Bureau of Alcohol, Tobacco and Firearms.

''The Atlanta massacre'' (*TIME*, Washington, D.C., August 9, 1999).

Bachman, James M., ''Hazardous materials in an office environment,'' (*BICEPP News*, Business and Industry Council for Emergency Planning and Preparedness, Spring 1992).

Berkeley Lab, ''Berkeley Lab researchers develop concise website on handling chemical-biological attacks against buildings'' (U.S. Department of Energy's Lawrence Berkeley National Laboratory, http://securebuildings.lbl.gov, April 3, 2002. Site development was led by Phillip Price).

BOMA, ''Considerations for specific types of emergencies,'' *Emergency Planning Guidebook* (Building Owners and Managers Association International, Washington, D.C., 1994).

Bordes, Roy N., ''Workplace violence,'' Security Concepts (Terra Publishing, Inc., Salamanca, NY, January 1994).

Boudreaux, Richard ''Airplane hits skyscraper in Milan; 3 die'' (The Times Mirror Company, Los Angeles, CA, April 19, 2002).

Broder, James F., *Risk Analysis and the Security Survey*, 2nd ed. (Butterworth–Heinemann, Woburn, MA, 2000).

Bryan, John L., ''Fire detection systems,'' *Fire Suppression and Detection Systems* (Macmillan Publishing Co., Inc., New York, 1982).

Caldwell, Carol, ''Occupancies in special structures and high-rise buildings,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Cal/OSHA, *Cal/OSHA Guidelines for Workplace Security* (California Division of Occupational Safety and Health, Department of Industrial Relations, San Francisco, August 15, 1994).

Carper, Alison, ''Workplace violence becomes frightening trend,'' (*Newsday*, September 1993); ''Signs are there to read before workplace violence hits,'' (*Business Wire*, May 1993). As reported in *Workplace Violence: Employer Obligations*, Thomas P. Burke, Esq., and Daniel Weisberg, Esq., Pettit and Martin, San Francisco.

Cauchon, Dennis, ''For many on Sept. 11, survival was no accident'' (*USA TODAY*, McLean, VA, December 20, 2001). Contributing: Barbara Hansen, Anthony DeBarros, and Paul Overberg. The information was obtained from a reprint of the article in the NFPA ''Emergency Response Planning Workshop Participant Workbook, Appendix 1V'' (San Francisco, CA, on March 6, 2002).

Cauchon, Dennis, and Martha T. Moore, ''Machinery saved people in WTC: row of elevator hoists sheltered stairwell when jet hit tower'' (*USA TODAY*, McLean, VA, May 17, 2002).

Chovanes, Michael H., ''Does regulatory compliance provide serious security?'' (*Security Management*, Arlington, VA, May 1994).

City of Los Angeles, Department of General Services, Emergency Preparedness Unit, High-Rise Fire Survival.

Clarke, Frederick B., ''Fire hazards of materials: an overview,'' *Fire Protection Handbook*, 18th ed. Arthur E. Cote, Editor-in Chief (National Fire Protection Association, Quincy, MA, 1997).

''Collapsed 7 WTC contained toxic chemicals'' (*Pasadena Star News*, Pasadena, CA, January 20, 2002).

Comeau, Edward, Mark C. Ode, and Robert F. Duval, *Office Building Fire Rockefeller Center, October 10, 1996, NFPA Fire Investigation Report* (National Fire Protection Association, Quincy, MA, 1996).

CTBUH, ''Council organizes task force'' (*The Times*, Council on Tall Buildings and Urban Habitat, LeHigh University, Bethlehem, PA, November 21, 2001).

Dames and Moore/URS Corporation, ''How buildings fared,'' *The Northridge Earthquake, January 17, 1994* (Dames and Moore, Los Angeles, 1994).

Dembart, Lee, ''Queens skydiver leaps safely from roof of the trade center,'' (*New York Times*, July 23, 1975), as reported in *Twin Towers: The Life of New York's World Trade Center* (Rutgers University Press, Piscataway, NJ, pp. 142–143, 1999) by Angus Kress Gillespie.

Donoghue, Edward A., ''Building transportation systems,'' *Fire Protection Handbook*, 18th ed. Arthur E. Cote, Editor-in-Chief (National Fire Protection Association, Quincy, MA, 1997).

Eagar, Thomas, commenting on the World Trade Center collapse in ''Why the towers fell'' (NOVA Online, http://www.pbs.org/wgbh/nova/wtc/collapse.html, April 30, 2002).

Engineering News Record (McGraw-Hill, Inc., New York, January 16, 1995).

Feasibility and Design Considerations of Emergency Evacuation by Elevators, NISTIR 4870 (U.S. Department of Commerce Technology Administration and the General Services Administration, September 1992).

FEMA 403, *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations, Federal Emergency Management Agency*, (FEMA, Washington, DC, May 2002).

Fire Problems in High-Rise Buildings (Fire Protection Publications, Oklahoma State University, Stillwater, OK, 1976).

Fire Safety on the Job (National Fire Protection Association, Quincy, MA, 1993).

Fischer, Robert J., and Gion Green, ''Fire protection, safety, and emergency planning,'' *Introduction to Security*, 6th ed. (Butterworth–Heinemann, Stoneham, MA, 1998).

''Fortune 1000 professionals list top security threats'' (*Securitas* magazine, Middlesex, UK, January, 2002).

Getlin, Josh, ''N.Y. building blast injures 42'' (The Times Mirror Company, Los Angeles, CA, April 26, 2002).

Gillespie, Angus Kress, ''Winning acceptance,'' *Twin Towers: The Life of New York's World Trade Center* (Rutgers University Press, Piscataway, NJ, 1999).

Giordano, Gerard M., ''Property owners, clean-up and OSHA regulations,'' (*Skylines*, BOMA International, Washington, D.C., January 1995).
Gips, Michael A., ''Reexamining premises for high-rise design'' (*Security Management*, Arlington, VA, September 2002).
Gold, Matea, and Maggie Farley, ''ATTACK: a day of terror'' (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, September 12, 2001).
Hall, John F., *Response of Modern Steel Buildings*. Paper presented to the Seismological Society of America and the Earthquake Engineering Research Institute Joint Symposium, ''Living with Earthquakes in Southern California'' (Pasadena, CA, April 7, 1994).
Hall, John R., Jr., *High-Rise Building Fires*, (National Fire Protection Association, Quincy, MA, September 2001).
Hartzel, Gordon E., ''Combustion products and their effects on life safety,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).
''High-rises remain vulnerable after 9/11,'' Patrick O'Driscoll (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, September 25, 2002).
Hinman, Eva E., and David J. Hammond, *Lessons Learned from the Oklahoma City Bombing Defensive Design Techniques* (ASCE Press, American Society of Civil Engineers, New York, NY, 1997).
IREM, ''Hurricanes,'' *Before Disaster Strikes: Developing an Emergency Procedures Manual* (Institute of Real Estate Management, Chicago, 1990).
IREM, ''Nuclear attack,'' *Before Disaster Strikes: Developing an Emergency Procedures Manual* (Institute of Real Estate Management, Chicago, 1990).
Isaiah, Chapter 24, Verses 18–19, Old Testament, New American Standard Version Bible, The Open Bible (Thomas Nelson Publishers, The Lockman Foundation, New York, 1977).
Isner, Michael S., and Thomas J. Klem, ''Discussion,'' *Fire Investigation Report, World Trade Center Explosion and Fire* (National Fire Protection Association, Quincy, MA, 1993).
Isner, Michael S., ''Five die in high-rise office building fire'' (**FIRE**JOURNAL, National Fire Protection Association, Quincy, MA, July/August 1990).
Jackson, Robert L., ''Survey faults security at federal buildings'' (*Los Angeles Times*, June 29, 1995). Adapted from *Vulnerability Assessment of Federal Facilities* (June 28, 1995)—for sale by the U.S. Government Printing Office, Superintendent of Documents, Mail Stop SSOP, Washington, D.C. 20402-9328, Stock #027-000-01362-7.
Jennings, Charles, ''High-rise office building evacuation planning: human factors versus 'Cutting edge' technologies'' (*Journal of Applied Fire Science*, Vol. 4(4) 289-302, 1994-95, Baywood Publishing Co., Inc., 1995).
Johnson, William H., and Warren R. Matthews, ''Disaster plan simulates plane crash into high-rise building'' (*NFPA Journal*, National Fire Protection Association, Quincy, MA, November/December 1993).
Keating, John P., and Elizabeth F. Loftus, ''The logic of fire escape,'' (*Psychology Today Reprint*, June 1981).
Kimball, Virginia, *Earthquake Ready*, 2nd ed. (Roundtable Publishing, Inc., Santa Monica, CA, 1988).
Klem, Thomas J., ''3 major high-rise fires reveal protection needs'' (NFPA *Journal*, National Fire Protection Association, Quincy, MA, September/October 1992).
Klote, John H., *An Analysis of the Influence of Piston Effect on Elevator Smoke Control* (U.S. National Bureau of Standards, NBSIR 88-3751, 1988). As reported in *Feasibility and Design Considerations of Emergency Evacuation by Elevators* (U.S. Department of

Commerce Technology Administration and the General Services Administration, September 1992).
Klote, John H., and G. T. Tamura, ''Elevator piston effect and the smoke problem'' (*Fire Safety Journal*, 11(3), 227–233, May 1986). As reported in *Feasibility and Design Considerations of Emergency Evacuation by Elevators*, NISTIR 4870 (U.S. Department of Commerce Technology Administration and the General Services Administration, September 1992).
''Man falls to death from stalled elevator'' (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, October 26, 2000).
McNally, Karen C., ''Earthquake,'' *World Book Online Americas Edition* (http://www.aolsvc.worldbook.aol.com/wbol/wbPage/na/ar/co/171680, June 14, 2002).
Merritt Company, The, ''High-rise structures, Section B, Security considerations,'' *Protection of Assets Manual*, Vol. III (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, 1991).
Meyer, Josh, ''FBI expects suicide bomb attack in U.S.'' (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, May 21, 2002).
MobileSearch™ (Information obtained at a demonstration of the American Science and Engineering [AS&E] MobileSearch system, Billerica, MA, www.as-e.com, June 2002).
Neuman, Johann, ''Scientists weigh in with deductions on anthrax killer'' (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, April 21, 2002).
New Webster Encyclopedic Dictionary of the English Language, 1980 Edition, Editor-in-Chief Virginia S. Thatcher (Consolidated Book Publishers, Chicago).
Neuman, Johanna, ''Scientists weigh in with deductions on anthrax killer'' (The Times Mirror Company, Los Angeles, CA, April 21, 2002).
''Never Again!'' (*SECURITY*, Highlands Ranch, CO, July 2000).
''The next big one'' (*TIME*, Washington, D.C., January 24, 1994).
NFPA Fire Analysis and Research Division, ''International Listing of Fatal High-Rise Structure Fires 1911–Present'' (National Fire Protection Association, Quincy, MA, 1993).
NFPA *Glossary of Terms* from the National Fire Code (National Fire Protection Association, Quincy, MA, 2001).
NFPA 101, ''Fundamental Requirements,'' *Life Safety Code*, Section 4.5.3.1 (National Fire Protection Association, Quincy, MA, 2000).
NFPA 2002 *High-Rise Evacuation* video (National Fire Protection Association, Quincy, MA, http://nfpacatalog@nfpa.org, Copyright 2002).
NIOSH, http://www.cdc.gov/niosh/violpurp.html (The National Institute for Occupational Safety and Health, May 2002). Jenkins 1996, Bachman 1994, Windau and Toscano 1994, and the FBI 1994 are cited in this reference on workplace violence.
NIOSH, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, Publication No. 2002-139 (Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, May 2002).
''N.Y. building blast injures 42'' (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, April 26, 2002).
''Official death toll of tsunami at 2,000'' (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, July 28, 1998).
OSHA, *General Industry: Safety and Health Regulations*, Title 29 of the Code of Federal Regulations, Part 1910 (U.S. Department of Labor, OSHA, Washington, DC, 1974).
Otis Elevator Company, 5811, *How to Operate Elevators Under Emergency Conditions* (United Technologies/Otis, SPF-513 [5811]).
Plenzler, Jerry, ''Elevator, escalator safety is no accident,'' (*Skylines*, BOMA International, Washington, D.C., November/December 1994).

POA, ''Bombs and bomb threats,'' *Protection of Assets Manual*, Vol. IV (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, 1995).

POA, ''High-rise structures, Section A, Life safety considerations,'' *Protection of Assets Manual*, Vol. III (Used with permission of POA Publishing, LLC, Los Angeles, CA, 2000, 323/663-4887).

Post, Nadine M., ''Defending against bioterrorism'' (*Engineering News-Record*, McGraw Hill, New York, NY, January 21, 2002, p. 12).

'' 'Powerful' Sept. 11 observances set'' (*Los Angeles Times*, The Times Mirror Company, Los Angeles, CA, August 7, 2002).

Prouix, Guylène, and Rita Fahy, *A Comparison of the 1993 and 2001 Evacuations of the World Trade Center*, Presentation to the NFPA World Safety Congress & Exhibition, Minneapolis, MN, May 21, 2002.

Pyes, Craig, and Wiiliam Rempel, ''Poison gas plot alleged in Europe'' (The Times Mirror Company, Los Angeles, CA, November 12, 2001).

Reader's Digest Great Encyclopedic Dictionary, 3rd ed. (The Reader's Digest Association, London, compiled by Oxford University Press, 1979).

Reich, Kenneth, ''Study raises Northridge quake toll to 72,'' results of a study by Michael E. Durkin, A Woodland Hills public health researcher as reported in the *Los Angeles Times* (The Times Mirror Company, Los Angeles, CA, December 20, 1995).

Salvadori, Mario, ''Structures,'' *Why Buildings Stand Up: The Strength of Architecture* (W.W. Norton & Company, Inc., New York, 1980).

Sahagun, Louis, ''5 injured in explosion at Westwood high-rise'' (The Times Mirror Company, Los Angeles, CA, December 22, 2000).

''Security soars to new heights'' (*SECURITY*, September 1997).

''Sensors of chemical warfare agents make a mass-transit debut'' (Corporate Security Publishing, ssbrooks@gateway.net, July 14, 2000).

Solomon, Robert E., Assistant Vice President–NFPA, in correspondence with the author (July 8, 2002).

Stratton, David R., ''New ideas about bomb searches,'' (*Security Management Bulletin*, Bureau of Business Practice, Waterford, CT, 1994).

Tawa, Renee, ''The three-second rush'' (*Los Angeles Times*, March 24, 2002).

''Tornado rips downtown Fort Worth'' (*Los Angeles Times*, March 29, 2000).

''Towering team leader,'' (*Access Control & Security Systems*, Atlanta, GA, September 2000).

U.S. Geological Survey, ''Earthquakes occur throughout the United States'' (National Earthquake Information Center, Denver, 1990).

Weiger, Pamela R., and John Nicholson, ''Learning from 9-11,'' (*NFPA Journal*, National Fire Protection Association, Quincy, MA, May/June 2002).

Webster's College Dictionary, 1992 Edition (From Random House Webster's College Dictionary by Random House, Inc. Copyright © 1995, 1992, 1991 by Random House, Inc. Reprinted by permission of Random House, Inc., New York, 1992.)

Willman, David, and Michelle Munn, ''Dirty bomb's greatest impact likely would be psychological'' (The Times Mirror Company, Los Angeles, CA, June 11, 2002).

''WTO riot energizes new wave of domestic terrorism'' (*SECURITY*, Highlands Ranch, CO, January 2000).

Yanez, Lulsa, and Tere Figueras, ''Teen dies after flying plan into skyscraper's 28th floor'' (*Pasadena Star News*, Pasadena, CA, January 6, 2002).

Zimmerman, Rachel, '' . . . Mail,'' comments by Jerry Hauer, Kroll Inc. (*The Wall Street Journal*, New York, March 11, 2002).

Additional Reading

ASIS Relevant Security Resources on the Internet For Terrorism, Disaster Recovery and Related Subjects, ASIS International, O.P. Norton Information Resources Center. http://www.asisonline.org/pdf/resources.pdf.

FEMA 403, *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations*, (Federal Emergency Management Agency [FEMA], Washington, DC, May 2002), http://www.fema.org.

Hinman, Eva E., and David J. Hammond, *Lessons Learned from the Oklahoma City Bombing Defensive Design Techniques* (ASCE Press, American Society of Civil Engineers, New York, NY, 1997).

Klaene, Bernard J. ''Ben,'' and Russell E. Sanders, *Structural Fire Fighting* (National Fire Protection Association, Quincy, MA, 2000).

NFPA Fire Investigations Selected Investigations Reports on CD (National Fire Protection Association, Quincy, MA).

NIOSH, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, Publication No. 2002-139 (Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, May 2002), http://cdc.gov/niosh.

United States Department of Energy's Lawrence Berkeley National Laboratory web site: http://securebuildings.lbl.gov. Developed by Berkeley Lab Researchers, headed by Phillip Price, these ''Guidelines Are Intended to Assist 'First Responders'—Police, Fire, Emergency Services Agencies and Building Operators on Handling Chemical-Biological Attacks Against Buildings'' (Berkeley Lab, April 2002).

This Page Intentionally Left Blank

11 *Building Emergency Planning*

For a building owner or manager to effectively handle an emergency that may affect a high-rise office building, it is necessary to plan ahead. There may be chaos during an emergency, particularly if there is a disruption in normal communications. A *plan* is defined by the *Webster's College Dictionary* as ''a scheme or method of acting or proceeding developed in advance.'' The Building Owners and Managers Association International (BOMA) defines an *emergency plan* as ''a set of actions intended to reduce the threat from emergencies that may affect a facility. A comprehensive plan reduces the threat from emergencies through prevention, early detection, notification, effective evacuation or relocation measures, control and mitigation, and recovery operations'' (BOMA, 1994, p. 1).

Fire Emergencies

Any building fire emergency plan should incorporate the features in the following sections.

Prevention

All building occupants should receive adequate training in fire prevention practices. New occupants or employees should receive this training when they move into a building or at the start of their employment. Training should include what a fire alarm sounds like and, in modern high-rise buildings (or older buildings that have been retrofitted), looks like (a strobe light for hearing impaired persons); how to protect oneself if a fire occurs, including the location of emergency exits; how to tell others who may be at risk; how to confine a fire; and how to notify those who will respond to the fire. Prevention also should include training in the following fire prevention practices to reduce the threat of fire before it occurs:

- Occupants should adhere to smoking rules and regulations. High-rise office buildings have designated safe, supervised, and convenient smoking areas, with many prohibiting any smoking within the building because of health concerns related to second-hand smoke. Any smoking areas must be clearly marked and equipped with nontip ashtrays, metal waste receptacles, and fire extinguishers.

All NFPA material used with permission from the National Fire Protection Association, Quincy, MA.

- Areas within tenant spaces, storage areas, and public corridors should be free of obstructions and of fire hazards such as empty cartons, dirty rags, trash, and improperly stored materials. Good housekeeping practices should keep areas clean and as neat as possible. Violations should be reported promptly.
- Electrical equipment should be inspected regularly to ensure proper and safe functioning. Appliances and cords should be UL-listed; there should be limited use of extension cords; frayed or cracked cords and broken connections should be replaced; cords should not be run across doorways or under carpets and mats where they may be stepped on; heat-producing appliances should have space around them for ventilation; all problems with electrical equipment should be immediately reported and/or the equipment should be taken out of service; and appliances such as cooking equipment, coffee makers, hot plates, and photocopiers should be switched off when not in use, particularly at the end of each business day.

A sample Fire Prevention Inspection Checklist is included in Appendix 11-1.

Early Detection and Notification

During normal business hours in fully occupied high-rise office buildings there are usually plenty of people—building management, engineering, security, parking, janitorial staff, contractors and repair personnel, or occupants and visitors—moving throughout many areas of the building. As a result, if a fire occurs, there will be early detection and notification of it by human means or by the building's automatic fire detection system, and the fire usually will be suppressed before it has an opportunity to develop into a major conflagration. However, after normal business hours and on weekends and holidays, the number of people present in the building is severely reduced, so there is more dependence on the building's automatic fire detection and notification systems and security staff. According to Klem (1992, p. 61):

> The reliability of such protection depends on the completeness of the fixed detection and suppression equipment and the emergency fire procedure training of security staff. If any of these are deficient, severe fires are more likely to occur. For these reasons, high-rise buildings where reliable fixed fire protection systems are not present simply are more vulnerable to the potential for large losses during nonbusiness hours.

Effective Evacuation or Relocation Measures

The size of high-rise buildings and the high number of people often contained in them make it impractical to quickly evacuate all occupants during a fire emergency. *Evacuation* or *relocation* is the movement of people during an emergency to a location, inside or outside of the building, that is considered a safe refuge area. Evacuation* usually involves leaving the building, whereas relocation involves moving to an area of relative safety within the building.

**Total* evacuation of a building means all occupants leave the structure, whereas a *staged* evacuation means only occupants on certain floors are evacuated.

Control and Mitigation and Recovery Operations

It is critical to quickly apply appropriate control and mitigation measures during a fire emergency. Automatic fire detection and suppression systems found in modern high-rise office buildings are essential in controlling a fire and mitigating its impact on operations. After the fire emergency has been handled successfully, recovery operations should restore any affected areas of the building to their normal condition.

Emergency Planning Guidelines

A *Building Emergency Plan* incorporates the planning and preparation leading up to an emergency and shortly thereafter, whereas a *Business Resumption Plan* addresses issues that permit a business to resume normal operations as soon as possible after an incident. This chapter addresses the former but does not specifically address the latter.

> The objective of a [Building Emergency Plan] should be to allow those responsible for the [facility] during an emergency to focus on the solution of major problems, not to attempt immediately to bring order out of chaos. If all predictable and routine items are considered in the plan, those responsible for actions during an emergency will be able to deal with the unpredictable or unusual situations that will surely develop. (The Merritt Company, 1991, p. 10-3)

A Building Emergency Plan consists of the following: (1) Building Emergency Procedures Manual, (2) occupant documentation and training, (3) Floor Warden Manual and training, (4) building emergency staff training, and (5) evacuation signage. The sections that follow address these areas in detail.

Building Emergency Procedures Manual

This manual is a written document that describes actions formulated to reduce the threat to life safety from emergencies that are most likely to occur in a specific building. The authority having jurisdiction, such as the local fire department, often will develop written criteria and guidelines on which plans may be based. The following suggested format for material that may be contained in the manual has been developed using the Los Angeles Fire Department *Guideline Format for High-Rise Buildings: Emergency Procedures City of Los Angeles 1993*. For ease of explanation, some reference is made in this format to a hypothetical high-rise office building, Pacific Tower Plaza, which was mentioned in Chapter 4. Building owners and managers developing a Building Emergency Procedures Manual should consult with the authorities having jurisdiction, including local officials, for precise criteria and guidelines on which their plan should be based.

Title Page

A typical title page indicates the name and address of the building, the name of the person by whom the manual is compiled, what authority having jurisdiction has approved the plan, who is authorized to change or modify the Building Emergency Procedures Manual, the authority having jurisdiction to which any future changes or updates of material should be sent, the date, and a notation of the copy number. The next page should list the number of copies of the manual and to whom each copy is to be distributed. Figure 11.1 shows a sample title page.

Table of Contents

The table of contents consists of a listing by page number of all pertinent sections of the manual.

Introduction

The introduction is a statement of the Building Emergency Procedures Manual's purpose, the name of the authority having jurisdiction, with whose cooperation it was compiled, and which material in it is required by law. For example, the introduction may be as follows:

> Management of Pacific Tower Plaza, in cooperation with the City of Toluga Hills Fire Department, has produced this manual to help ensure the safety of occupants in the event of an emergency. The material pertaining to the State Fire Code and the Toluga Hills Fire Code is required by law. Owners, managers, and tenants of high-rise office buildings in the City of Toluga Hills are required to comply with these requirements or be subject to prosecution and penalties, including fines as set forth in the State Fire Code. Additional procedures for explosions, bombs, bomb threats, aircraft collisions, violence in the workplace, medical emergency, power failure, elevator malfunctions and entrapments, natural disasters, water leaks, hazardous materials incidents, and labor disputes, demonstrations, riots, and civil disorder are provided by Pacific Towers Plaza Management for the life safety of building occupants. This manual and its contents remain the property of Pacific Tower Plaza and should be readily available to the Toluga Hills Fire Department on request.

Legal Requirements

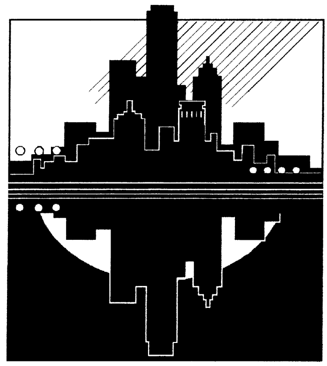
This section is a statement of the applicable state and local laws pertaining to emergency planning and evacuation requirements for high-rise buildings.

Emergency Telephone Numbers

This section of the manual lists telephone numbers and ways to contact persons and agencies when a building emergency occurs. Because an emergency can occur at any time of day or night, on weekdays or on weekends and holidays, it is essential to have a readily available means of contacting appropriate individuals and agencies. Included in this section are the following:

1. Telephone numbers for outside emergency response agencies including fire and police departments, paramedic ambulances, local hospitals, poison control centers, hazardous material response agencies, and public utility companies.

Building Emergency Procedures Manual



Pacific Tower Plaza

One Poppyfields Drive

Toluga Hills

The content of this manual has been approved by the City of Toluga Hills Fire Department. If changes in content, including either of the following changes, occur, it is the responsibility of the Building Owner, Manager, or Operator to cause notification of these changes to the City of Toluga Hills Fire Department:

1. Change of Building Owner, Manager, or Operator.
2. Change of Building Fire Safety Director.

This revised information shall be communicated to:

Toluga Hills City Fire Department High-Rise Division

300 Main Street, Toluga Hills

Telephone (613) 726-0773

This manual is the property of Pacific Tower Plaza and was compiled by J. Smith.

January 1, 2003

Figure 11.1 Building Emergency Procedures Manual sample title page.

2. Location and contact means (both during and after normal business hours) for building emergency staff such as the owner or manager, the building Fire Safety Director, the building Alternate Fire Safety Director, engineering, security, janitorial, parking, and other applicable departments. Management succession lists should be developed to include sufficient names to ensure that someone can be contacted during an emergency, no matter when it occurs. A notation should be made here about the confidentiality of this information and that it is to be used only for emergency purposes.
3. Locations and telephone numbers of floor wardens and their designated alternates. (A sample *Floor Wardens and Alternates Roster* is included in Appendix 11-1.)
4. Locations, telephone numbers, and type of disability of disabled and non-ambulatory persons and their assistance monitors. A confidentiality notation should be made here, as for building emergency staff. (A sample *Disabled or Non-Ambulatory Persons List* is included in Appendix 11-1.)

These emergency telephone numbers should be revised immediately if changes occur; also, all numbers should be verified, preferably monthly, or at least quarterly.

Building Emergency Staff Organization

This section explains the Building Emergency Staff Organization that will carry out emergency response procedures until relieved by outside response agencies. A typical staff organization for a high-rise office building is outlined in Figure 11.2.

Each unit of the Building Emergency Staff Organization will have duties and responsibilities developed and tailored to the specific needs of the building and to each type of emergency they may be required to handle. These duties and responsibilities should be defined clearly so that there will be a coordinated and effective response to each emergency situation. For example, the duties and responsibilities of building management, the building Fire Safety Director, and the building engineering and security staff in handling a fire emergency will include ensuring that the fire department has been immediately notified, all occupants have been advised, any necessary evacuation or relocation of affected occupants has begun, fire life safety systems are operating under emergency conditions, any investigation or initial suppression of the fire is carried out, and that the fire department and other responding personnel are met on arrival at the facility. In contrast, during a bomb threat incident, these personnel may be involved in supervising the evacuation or relocation of occupants or assisting in searching certain building areas. Building parking staff may be called on to assist in the evacuation of occupants from parking areas. Building janitorial staff may be required to clean up areas after water leaks, liquid spills, or water discharged from sprinklers, or, in the case of a bomb threat, to search areas with which they are familiar.

Floor response personnel (floor wardens, stairwell monitors, elevator monitors, search monitors, and disabled assistance monitors) have specific duties and responsibilities that vary according to the type of emergency encountered. Primarily, these individuals oversee the safe and orderly evacuation or

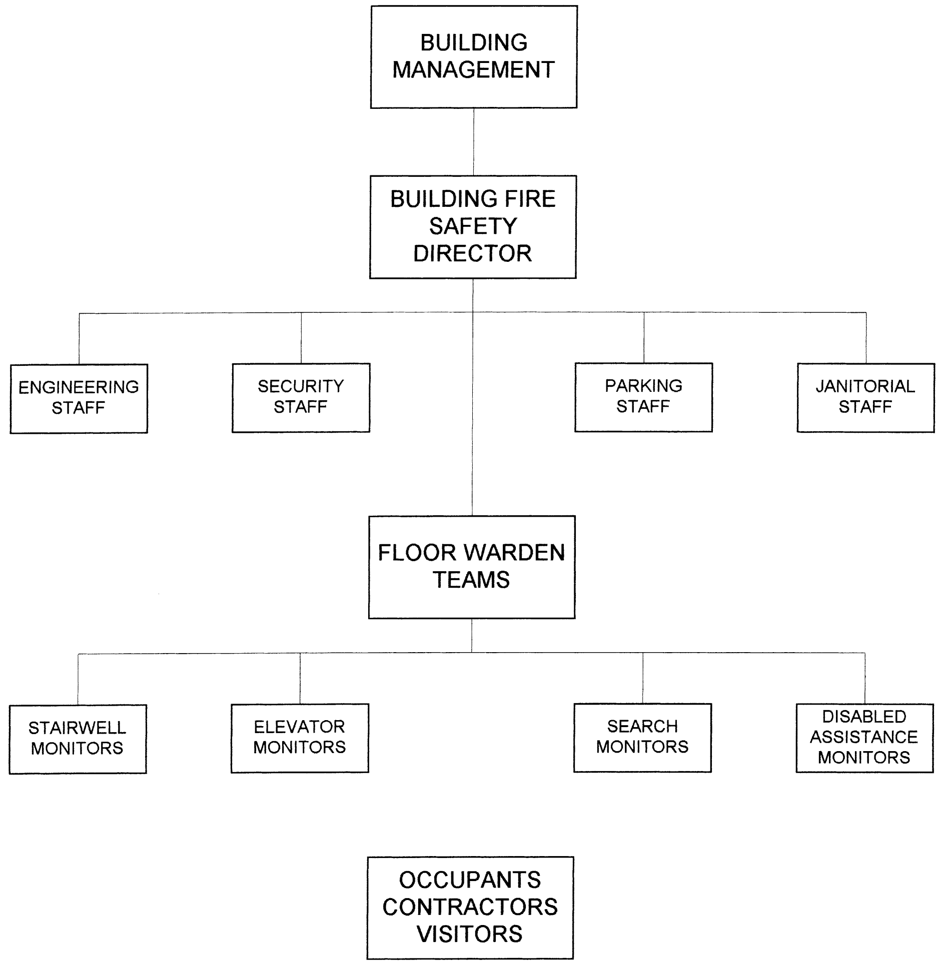


Figure 11.2 Building Emergency Staff Organization.

relocation of occupants from a building floor when a fire emergency exists. Their duties are described in the next sections.

Building Floor Wardens

Usually each floor has a *floor warden* (in some localities they are called a *fire warden* or an *emergency floor coordinator*) and a designated *alternate floor warden*; if the *floor plate*—the entire floor area including the public access or common areas, tenant areas, and maintenance spaces—is particularly large or there are many individual tenants, there may be additional floor wardens (some buildings refer to the floor warden of an individual suite as a *suite warden* or *deputy floor warden*). Some fire departments stipulate the number of floor wardens to be provided. For example, in New York City, "Each floor of a building shall be under the direction of a designated Fire Warden for the evacuation of occupants in the event of a fire. Deputy Fire Wardens shall assist him or her in his on her duties. A Deputy Fire Warden shall be provided for each tenancy. When the floor area of a tenancy exceeds 7,500 square feet of occupiable space, a Deputy Warden shall be assigned for each 7,500 square feet or part thereof'' (NYFD, 1972, p. 5). Whenever these persons are called to duty an armband, a vest, or a hardhat may identify them.

Floor wardens are selected for their ability to make sound decisions during emergency situations, provide direction, and maintain order. They should be thoroughly familiar with the Building Emergency Plan and, in cooperation with the building Fire Safety Director, should oversee and ensure safe and complete evacuation or relocation of occupants under their supervision during a fire or other emergency, or during a fire drill.

Basic Duties

Duties of floor wardens and alternate floor wardens include:

1. Overseeing training and instruction of occupants.
2. Determining and coordinating appropriate emergency response actions for a particular floor or portion of a floor.
3. Ensuring a safe and complete evacuation of all occupants, including individuals with disabilities, from unsafe areas.
4. Ensuring that evacuated or relocated occupants are kept at a safe refuge area and prevented from reentering the building or returning to their workplace until proper authorization has been received from building management or the fire department. A safe refuge area inside and outside the building should be specifically designated. The authority having jurisdiction may need to be consulted to determine what areas are considered safe—the location of interior safe refuge areas will be largely determined by fire codes; outside safe refuge areas will depend on the site layout, adjacent streets, alleys, parking lots, and so on.

Other Response Team Members

To carry out these responsibilities, as outlined by the Los Angeles Fire Department *Guideline Format for High-Rise Buildings*, floor wardens should select and supervise floor response personnel and ensure that these positions are always staffed. These personnel should be trained ahead of time for their respective duties, or, if designated on the spot by the floor warden or alternate floor warden, quickly be instructed on what to do. The following response personnel are needed:

- *Stairwell monitors*, of which there is one per stairwell, lines up occupants in an orderly fashion at the entrance to the stairwell, controls access, organizes an orderly flow of persons into the stairwell when evacuation begins, and closes the door when no one is moving through it.
- *Elevator monitors* direct all passengers who arrive at the floor to proceed to the nearest safe stairwell and prevent any occupants from using the elevators during a fire emergency for evacuation. (This can be a problem, particularly on heavily populated floors.)
- *Search monitors* systematically and thoroughly search all assigned floor areas to ensure that all occupants evacuate (this includes closed areas such as offices, photocopier rooms, restrooms, kitchens, rest areas, conference rooms, libraries, computer rooms, and data centers). After an area has been searched, doors

leading to it are closed (but not locked) and each door is marked (for example, with a self-stick note or piece of tape) to identify the area within as having been searched and cleared of all occupants. This avoids duplication of effort.

- *Disabled assistance monitors* locate disabled and non-ambulatory persons and assist them to the nearest ''area of rescue assistance'' (a term defined later in this chapter). Usually two monitors or ''buddies'' are assigned to each person.
- *Telephone monitors* provide telephone liaison between floor warden and floor response personnel, liaison between the floor warden and the Fire Safety Director or the fire department, and liaison between floors.
- *Runners/Messengers* provide physical liaison in the areas normally covered by the telephone monitors when there is a failure of telephone communications.

Because fire poses such a threat to people and property, and medical emergencies normally require rapid attention, some high-rise buildings provide training in the correct use of fire extinguishers, basic first aid, and cardiopulmonary resuscitation (CPR) for all floor wardens and alternates. In a building where stairwell doors are not equipped with locks that automatically unlock on activation of the fire life safety system, the floor warden and assistant floor wardens on the relocation floor will need to be notified, usually through the building public address (PA) system, to open the stairwell doors so that occupants can enter the relocation floor. As with building floor wardens, floor response personnel should have designated alternates who can assume their positions when necessary.

Building Fire Safety Director

The Fire Safety Director should be a responsible person who is employed on the premises, unless otherwise approved by the local fire department having jurisdiction. This person is a key component of any high-rise building's fire life safety program. He or she represents the building owner and manager in all fire life safety issues—in particular, the building's response to on-site emergencies—and works closely with the fire department to establish, implement, and maintain the Building Emergency Plan. The Fire Safety Director should be an energetic self-starter with good organizational skills; have the ability and inquisitiveness to understand complex building systems; be able to communicate well, both verbally and in writing; and be able to train and supervise others' activities. He or she must deal effectively at all levels with building management, emergency staff, tenants, occupants, and public agencies such as law enforcement and the fire department.

This individual is the driving force behind any successful fire life safety program. If an experienced and highly motivated person occupies this position, the Building Emergency Plan will be up to date, effectively communicated to all building occupants, properly executed, and a valuable asset to building management in its relationship with its present tenants and its efforts to attract future tenants. Building emergency staff, floor wardens, and occupants will be well trained and in a state of readiness to successfully handle the types of emergencies the building is likely to experience.

The Los Angeles Fire Department's *Guideline Format for High-Rise Buildings* outlines the responsibilities and duties of a Fire Safety Director. This staff member needs to do the following:

1. Implement the fire life safety program for the building as called for by state and local laws and the fire authority having jurisdiction.
2. Establish and maintain an up-to-date Building Emergency Procedures Manual.
3. Ensure that the building is maintained in a safe condition for occupants by conducting regular safety inspections of all areas, including tenant spaces, and documenting all efforts to correct hazards and problems.
4. Maintain up-to-date lists of floor wardens and alternates.
5. Maintain up-to-date lists of disabled and non-ambulatory persons.
6. Distribute documentation and printed material to building occupants, floor wardens, and building emergency staff outlining procedures to be followed when an emergency occurs.
7. Provide training that details the duties and responsibilities of all persons in an emergency situation and maintain documentation of dates, subject, and attendance for each training session.
8. Conduct fire evacuation drills as required by state and local fire codes.

See Appendix 11-1 for samples of a *Fire Prevention Inspection Checklist*, a *Floor Wardens and Alternates Roster*, and a *Disabled or Non-Ambulatory Persons List*.

In addition, during tenant build-outs, building interior construction, or upgrades of tenant and building systems and equipment, the Fire Safety Director should, as Studer (1992) points out, ''verify that wall and floor slab openings around piping, conduit, and duct work are properly sealed with Underwriters Laboratories (UL)-listed fireproofing material to match the existing fire rating of the walls and slabs; ensure that new duct work passing through walls or floor slabs have been properly provided with fire dampers'' (p. 8). Tenant storage areas should be a particular focus for inspections because they are often crammed full of material. Also, any loading docks and parking structures that have been converted for storage should be inspected. Studer (1992, p. 8) continues:

> To minimize the risk of fire in storage areas, building code requirements for these areas should be rigidly enforced, including:
>
> - Limit the size of storage areas and/or provide automatic sprinkler protection throughout the storage area.
> - When sprinklers are installed in a storage area, the height of the storage area should be kept at least 18 inches [or 0.5 meters] below the sprinklers' deflectors.
> - Storage should be prohibited [in] electrical rooms, mechanical rooms, elevator equipment rooms, electrical switchgear rooms, and other similar occupancies.

Whenever it is determined that a building or premises presents a hazard to life or property as a result of a fire or other emergency, or when it is determined that any fire protection equipment or system is inoperable, defective, or has been taken out of service, the Fire Safety Director needs to institute a fire watch. Patrols at appropriate intervals, as required by the authority having jurisdiction, should be conducted with the purpose of ''notifying the fire department and/or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety danger'' (NFPA *Glossary of Terms*, 2001).

The Fire Safety Director, alone or in conjunction with the engineering staff, generally is responsible for ensuring that fire life safety systems and equipment are inspected, tested, maintained, and repaired according to the specified guidelines of the authority having jurisdiction. Typically in large high-rises, building engineers do not have the time to perform these labor-intensive inspections, and sometimes they do not possess all the skills necessary to perform the required maintenance services on the wide variety of equipment. Most directors, therefore, hire a licensed contractor to perform this work using a support team. Further, the directors (or possibly the engineers) maintain the documentation of these activities so that it is readily available for review by the authority having jurisdiction.

Emergency Duties

During an emergency, a Fire Safety Director:

1. Ensures that the appropriate outside emergency agencies have been notified.
2. Coordinates the activities of all building emergency staff and floor wardens.
3. Coordinates all occupant notification and makes sure that any necessary evacuation or relocation begins.
4. Ensures adequate monitoring and control of all building life safety systems and equipment. During a fire emergency, some authorities having jurisdiction require that the building Fire Safety Director must make sure that all elevators serving the fire floor are recalled to the lobby level (unless the fire is occurring in the lobby) and taken out of service.
5. Confirms that any investigation of the fire or source of the fire alarm, or initial suppression of a fire, is performed.
6. Arranges for responding emergency personnel to be met at the designated entrance of the building and given an up-to-date report on the incident (including its location and any reported injuries), the status of security and building fire life safety systems, and the location and status of all evacuees and building emergency staff addressing the incident (building information forms, notification of specific hazards, floor plans, essential keys and access cards, etc., also should be readily available).
7. Ensures that every incident is thoroughly documented and that required notifications and reports to the appropriate authorities are carried out.

During a fire emergency, the Fire Safety Director should go to the Fire Command Center to supervise the direction and execution of the Building Emergency Plan. Some authorities having jurisdiction specify this requirement in their local fire codes to ensure that it occurs—for instance, the City of New York Fire Department's Administrative Code, Section 27-4627, clearly states, ''During fire emergencies, the primary responsibility of the fire safety director shall be the supervision and manning of the fire command station and the direction and execution of the evacuation as provided in the fire safety plan.'' To help facilitate this, the office of the Fire Safety Director should be located on lower floors of the building in reasonable proximity to the Fire Command Center.

During normal business hours, if the Fire Safety Director is not on site at the time an emergency occurs, there should be an *Alternate* or *Deputy Fire Safety Director* who assumes the duties of the Fire Safety Director. Also, after normal business hours, when the Fire Safety Director is normally not on site, the plan should assign the duties and responsibilities to another individual. Sometimes—in New York City, for example—this after-hours individual is referred to as a *Building Evacuation Supervisor*.

Procedures for Handling Building Emergencies

This section outlines the procedures for handling emergencies that are most likely to occur in the building. Each emergency should be separately addressed, with the duties and responsibilities of each member of the Building Emergency Staff Organization documented in detail. It should be kept in mind that ''no one individual can be expected to think of all the things necessary[*] to a successful response to an emergency event. It is imperative that group interaction take[s] place during planning so the multitude of things that must be considered are addressed. It is always smarter to have something and not need it than need something and not have it'' (Gigliotti and Jason, 1991, p. 53). Key members of the emergency staff should be consulted when a Building Emergency Plan is being formulated. The input of individuals such as the head of engineering (called the *Chief Engineer* in most large high-rises) is crucial to the success of any plan.

It is only through such a plan that training can be effectively conducted and much of the confusion frequently associated with emergencies can be substantially reduced. ''All of the senses tune up and the adrenaline starts to flow. We react better in emergencies and in one like this, everything comes into play . . . and people get into doing those types of things they are trained to do'' (Anthony, 1988). Chapter 10 contains a description of emergencies that may affect a high-rise building and ways they may be handled.

Evacuation and Relocation

This section of the Building Emergency Procedures Manual outlines the evacuation and relocation procedures formulated for the building during certain emergencies. Evacuation and relocation are defined earlier in this chapter, under ''Effective Evacuation or Relocation Measures.'' The authority having jurisdiction over the building usually will establish the policy by which occupants will evacuate or relocate during a particular emergency. For example, in the city of New York, if a fire occurs in a high-rise building, the fire floor and the floors immediately above are the most critical areas for rapid evacuation.[†] However, in Los Angeles, if a fire occurs in a high-rise building and it is serious enough to evacuate one floor, five[‡] floors are evacuated

[*]No emergency plan can possibly cover all eventualities. For example, during an emergency there may be failure of critical life safety systems (as was the case during the 1993 New York World Trade Center bombing when vital communication and lighting systems were lost due to the explosion). Therefore, it is important that staff and occupants are aware that they may need to make independent decisions as to the best course of action.

[†]''In the event that a fire or smoke condition exists, occupants will evacuate at least two floors below the fire floor, re-enter the [building at that] floor, and wait for instructions'' (Jennings, 1995, p. 297).

[‡]Also recommended in the 2002 NFPA video, *High-Rise Evacuation* (National Fire Protection Association, Quincy, MA, 2002).

(commonly referred to as the ''Rule of 5''): the fire floor, two above it for safety, and two below it (so that the second floor below the fire floor can be used as a staging area for fire department operations). Occupants on these five floors are relocated down five floors and are thus *at least three floors from the fire floor*; if the fire is on or below a floor that is six floors from street level, the occupants usually will be evacuated from the building. Figure 11.3 shows the floors from which occupants are usually evacuated or relocated during a fire situation in a Los Angeles high-rise office building.

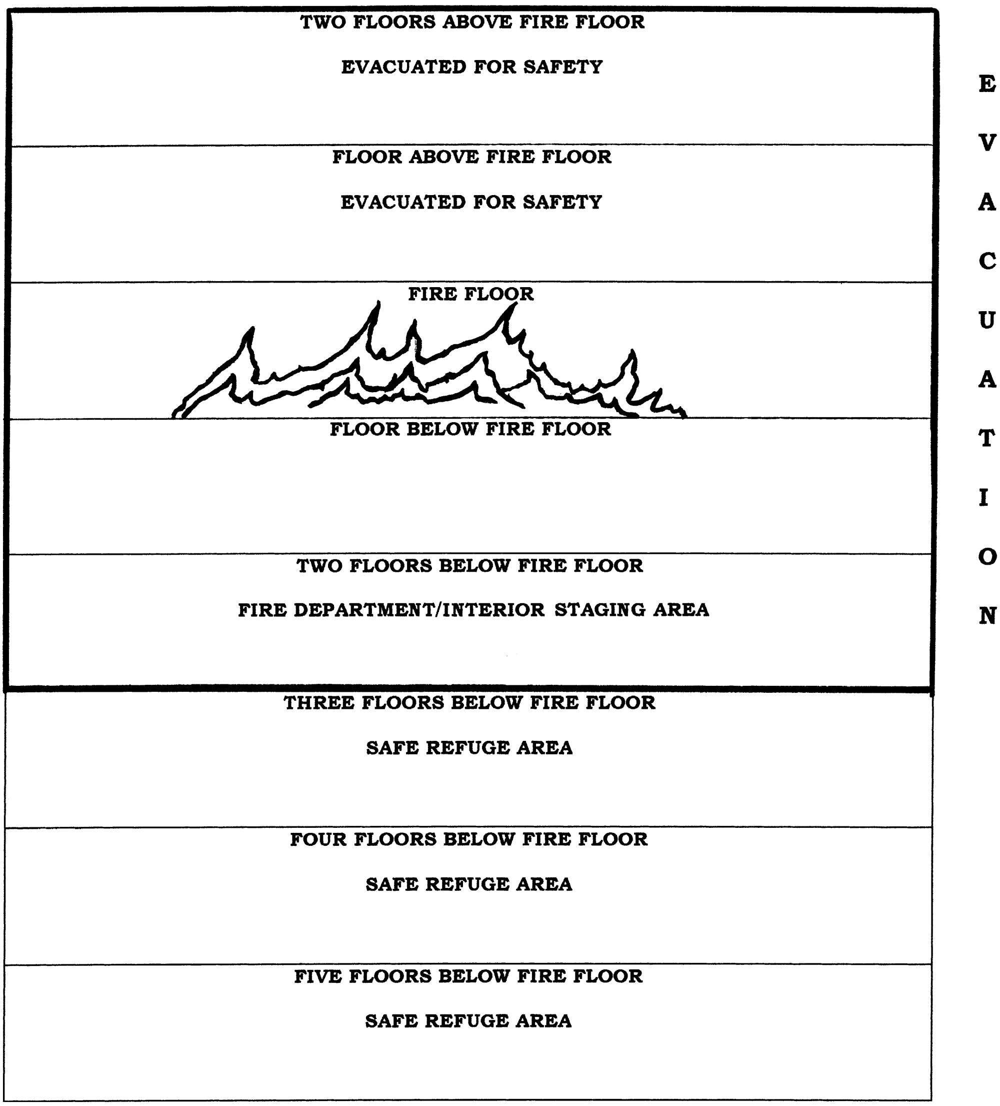


Figure 11.3 Floors from which occupants are usually evacuated or relocated during a fire situation in a Los Angeles high-rise office building.

Once the occupants of the involved floors have been relocated, the decision whether to evacuate them further, using stairwells or elevators, or whether additional floors need to be evacuated will be determined by building management, the Fire Safety Director, or the fire department if they have arrived. Total building evacuation usually is ordered only by the fire department. Such an evacuation would take considerable time. It is estimated that it takes over an hour to evacuate a 50-story building (Taubman, 1974). Of course, the time to evacuate any building will depend largely on the building population at the time of evacuation and on the nature of the event that caused the evacuation.[*]

In the 1993 NFPA video *High-Rise Evacuation*, it is stated that it usually takes occupants, moving at a reasonable pace, a total of approximately 10 seconds to move down one floor in the stairwell of a high-rise building, allowing one second at each stairwell landing between floors. This means that for someone on the 36th floor of the theoretical high-rise Pacific Tower Plaza, it would take approximately 6 minutes to descend down the stairwells to the ground level if the person did not slow down or stop for a rest when tired. This statistic is for one occupant descending; a group of people will undoubtedly take longer.

It is advisable to go downward in a building during a fire; it is necessary or more desirable to go to an upper floor or to the roof only if the lower floors or stairwells are destroyed or untenable because of heat or smoke. The problem with occupants relocating to the roof, particularly in substantial numbers, is that once there they may need to be evacuated from the roof itself. If the building has a helipad or heliport (Figure 11.4), as some modern high-rise buildings do, there is not only the problem of obtaining a helicopter, but also of it landing safely to pick up occupants. During serious building fires, air turbulence and updrafts are caused by smoke and heated air.[†]

Evacuation of Individuals with Disabilities[‡]

Individuals with temporary or permanent disabilities, or other conditions that would require them to obtain assistance during an evacuation, require special consideration during evacuation or relocation. The Americans with Disabilities Act (ADA), Title 42, U.S. Code, Chapter 126, Section 12102, defines an individual's *disability* as ''a physical or mental impairment that substantially limits one or more of the major life activities of such individual.''

During an evacuation or relocation in a high-rise building, individuals who will require assistance from others may include persons confined to wheelchairs; persons dependent on crutches, canes, walkers, and so on; persons recovering from surgery; pregnant women; persons with significant hearing or sight impairment; extremely obese persons; elderly persons; children; persons with mental impairments; and persons who may have become

[*]In the 1993 World Trade Center bombing, ''the median evacuation time from the 90th floor [of Tower 1] was 2½ hours. No one evacuated in less than 2 hours'' (Prouix and Fahy, 2002).

[†]In the 1980 MGM Grand Hotel fire an estimated 300 persons were evacuated from the roof by helicopter. Favorable factors in the MGM helicopter evacuation operation included clear weather, daylight hours, and an unusual availability of the participating Air Force helicopters (Best and Demers, January 1982, p. 31). During the 1988 First Interstate Bank Building blaze, eight persons went to the roof and all were successfully airlifted to safety from the roof of this 62-story high-rise.

[‡]The previous term *handicapped* has been replaced.

Figure 11.4 Helipad of a modern high-rise building. Photograph by Roger Flores.

incapacitated as a result of the emergency. After the 1993 New York World Trade Center bombing, *Time* reported that two friends carried a woman in a wheelchair down 66 stories and that a pregnant woman was airlifted from a tower roof (''Fire and smoke,'' 1993, p. 17).

A listing of such individuals' names, locations within the building, telephone numbers, type of disability, and the names of assigned assistance monitors should be provided ahead of time to building management with the understanding that such information is confidential and is to be used only to facilitate safe and rapid evacuation or relocation during emergency conditions.

Areas of Rescue Assistance

Title III of the ADA requires the establishment of ''areas of rescue assistance'' in all nonsprinklered buildings with occupied levels above or below the level of exit discharge. *Exit discharge* is defined by the NFPA as ''that portion of a means of egress between the termination of an exit and a public way'' (NFPA *Glossary of Terms*, 2001). An *area of rescue assistance* is defined by the ADA as ''an area that has direct access to an exit, where people who are unable to use stairs may remain temporarily in safety to await further instructions or assistance during emergency evacuation'' (Cummings and Jaeger, 1993, p. 46).

Wayne ''Chip'' Carson (1993, p. 2), in the NFPA *Fire News*, states:

> These areas may include:
>
> - a portion of a landing within a smokeproof stairway.
> - a portion of an exterior exit balcony adjacent to an exit stairway. If there are openings to the building within 20 feet of the area of rescue assistance, they must be protected by 45-minute opening protection.

- a portion of a one-hour fire resistance rated corridor located immediately adjacent to an exit enclosure.
- a vestibule located immediately adjacent to an exit enclosure.
- a portion of a stairway landing.
- an area separated by a smoke barrier when approved by the local authority having jurisdiction.
- a pressurized elevator lobby.
- a horizontal exit.

Once the area of rescue assistance has been reached, assistance monitors and the individual with the disability have two options: (1) dispatch someone to relate the situation to the building Fire Safety Director, building management, security, engineers, or—in the case of a fire emergency—the fire department, and await their assistance; or (2) once all occupants have been evacuated from the involved floors and moved past, the assistance monitors may move the individual with the disability to the designated safe refuge area inside or outside the building.

Information covering basic methods of evacuating individuals requiring assistance during an emergency evacuation is provided in Figures 11.5 and 11.6.

Mel Harris (1995), Fire Protection Engineer of the General Services Administration (GSA), made the following comments regarding the emergency evacuation of disabled workers:

> The illustrated carries [in Figures 11.5 and 11.6] are not easy to perform. Not everyone has the physical strength to either carry another person or to participate with a partner in two-person carries. At best, going down stairs is difficult because of the ease with which one's grip can slip and allow the disabled person to be dropped. For many people it is very difficult to keep their balance while carrying the dead weight of a person.

The suggestions that follow, also from Harris (1995) with minor revisions, should be considered:

1. These carries should only be performed by trained personnel. Extensive initial training on how to safely perform them should be followed by retraining on a regular and periodic basis to ensure that personnel maintain their skills. Only in the most dire emergency should untrained co-workers attempt to evacuate the disabled. This is particularly critical in going down stairways.
2. The basic objective of evacuating a disabled person should be to have the disabled assistance monitors remove her or him to the nearest safe location. The monitors should stay with the disabled person, report their location to the floor warden, Building Fire Safety Director, or other designated member of the Building Emergency Staff Organization, and then wait for the fire department to accomplish the actual evacuation if they decide it is required.
3. If the building is equipped with automatic sprinklers, usually the disabled need only be moved to an adjacent safe area or floor, rather than being carried out of the building.
4. The evacuation procedures should be reviewed with disabled persons prior to an emergency so that they will know what assistance to expect during drills and actual emergencies.

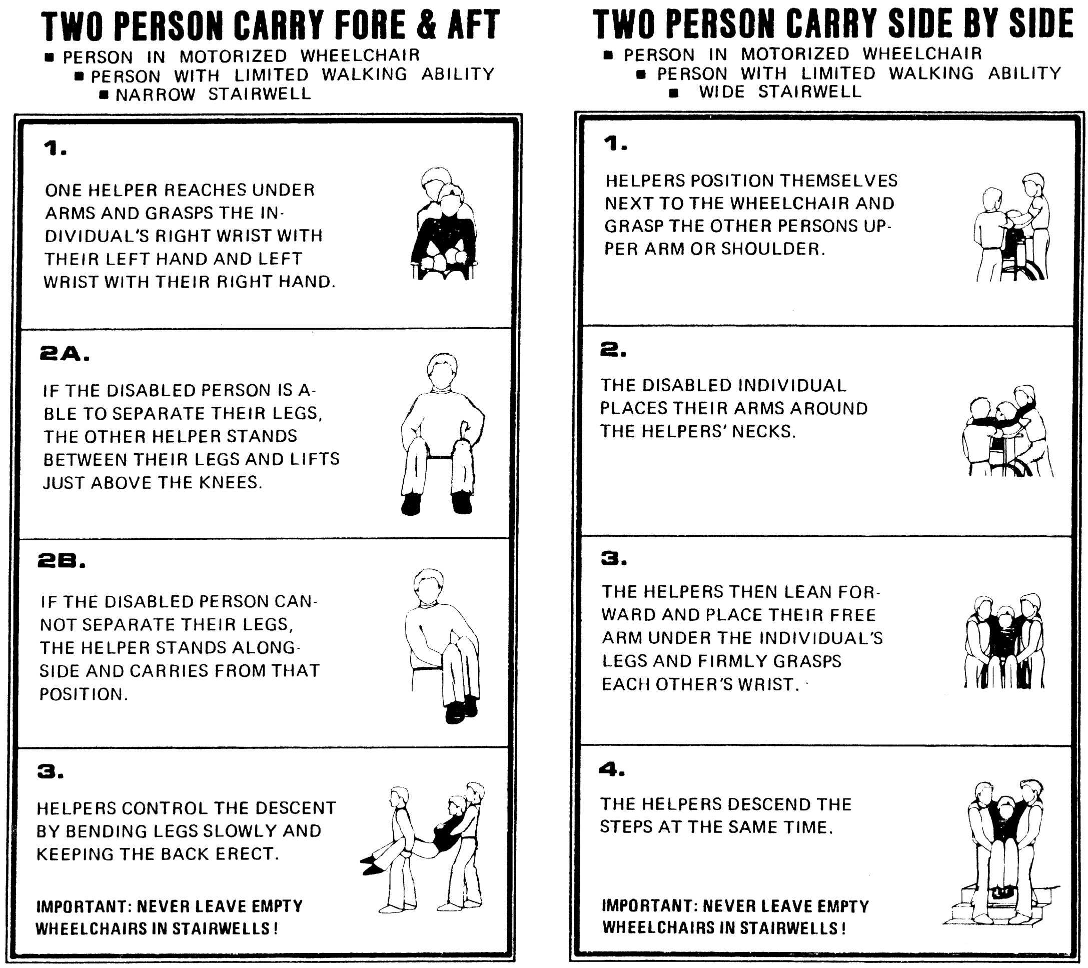


Figure 11.5 Two-person carries. Reprinted with permission from ''Emergency Evacuation Procedures for Disabled Individuals,'' developed through the cooperative efforts of the Los Angeles Fire Department and Joni and Friends.

5. Although elevators are not used for general population evacuation, they may, when the fire department directs,* be safely used for evacuating the disabled in some buildings. There is much discussion on this concept in

*''It is standard operating procedure in high-rise structures for fire fighters to use elevators not only to carry equipment for fire-fighting or evacuation purposes, but also to deliver fire personnel to non-fire floors'' (Donoghue, 1997, p. 8-56). However, ''elevators operated under Phase II recall continue to fail and trap firefighters'' (Routley, 1993). It is the author's opinion that when elevators are used to transport people to a fire or to investigate a fire alarm, this should be restricted to those elevator banks totally separate from the bank that serves a fire floor (i.e., the group of elevators not involved in the fire nor in the primary path of smoke flow). In the event that a fire is located in an elevator machine room, however, no elevator being operated by that machine room would be safe to use.

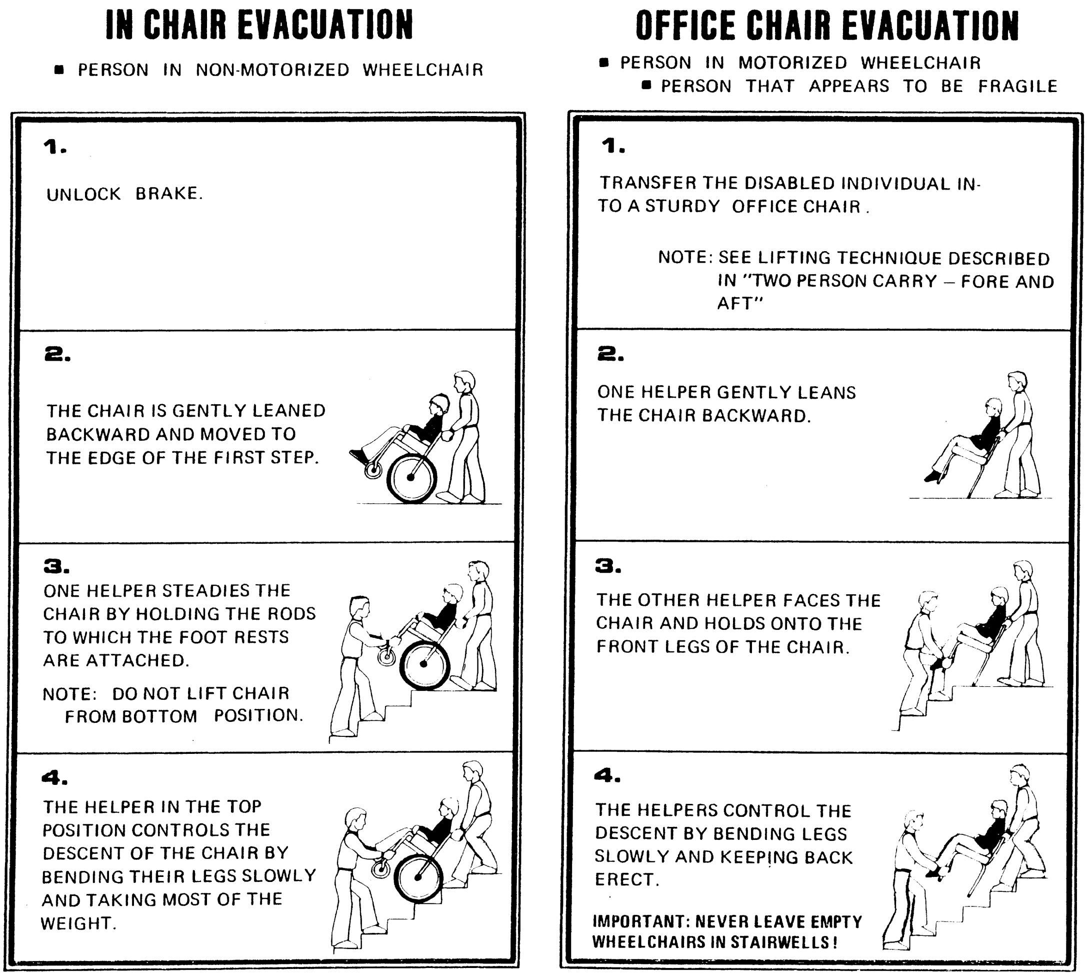


Figure 11.6 In-chair evacuation carries. Reprinted with permission from "Emergency Evacuation Procedures for Disabled Individuals," developed through the cooperative efforts of the Los Angeles Fire Department and Joni and Friends.

the fire protection field today.* Using elevators for disabled evacuation would require training and close coordination between the local fire department and the Building Emergency Staff Organization.

6. The AOK Medi-Chair is a convenient and safe device to evacuate the disabled down stairways. Although there are other evacuation chairs available, the AOK provides a unique belt mechanism to provide a controlled descent down steps. This chair is on the GSA Supply Schedule for ease in purchasing by government agencies.

---

*Research has been previously conducted by the National Institute of Standards and Technology (NIST) and sponsored by GSA. A discussion of this research is published in *Feasibility and Design Considerations of Emergency Evacuation by Elevators*, NISTIR 4870.

Accounting for all Occupants

Once all affected occupants have been evacuated or relocated there needs to be a method to determine if the unsafe areas are truly vacated. This can be achieved by taking a ''head count'' of occupants at the safe refuge area, or by conducting a thorough search of all unsafe areas from which they have come.

The head count method usually is not a reliable technique. Workers may be out of their office for an outside appointment or away from work because of illness or vacation when the evacuation or relocation occurs—hence when a head count is taken, these individuals may be incorrectly listed as missing. Another problem with this approach is that visitors or temporary workers in the tenant space at the time of the evacuation may still be trapped inside but will not show up as missing during the head count. If the evacuation involves a large number of people, there also may be difficulty in physically grouping together all evacuees to perform a head count.

A thorough search of all areas is a more reliable technique for determining if all occupants have vacated an area in a multiple-tenant/multiple-use high-rise office building. By focusing on the evacuated areas themselves, it can be positively determined if anyone has remained behind. Closed areas—computer rooms, data centers, conference rooms, libraries, restrooms, and break areas—are locations that may be overlooked in a hurried evacuation. The presence of well-prepared floor wardens, as described earlier, will alleviate much of the risk of someone accidentally being left behind in an evacuation.

Building Emergency Systems and Equipment

This section of the manual outlines the building emergency systems and equipment in the building. It should include an overview and description of each system, an account of how the systems operate under normal and emergency conditions, and how system components are related and connected. Photographs and diagrams are invaluable in effectively describing building fire life safety systems and equipment. The information should reflect the type of systems or equipment and their location within the building, the emergency function of systems and equipment, and the method of operating and resetting them. The systems and equipment should include the following:

- Voice communication and building PA system
- Fire department voice communication systems
- Public telephone for fire department use
- Stairwell intercom systems
- Fire detection and alarm system annunciator and control panels
- Manual fire alarm stations (sometimes called *manual fire alarm boxes*, *manual pull stations,* or *manual pull alarms*)
- Automatic detection systems (smoke detectors, heat detectors, and gas detectors)
- Automatic sprinkler systems, sprinkler control valve and water-flow detector annunciator panels and fire pump status indicators, and standpipe and hose systems
- Other fire protection equipment and system controls

- On-site and off-site monitoring arrangements of fire detection and suppression equipment
- Air-handling system controls and status indicators
- Elevator status panel displaying elevator operations
- Emergency and standby power systems
- Controls for simultaneous unlocking of stairwell doors locked from the stairwell side
- Utility service (gas, electrical, water) shutdown locations, tools, etc.
- Fire department lock box or rapid entry key vault
- Automated external defibrillators

Included in this section should be a description of the building—for example:

> Pacific Tower Plaza is a prestigious, multiple-tenant, multiple-use high-rise complex used primarily for commercial office purposes. It is located in Toluga Hills, a major downtown financial district. It occupies one half of the city block bounded by Mount Waverley, Poppyfields, and La Perouse Boulevards and is located in proximity to the Southwestern Freeway. A high-rise residential building, a low-rise hotel, and a high-rise office building surround it. Pacific Tower Plaza consists of a fully sprinklered 36-story office tower with a triple-level under-building parking garage. The tower has 600,000 square feet of rentable office space, 7000 square feet of rentable retail space, and 6000 square feet of rentable storage space. The approximate size of each floor plate is 18,500 square feet. The perimeter of the building consists of sculptures, fountains, an open-air restaurant, and large planters containing flowers and small trees. The entrance to the building is through a large main lobby. The building has an approximate population of 2400 occupants and 500 daily visitors. The on-site parking structure can accommodate up to 600 cars and connects to a subterranean pedestrian tunnel under Mount Waverley Boulevard.
>
> The tower of Pacific Tower Plaza consists of steel-frame and concrete construction with metal stud partitions. It has a conventional curtain wall consisting of glass in aluminum frames. The structural steel frame supports lightweight concrete floor slabs resting on metal decks atop horizontal steel beams, which are welded to vertical steel columns. The building is supported on a foundation of structurally reinforced concrete. The tower is designed with a concrete-reinforced center core which houses the electrical, plumbing, and communications systems; the heating and air-conditioning (air supply and return) shafts; 17 passenger elevators, one service/freight elevator, and three parking shuttle elevators; and two major enclosed stairwells. Both stairwells provide egress to the street level and access to the roof. The stairwells are pressurized and protected by fire-rated doors and walls.
>
> The Plaza has 24-hour security staff, seven days per week, and engineering staff present during normal business hours, Monday to Friday.

The manner in which systems and equipment operate in relation to each other also needs to be described. For example, see ''Controls in Elevator Lobbies'' in Chapter 6 for a description of how various systems usually are designed to respond to the activation of an elevator lobby smoke detector. A table detailing the sequence of operation of life safety systems, like the one shown in Table 6.1, is an invaluable tool in outlining building systems and equipment and how systems interrelate.

This section also should include building drawings and plans detailing site plans, floor layouts, evacuation routes, stairwell and elevator configurations, and so on. Figures 11.7 through 11.14 show these diagrams for the hypothetical Pacific Tower Plaza.

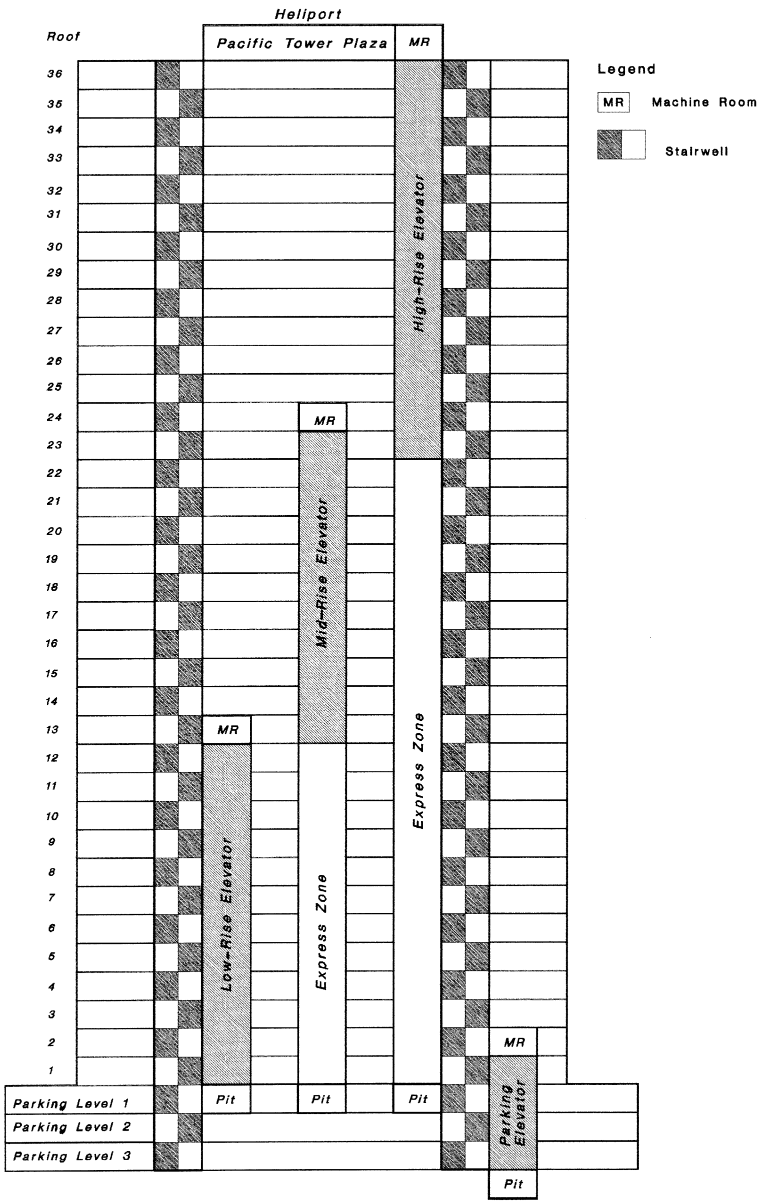


Figure 11.7 Building elevator shafts and stairwells.

Emergency Operations Center

As part of the Building Emergency Plan, there should be a designated area, or Emergency Operations Center (EOC), where building emergency staff can assemble to receive information, make decisions, and otherwise coordinate the handling of an emergency. For many buildings, depending on the incident, this area will be the Fire Command Center, the Security Command Center (if appropriate), or other locations as considered necessary by the Fire Safety

Text continued on p. 435

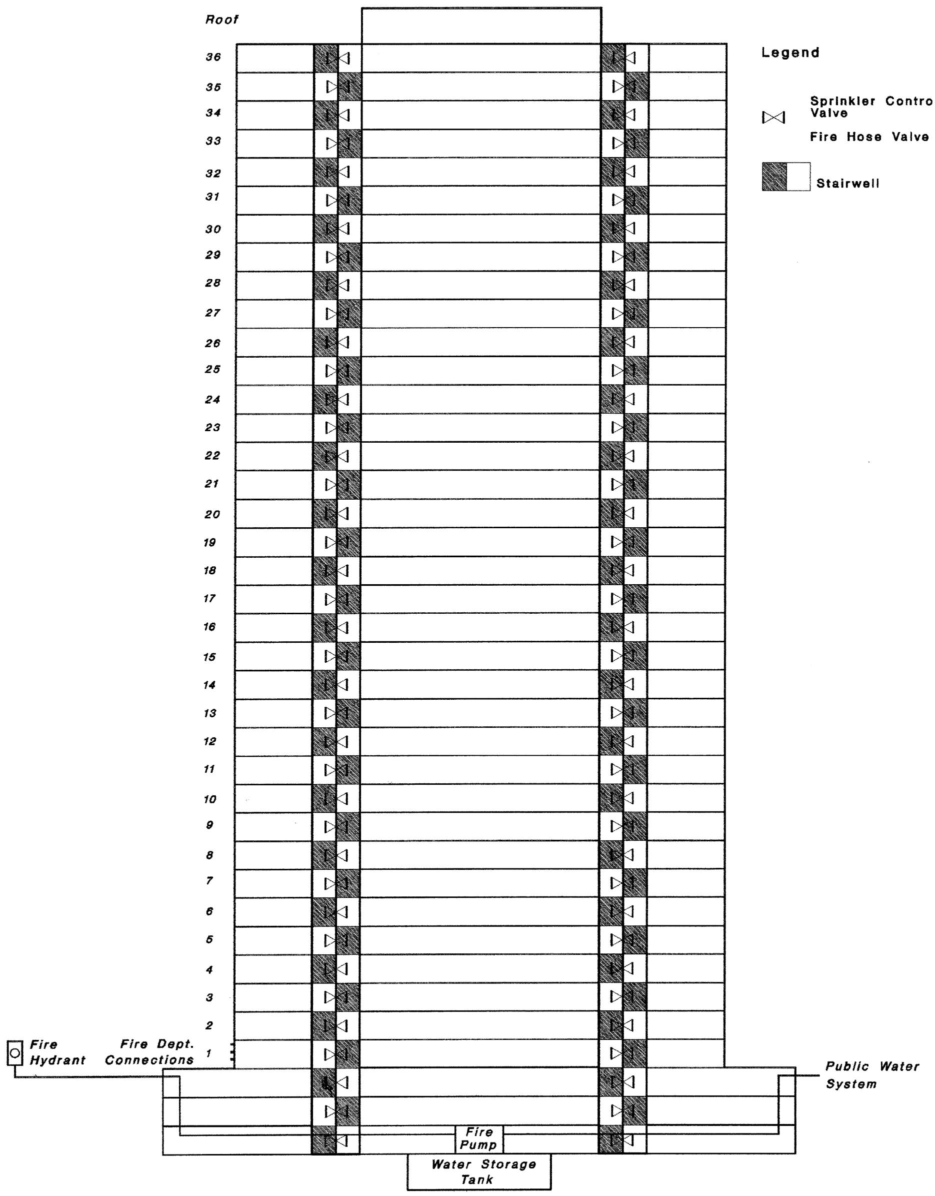


Figure 11.8 Fire protection riser diagram.

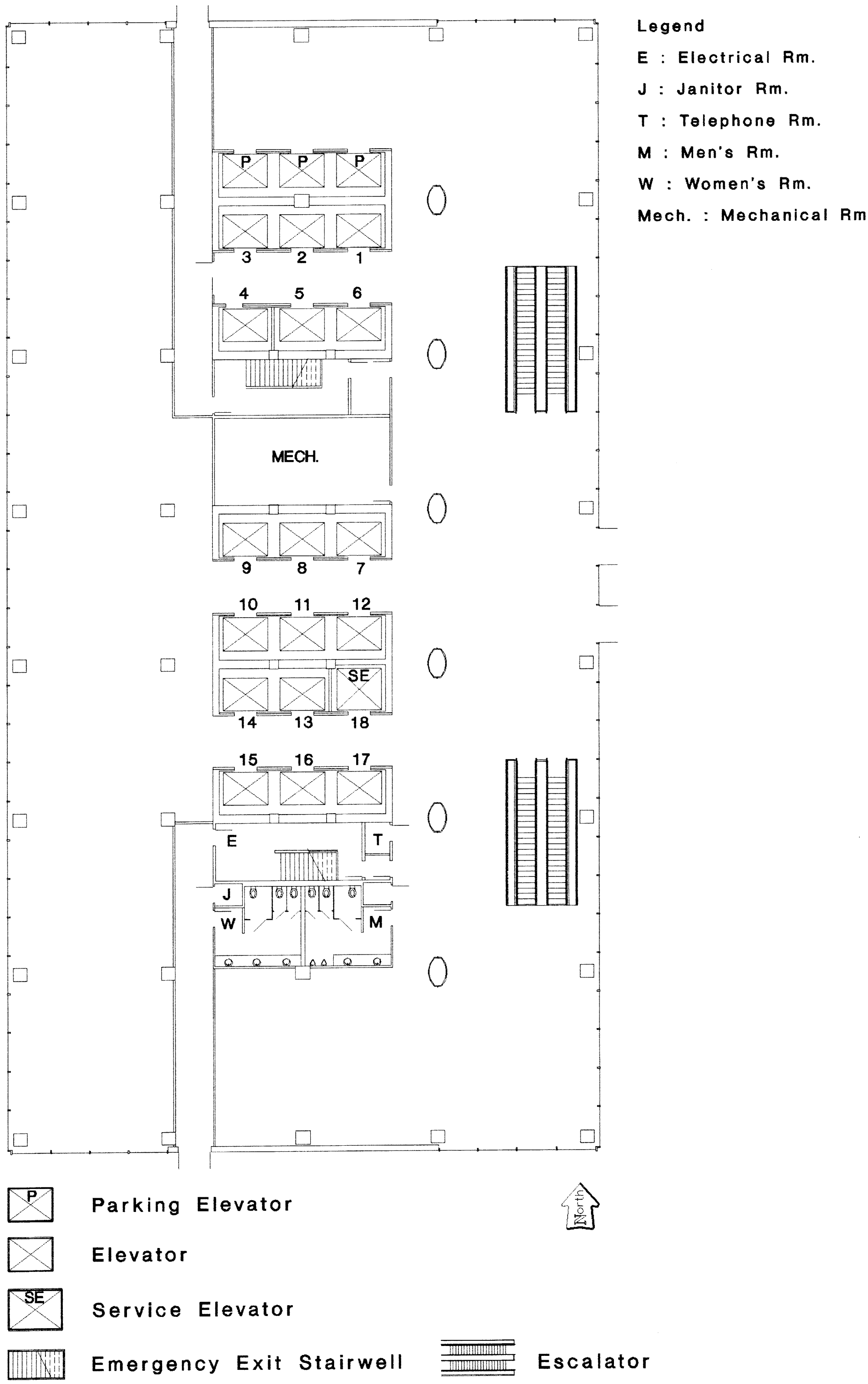


Figure 11.9 Ground floor plan.

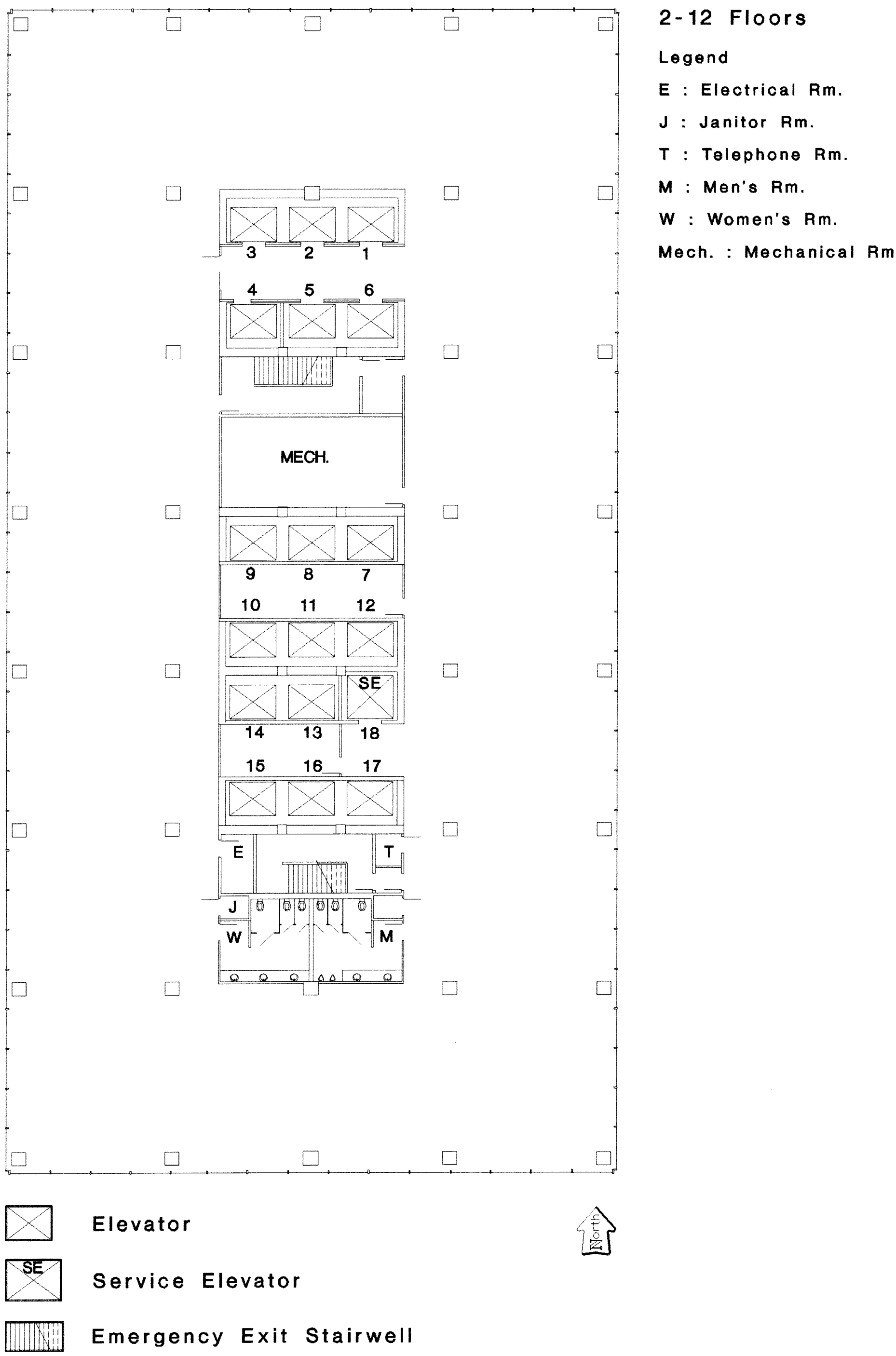


Figure 11.10 Low-rise floor plan.

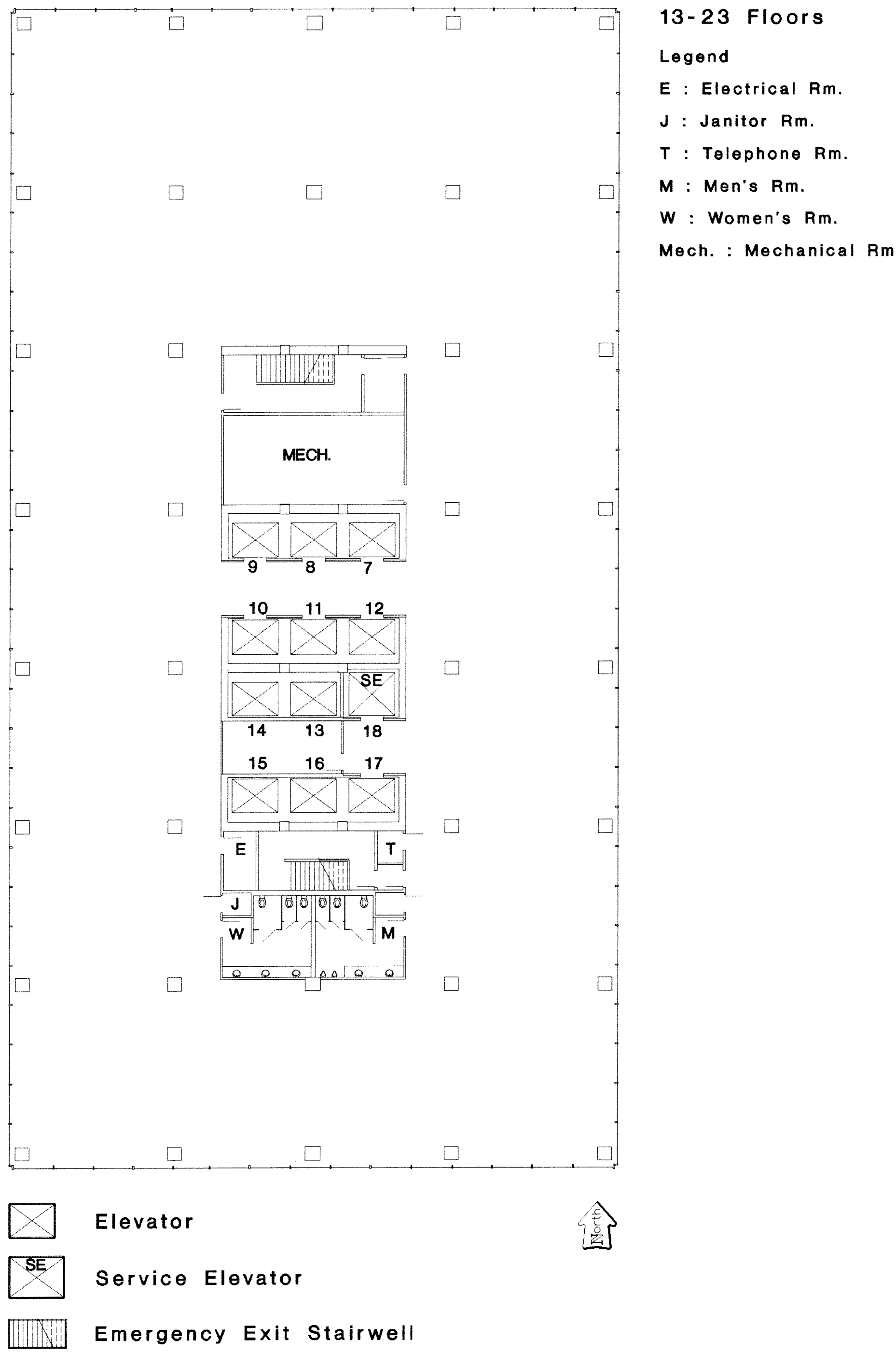


Figure 11.11 Mid-rise floor plan.

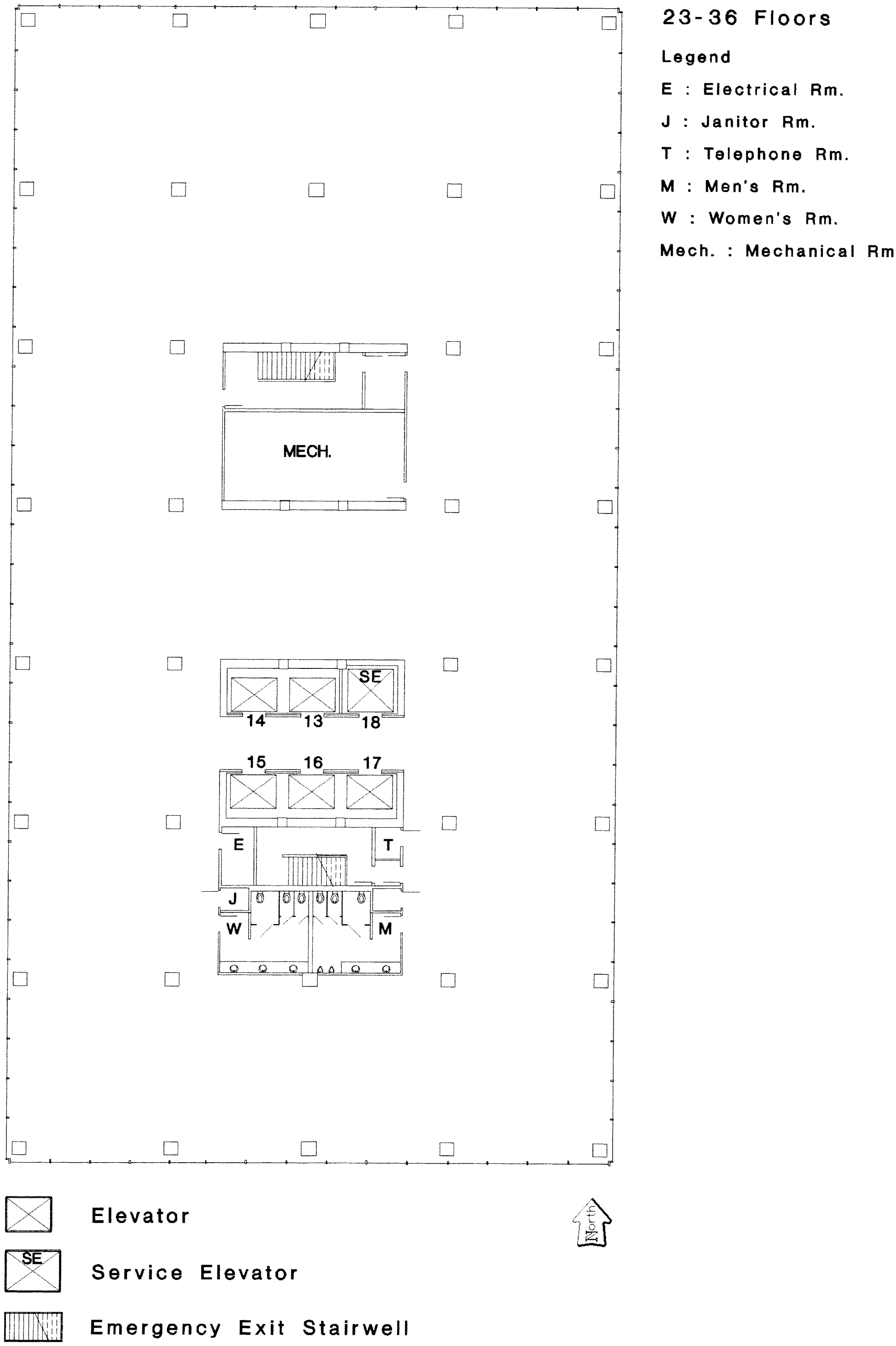


Figure 11.12 High-rise floor plan.

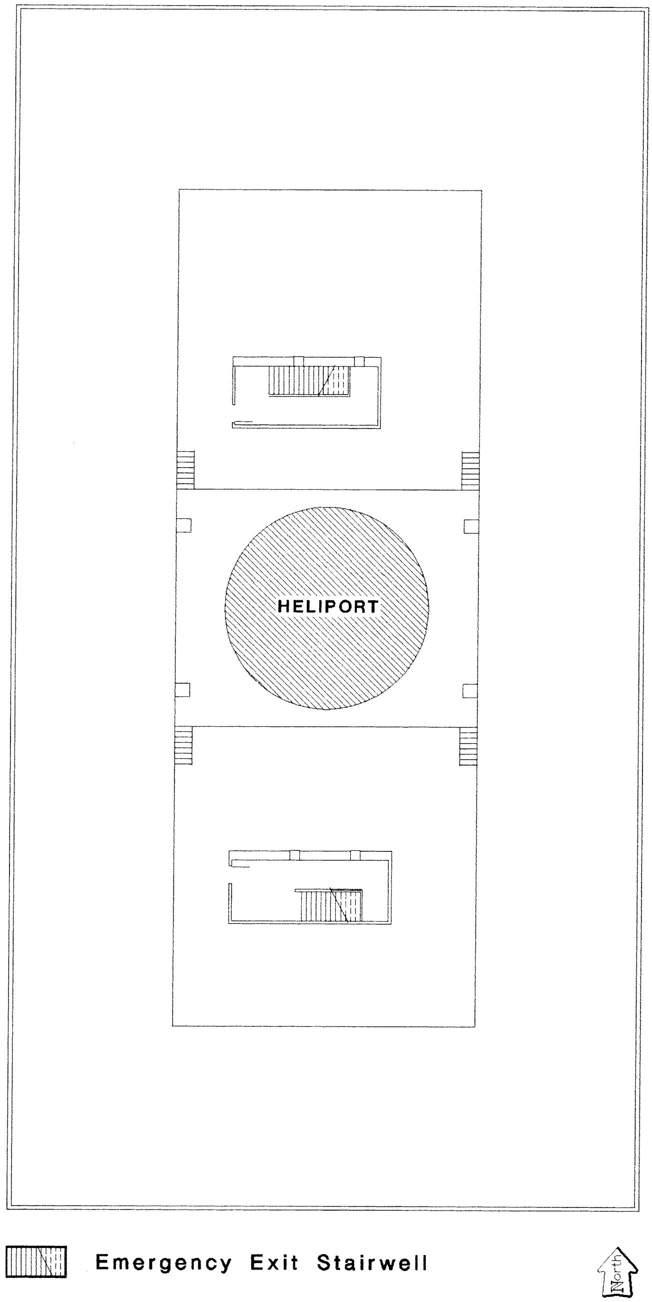


Figure 11.13 Roof floor plan.

Director. The Fire Command Center, described at the beginning of Chapter 6 is useful for most emergencies, particularly those that are fire-related, and those that require voice communication to the occupants of the building. However, in some situations, such as bomb threats and medical emergencies, the EOC is

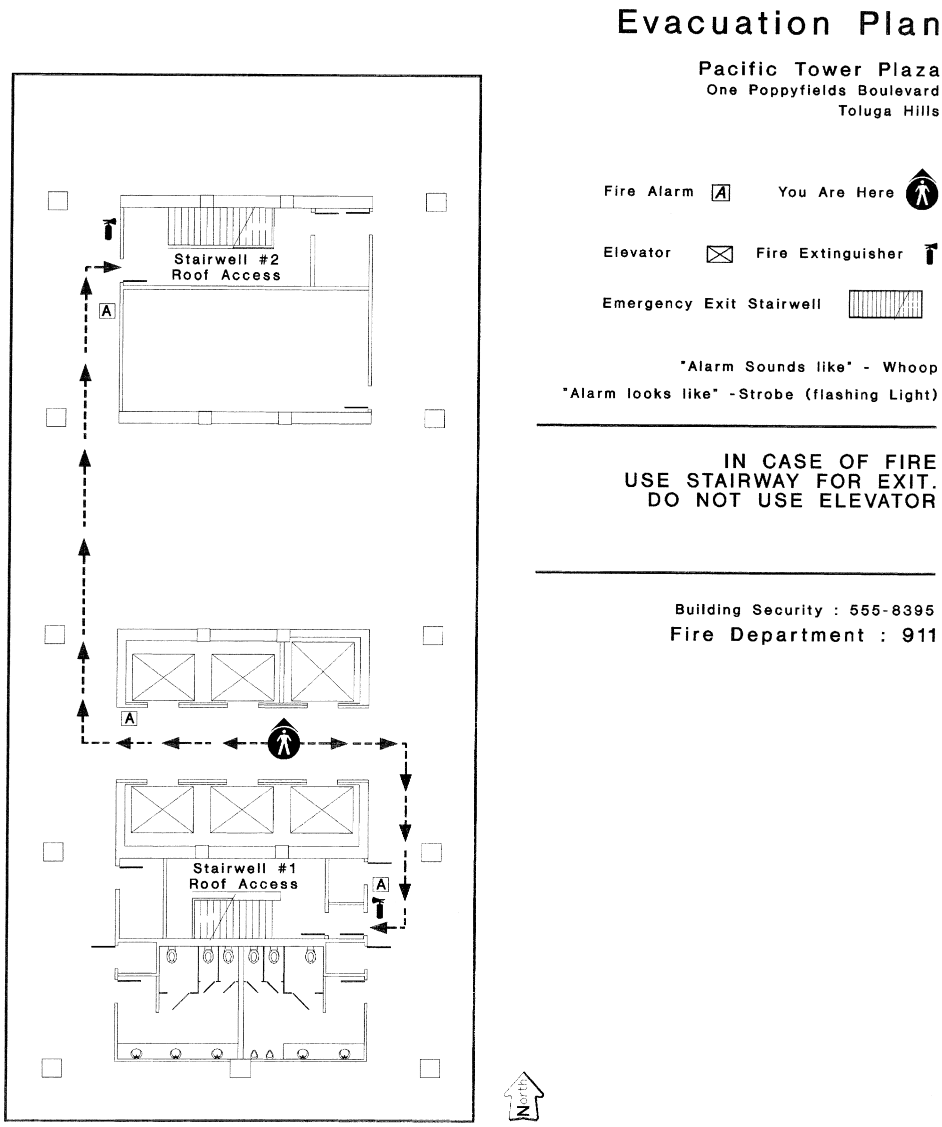


Figure 11.14 Sample floor evacuation plan.

more likely to be the Security Command Center or an area on a tenant floor designated at the time of the incident.

In a major emergency during which there is likely to be a large congregation of building emergency staff, the Fire Command Center may not be big enough to accommodate the EOC, so an alternate location should be found in advance. Some large high-rise buildings have a special room fully equipped and ready to be activated as the EOC. It may contain the following equipment:

- Communications equipment: multiple telephones, portable two-way radios, bullhorns or megaphones, portable telephones, radio-telephones, pagers, radios including CB and other licensed bands, televisions, fax machines, etc. (duplicate building PA, elevator communication, and intercom systems may also be provided)
- Tools for documenting the emergency incident: word processors, logs, notepads, tape recorders, digital cameras, video cameras, etc.
- A copy of the Building Emergency Procedures Manual and site plans and building floor plans that may, for convenience, be enlarged and displayed on walls
- Comprehensive contact lists for vendors and contractors who provide recovery services and materials, including general contractors; architects; plumbing, electrical, mechanical, and fire sprinkler contractors; generator technicians; security providers; janitorial and waste disposal services; companies providing materials to board up windows; etc.
- Duplicate building security and fire life safety systems such as building and elevator keys, CCTV, and video recorders
- An emergency generator that powers the Emergency Operations Center independent of building primary or emergency power systems
- Emergency supplies (or lists of emergency supply locations in accessible areas and various floors of the building)—bottled water, canned and dry food, first aid kits, sleeping bags, blankets, stretchers, portable emergency lighting, flashlights, batteries, safety gloves, heavy-duty plastic trash bags (to line toilets if sewer services are interrupted), body bags, hard hats, protective goggles, dust masks, and light rescue equipment such as shovels, crow bars, and heavy-duty gloves

Evacuation Drills

Evacuation drills—commonly called fire drills—are an important part of the Building Emergency Plan and as such they should be outlined in the Building Emergency Procedures Manual. Fire drills are an invaluable tool to train, instruct, reinforce, and test the preparedness of the emergency staff, occupants, and floor wardens to respond to the emergencies that are most likely to occur in the building. They also can be used to test the performance of building emergency systems and equipment.

Because fire safety is such a major concern of high-rise building owners, managers, and the local authority having jurisdiction, state and local laws specify intervals at which fire drills (or, as referred to in the NFPA 101, *Life Safety Code*, ''emergency egress and relocation drills'') shall be conducted. ''In the United States, the Life Safety Code first included requirements for fire drills in office occupancies in 1966'' (Jennings, Charles, personal correspondence with John L. Bryan, dated June 6, 1994). The NFPA recommends that emergency egress and relocation drills,

> Shall be held with sufficient frequency to familiarize occupants with the drill procedure and to establish conduct of the drill as a matter of routine. Drills shall include suitable procedures to ensure that all persons subject to the drill participate. (NFPA 101, 2000, 4.7.2)

For example, fire codes in the city of New York require established high-rise office buildings to perform fire drills every 6 months.* The city of Chicago requires drills ''twice annually for buildings over 780 feet, once for buildings over 540 feet tall'' (Archibald, Medby, Rosen, and Schachter, 2002, p. 47), whereas GSA buildings are required to conduct two fire drills a year, and the city of Los Angeles requires annual drills (however, Los Angeles is presently drafting a city ordinance to require evacuation drills in high-rise buildings to be conducted every 6 months).

To be successful, fire drills should be designed in cooperation with the local authorities, planned ahead of time, and thoroughly documented. This documentation is used to analyze the training readiness of all persons involved and, like all documented life safety training, can be used as legal evidence (especially in the event of litigation following a major incident that results in injuries or loss of life) to prove that the building owner or manager has taken steps to ensure the safety of occupants. Tenants, emergency staff, and drill monitors all need to prepare adequately for fire drills as follows:

1. *Tenants*. Tenant representatives and floor wardens should be informed of the dates and times fire drills have been scheduled for their respective floors. All tenant employees should be told of the upcoming drill and asked to review emergency procedures. Floor wardens should ensure that their floor response personnel are in place and prepared for fire drills—to assist in this preparation, meetings may be conducted to review evacuation procedures.
2. *Building Emergency Staff*. All staff participating in the drills should rehearse their duties, including performing special drill announcements. The local fire department should be telephoned before the drills start and immediately after the drills have been completed. These calls reduce the chance that the fire department will unnecessarily respond to a person mistaking the drill for an actual fire and making an emergency call to them.
3. *Drill Monitors*. There should be drill monitors stationed at strategic locations throughout the drill floors to observe and document on a *Fire Drill Checklist* the conduct of participants from the time the fire alarm first is activated.
4. After the evacuation or relocation has occurred, all evacuees should be grouped together at the safe refuge area and asked to sign a *Fire Drill Register*. The Fire Safety Director should verbally critique the performance of the drill before the participants are directed to return to their offices.

Appendix 11-1 includes samples of a *Fire Drill Notification* letter, fire drill announcements, a *Fire Drill Checklist*, a *Fire Drill Register*, and a *Bomb Threat Checklist*.

On completion of drills, the Fire Safety Director should produce a report. This report should include a brief goal statement; a description of how the drills were conducted; an overall review of how building fire life safety systems performed; an overall review of how floor wardens, occupants, and building emergency staff performed; and recommendations on training improvements.

*In the city of New York, fire codes for office buildings require that ''Fire drills shall be conducted, in accordance with the Fire Safety Plan, at least once every three months for existing buildings during the first two years after the effective date of these rules, or for new buildings during the first two years after the issuance of the certificate of occupancy. Thereafter, fire drills shall be conducted at least once every six months'' (RCNY 1625, 6-30-91).

Copies of all documentation should be included with the report. After these drills management of some buildings determine which single-floor tenant and multiple-tenant floors performed the best and then present those involved with awards acknowledging their achievements.

A word of caution: Fire emergencies are not the only type of emergency for which drills should be conducted. To have an effective fire life safety program, staff and occupants should be kept ready to handle all types of emergencies that are likely to occur at their building.

Documentation and Record Keeping

This section of the Building Emergency Procedures Manual contains documentation, records, and forms (see samples in Appendix 11-1) for all activities and training conducted under the Building Emergency Plan, including training for building emergency staff (building management, Fire Safety Director, Alternate Fire Safety Director, engineers, security, janitors, parking staff, etc.), building occupants, and floor wardens.

Design of the Manual

The Building Emergency Procedures Manual should be in a three-ring binder so that outdated information can be removed easily and revised material can be added. Pages should be numbered and dated—this alleviates confusion when changes or revisions are made. Each section outlined in the table of contents and each emergency identified in the manual should be tabbed for easy identification and immediate reference. Use of colored tabs can aid reference—for example, a red tab for ''Emergency Telephone Numbers.''

The manual needs to be designed so that material from it can be taken out and used for the training and instruction of building management; the building Fire Safety Director; engineering, security, parking, and janitorial staff; floor wardens; floor response teams; and occupants. Copies of the Building Emergency Procedures Manual should be placed in the Main Office of the Building (or Building Management Office), the office of the Fire Safety Director, the Fire Command Center, the Security Command Center (if appropriate), the office of building engineering, and other locations as deemed necessary by the Fire Safety Director. Copies of Floor Warden Manuals should be given to each tenant, floor warden, and alternate floor warden. Occupant documentation should be distributed to every person in the building. Of course, copies of all these items should be submitted for approval to the local fire authority having jurisdiction.

It cannot be stressed enough that the structure of the Building Emergency Procedures Manual just described is only an example. Every site and high-rise building is different, and plans vary according to state and local laws and the requirements of the authority having jurisdiction. Every emergency manual should be periodically reviewed (at least annually, and in some jurisdictions every 6 months) and updated to incorporate any changes or modifications. When these changes are made, the authority having jurisdiction that approved the manual should be notified in writing, and all Building Emergency Procedures

Manuals in existence should have the changes incorporated into them. The outdated material should be retained indefinitely as part of the building's fire life safety records in case it is needed later as evidence for legal purposes.

Occupant Documentation and Training

Occupant Documentation

Booklets, brochures, pamphlets, or leaflets (or possibly a computer disk) are often used to train occupants. These materials are designed to contain the correct procedures to be followed in any emergency likely to happen in the building. Some buildings limit the documentation to fires, fire alarms, bomb threats, medical emergencies, and natural disasters relevant to the location. Figure 11.15 is a sample occupant safety brochure for Pacific Tower Plaza, the hypothetical high-rise, which is located in an area where earthquakes are likely to occur.

Many of these brochures include floor evacuation plans that show the building core, perimeter, stairwells, elevators, and every wall that faces every exit route; exit routes to the appropriate stairwells; symbols depicting the location of fire equipment and manual fire alarm devices; floor number; fire department and building emergency telephone numbers; what stairwells have roof access; and what the fire alarm looks and sounds like. (Refer to Figure 11.14 for a sample floor evacuation plan.) The brochure may also include a *Certificate of Occupant Training* (see Figure 11.16) to be filled out by the occupant receiving training, and returned to the floor warden or building Fire Safety Director for record keeping.

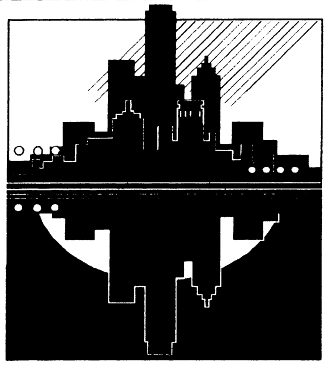
Occupant Training

A class that is taught by a qualified person (preferably the building Fire Safety Director) is an invaluable way to inform high-rise building occupants of what to do in the event of a fire or other emergency. The Los Angeles Municipal Fire Code, for instance, requires all high-rise buildings to instruct occupants annually on the procedures to be followed in a fire, earthquake, or other emergency; instruction of all new occupants is required within 14 days of their assuming occupancy in the building. Documentation of this instruction needs to be maintained by the Fire Safety Director and be available for inspection by the Chief of the Los Angeles Fire Department. To satisfy this legal requirement, many of the city's 750-plus high-rise buildings conduct one-hour occupant training classes every 2 weeks.

In such a class, it is important to explain fire life safety legal requirements, the building's emergency systems and equipment, and relevant emergency procedures. The instructor must be thoroughly familiar with the building in which the occupants work and with the Building Emergency Plan. Audiovisual aids and handout materials are extremely helpful. In fact, many high-rise office building owners and managers throughout the United States have contracted with professional fire life safety consultants to produce films describing their emergency systems and equipment and vividly portraying the expected response actions of occupants to building emergencies.

OCCUPANT SAFETY BROCHURE

Pacific Tower Plaza is a modern high-rise building with systems designed to address any emergencies that could take place anywhere in the structure at any point in time. Fire life safety systems are monitored 24 hours a day, seven days a week by a well-trained, on-site security staff. State-of-the-art automatic fire detection and suppression systems are designed to provide early detection and control of fires, permitting occupants to remain in the building for a period of time, safely isolated from a fire. The Toluga Hills City Fire Department is familiar with the building's emergency systems and usually will be on-site within minutes in the event of an emergency.



Pacific Tower Plaza
One Poppyfields Boulevard
Toluga Hills

Nearest Cross Street:
Mount Waverley Boulevard

The risk of a fire spreading at Pacific Tower Plaza is minimized, but if any emergency should occur, it is essential that you know what to do to protect yourself and warn others of any possible danger.

If a Fire Alarm Occurs:

1. Stay as calm as possible.
2. Immediately proceed to your nearest safe stairwell. Follow the directions on the public address system, or from Floor Wardens. DO NOT USE ELEVATORS.
3. In leaving an area, to confine the fire/smoke, close doors but do not lock them.

If You Discover Fire or Smoke:

1. Notify anyone in the immediate area of danger.
2. To confine the fire/smoke, close doors but do not lock them.
3. Activate a Manual Fire Alarm Station, if close by.
4. Call the Fire Department by dialing 911. Tell them:
   - Building name and address
   - Nearest cross street
   - Floor and room/suite number
   - Known information about the fire/smoke
   - Your call-back phone number

   DO NOT HANG UP UNTIL OPERATOR DOES SO.
5. If time allows, notify Building Management and/or Building Security by dialing 555-8395.
6. If time permits, notify the Floor Warden.
7. If you evacuate, use the nearest safe stairwell. DO NOT USE ELEVATORS.

If You Receive a Bomb Threat Call:

1. Keep the caller on the line and obtain as much information as possible:
   - When is bomb going to explode?
   - Where is the bomb?
   - What does it look like?
   - What will cause it to explode?
   - Did the caller place the bomb? Why?
   - What is the caller's name and address?
2. Record the time of call, words of the caller, and any background noises.
3. Notify Building Management and/or Building Security by dialing 555-8395. They will notify tenants and law enforcement.
4. If any suspicious object is found, DO NOT TOUCH IT. Move people away and notify Building Management.
5. The decision whether or not to evacuate usually is the responsibility of the senior officer of a tenant.

If There Is a Medical Emergency:

1. Call Paramedics by dialing 911. Tell them:
   - Building name and address
   - Nearest cross street
   - Floor and room/suite number
   - Location and name of victim
   - Nature of the emergency or victim's condition
   - Caller's call-back phone number

   DO NOT HANG UP UNTIL OPERATOR DOES SO.
2. Notify Building Management and/or Building Security by dialing 555-8395. (If a physician has been called, an escort should be arranged for him or her.)
3. If time permits, notify the Floor Warden.
4. Station someone at the service elevator lobby on the floor involved so paramedics can be escorted to the victim.
5. If properly trained, assist the victim, but do not move the victim unless there is danger of additional, more serious injury.

If There Is an Earthquake

1. Stay as calm as possible.
2. If in an office, move away from windows and interior glass partitions. Get under a strong desk or table and hold on to it.
3. If in a corridor or lobby, drop to the floor near an interior wall and take cover with your arms.
4. If inside an elevator, wait until it stops and the doors open, or summon emergency assistance.
5. Do not run outside the building. If outside, move to a clear area.
6. DO NOT USE ELEVATORS.
7. After the earthquake, if there is damage, assist Floor Wardens and Building Emergency Staff.

   BE PREPARED FOR AFTERSHOCKS.

Figure 11.15 Sample Occupant Safety Brochure.

CERTIFICATE OF OCCUPANT TRAINING

Name (PRINT): ____________________

Tenant Name (PRINT): ____________ Floor and Room/Suite Number: ________

I acknowledge the following (mark box to certify):

[ ] I have received training in building fire life safety.

[ ] I have received a copy of the Occupant Safety Brochure.

[ ] I will check the specific layout of my floor, including the location of my primary and secondary stairwells, location of manual fire alarm stations, and type and location of fire extinguishers.

[ ] Presently I am non-ambulatory or a person with a disability.

Nature of Disability or Reason for Non-Ambulatory Condition: ____________

Signature: ____________ Date: ____________

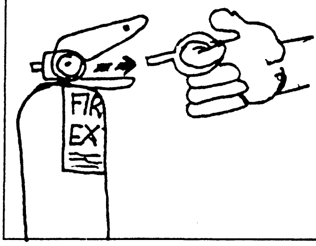
PLEASE FILL OUT AND RETURN TO FLOOR WARDEN OR BUILDING FIRE SAFETY DIRECTOR

Figure 11.16 Sample Certificate of Occupant Training.

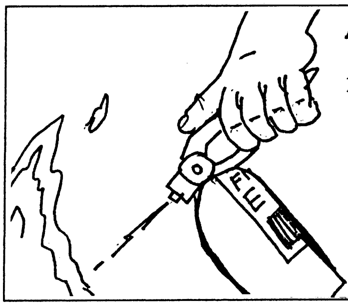
Occupant Training Class

A suggested outline for an occupant training class follows:

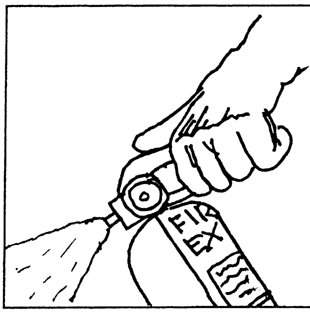
1. Sign in participants (or have them fill out a *Certificate of Occupant Training*).
2. Give a personal introduction—presenter's name, position, experience, and qualifications.
3. Explain legal requirements (state and local laws).
4. Give emergency telephone numbers, or explain where to find them.
5. Outline the Building Emergency Staff Organization—including an explanation of the concept of floor wardens and floor response personnel.
6. Explain building emergency systems and equipment, including a description of the fire detection and suppression systems, what the building's fire alarm sounds and looks like, and the configuration of a typical floor (the position of elevators and stairwells, which stairwells have roof access, etc.).
7. Describe procedures for handling building emergencies—what is expected of occupants in each type of emergency? For example, describe the occupant guidelines in the section on "Occupant Response to a Fire" in Chapter 10.
8. Familiarize the class with the evacuation and relocation plan of the building, locked stairwell door procedures, safe refuge areas, and emergency evacuation procedures for individuals with disabilities.
9. Demonstrate or explain portable fire extinguisher usage. (Some high-rise building owners and managers, for liability reasons, do not train occupants—or even floor wardens—to use fire extinguishers.) The operation of each type of portable fire extinguisher varies depending on its type and the type of fire that it is being used to extinguish. (Chapter 6 includes a description of how to use the various types of extinguishers.) Thoroughly review the specific operating procedures for an extinguisher that a trained occupant may use. An excellent basic method to teach occupants how to correctly use portable fire extinguishers is the four-step P-A-S-S procedure approved by the NFPA (Figure 11.17).



Pull the pin or ring: The pin normally keeps the operating lever locked and prevents accidental discharge of the extinguisher. (Depending on the type of extinguisher there may be different lever-release devices, and seals or devices to indicate whether it has been tampered with.)



Aim the extinguisher hose, nozzle, or discharge horn low at the base of the fire.



Squeeze or press the operating lever or button (usually located directly above the handle). Discharge will stop when the lever is released.

Sweep the discharge back and forth slowly across the fire. Keeping the extinguisher aimed at the base of the fire, move carefully toward it. Continue this sweeping motion until the flames appear to be extinguished. Repeat this action if the fire re-ignites.

Figure 11.17 Portable extinguisher operation using the P-A-S-S procedure. Artwork by Pip Craighead.

10. Give fire drill instructions.
11. Tour a building floor to familiarize occupants with layout of a typical floor, including primary and secondary stairwells, location of manual fire alarm stations, and type and location of fire extinguishers.

Building owners and managers should require all tenants to participate in the building fire life safety program, and some mandate these occupant training requirements in their leases.

Floor Warden Manual and Training

Floor Warden Manual

A Floor Warden Manual often is used to help train high-rise buildings' floor wardens, their alternates, and floor response personnel (including stairwell monitors, elevator monitors, search monitors, and disabled assistance monitors) in their duties and responsibilities. These manuals cover emergencies such as fires, fire alarms, bombs and bomb threats, aircraft collisions, violence in the workplace, medical emergencies, power failures, elevator malfunctions and entrapments, natural disasters, water leaks, hazardous material incidents, labor disputes, demonstrations, and riots and civil disorder. The general information and outline is taken directly from the Building Emergency Procedures Manual described in this chapter, but because the manual is meant for these specific persons, only their duties and responsibilities are emphasized.

Floor Warden Training

A qualified person, preferably the building Fire Safety Director, should conduct a floor warden training class, lasting from 1 to 2 hours, at least every 3 to 6 months. The class should include not only fire life safety legal requirements and emergency systems and equipment, but also an outline of floor wardens' duties and responsibilities in training occupants under their supervision, and a description of the emergency procedures addressed in the Floor Warden Manual.

This class's outline and content should be similar to that described in the preceding ''Occupant Training'' section. It should naturally specify floor wardens' responsibilities in each area and include a time at the beginning to hand out Floor Warden Manuals, floor warden identification material (vest, armband, hard hat, etc.), and any equipment (flashlights).

Some buildings vary the content of floor warden classes over the course of a year. This both stimulates interest and ensures that vital areas are adequately covered. For example, if four classes are provided in a year, the first may address fire emergencies and preparations for building fire drills; the second may address explosions, bombs, and bomb threats; the third may address violence in the workplace; and the fourth may address natural disasters. In addition, a hands-on ''live fire'' portable fire extinguisher class may be offered to floor wardens and conducted by representatives of the local fire department.

This class could be scheduled to coincide with the annual recharging of building fire extinguishers.

Guest speakers may be invited to give special presentations to aid in the education process. A uniformed member of the local law enforcement bomb squad, the local fire department or representatives of organizations such as Alcohol, Tobacco, and Firearms (ATF), the Federal Bureau of Investigation (FBI), and the Federal Emergency Management Agency (FEMA) can be great crowd-drawers and in the process provide floor wardens and building management with up-to-date, interesting, and invaluable information.

Building Emergency Staff Training

Written Instructions

Building emergency staff procedures must be clearly and simply written. Each emergency should be addressed separately, and each member's duties and responsibilities should be documented in detail. This point cannot be stressed enough. Many Building Emergency Procedures Manuals are written in a generic fashion and do not get to the heart of the matter. Yet if staffs are to be adequately trained to handle emergencies, the emergency scenario must be thoroughly analyzed and the best courses of action decided on, documented, and then used for training. This is not to say that everything can be written down or that every planned event can be explicitly defined. As defined by the *New Webster Dictionary*, an *emergency* is ''any event or combination of circumstances calling for immediate action,'' and sometimes these circumstances do vary. The geographic and topographic location of a building, its design and construction, the type and location of security and life safety systems and equipment within it, the type of emergency, and where in or outside the building the emergency occurs are all factors that may affect the impact a major emergency has on a building and its occupants. Despite this, the procedures for handling most emergencies can be planned and well documented.

All instructions for complex emergency procedures and systems material must be written in easy-to-understand, action-oriented terms, keeping in mind the principles in ''Security Staff Duties and Written Instructions'' in Chapter 8.

For example, if a fire alarm occurs on the 20th floor during normal business hours of the hypothetical Pacific Tower Plaza, the security officer whose responsibility it is to go to the Fire Command Center may need to carry out the following tasks:

1. Identify the type of fire alarm and its location by checking the fire computer and the building fire detection and alarm system annunciator and control panels.
2. Acknowledge the alarm by pressing a button or flipping a switch on the control panel (this often also directs the panel to silence the audible signal sounding in the Fire Command Center but does not affect in any way the operation of fire systems in the building).
3. Telephone the fire department by dialing 911 and notify them of the building name and address, nearest cross street, type of fire alarm and its location and any other known details, and the security officer's call-back telephone number. The officer must not hang up until the emergency services operator does so.

4. Broadcast on all radio channels the type of alarm and its location. Direct appropriate engineering and security staff to report to the alarm location to investigate its source.
5. By radio, direct the lobby security officer to report to the main lobby and prepare for the arrival of the fire department.
6. Manually select the 18th, 19th, 21st, and 22nd floor paging zones on the PA system (the 20th floor is automatically activated because it is in alarm); key the microphone; and speak loudly, slowly, and clearly to make the following PA announcement to the floor in alarm, two floors above it, and two floors below it:

   May I have your attention, please. This is Building Security. There is an emergency on the 20th floor. All occupants on the 18th, 19th, 20th, 21st, and 22nd floors, please move to your nearest stairwell and stand by for further instructions.* (Repeat the message loudly, slowly, and clearly.)

   If the order to evacuate is given, make the following announcement:

   May I have your attention, please. This is Building Security. All occupants on the 18th, 19th, 20th, 21st, and 22nd floors, please enter your nearest stairwell, descend five floors, and reenter the building. (Repeat the message loudly, slowly, and clearly.)

7. Manually select the 13th, 14th, 15th, 16th, and 17th floor paging zones on the PA system, key the microphone and speak loudly, slowly, and clearly to make the following announcement to the relocation floors:

   May I have your attention, please. This is Building Security. In response to an emergency occurring on the 20th floor, all floor wardens on the 13th, 14th, 15th, 16th, and 17th floors, please proceed to your nearest stairwell to assist relocating occupants. (Repeat the message loudly, slowly, and clearly.)

8. Broadcast on all radio channels any additional alarms that are received.
9. When the Fire Safety Director, Assistant Fire Safety Director, Chief Engineer, or the fire department has given the all-clear verification, reset the alarm on the control panel.
10. Make the following announcement to the five relocation floors and stairwells:

    May I have your attention, please. This is Building Security. The emergency on the 20th floor is over. It is safe for all occupants to return to their floors. (Repeat the message loudly, slowly, and clearly.)

11. Manually deactivate the PA system on all floors where it was activated.
12. Broadcast on all radio channels that the alarm situation is over and that staff can return to their normal duties.
13. Document all actions on a Fire Alarm Report.

This procedure is designed for a fire alarm that occurs during normal business hours of the building. If a fire alarm occurs after normal business hours, the procedure may need to be modified because the engineering staff may not be available and therefore security staff may need to assume additional duties.

*Some fire departments allow building occupants to wait at the stairwell entrance; others mandate that occupants immediately move into the stairwell and evacuate from the floor in alarm.

From the preceding example, it is apparent that procedures for handling emergencies can become quite complicated for building emergency staff. Moreover, these procedures will vary according to the mandates of the authority having jurisdiction, the custom-designed policies for each building, and the actual operation of the fire detection and alarm system annunciator and control panels. Therefore, as much explanatory documentation as possible should be provided for each building.

Several documents can be kept in the Fire Command Center. The first is the Building Equipment Manual, which contains descriptions and photographs of systems and devices in the station itself and specific explanations as to how the equipment operates under normal and emergency conditions.

A *Normal Business Hours Fire/Fire Alarm Checklist* and an *After Hours Fire/Fire Alarm Checklist*, each outlining steps to handle these emergencies (including flow charts outlining critical procedures), can be conspicuously placed or posted near the control panel for easy reference.

Also, a *Building Emergency Announcement Book* should provide PA messages to give in case of emergencies such as fires and fire alarms; workplace violence; power failures; labor disputes, demonstrations, riots, and civil disorder; bombs and bomb threats; hazardous materials; aircraft collisions; and natural disasters. Fire and fire alarm announcements can be customized for each individual floor of the building—this alleviates the need for the person reading them to work out which floors usually will be evacuated and relocated during such emergencies. In addition, the book should contain sample announcements for fire life safety system testing and drills. All messages must be short, to the point, and easy to understand. For example, this announcement should be made to the floor where testing will occur right before the testing starts:

> May I have your attention, please. This is Building Security. Testing of the building's fire life safety system on your floor will begin shortly and continue for approximately 15 minutes. During that time, please ignore all audible and visual fire alarms unless Building Security or your floor warden otherwise instructs you. Thank you for your assistance. (Repeat the message loudly, slowly, and clearly.)

After testing is completed, this announcement should be made to the floor where the testing occurred:

> May I have your attention, please. This is Building Security. Testing of the building's fire life safety system on your floor has now been completed. Thank you for your assistance. (Repeat the message loudly, slowly, and clearly.)

Documentation not only helps train new staff and refreshes the memory of established staff, but also boosts their confidence, particularly if they fear suddenly ''blanking out'' during a building emergency or announcement.

Training and Testing Methods

Emergency staff members must be properly trained and tested to carry out their duties in the event of a fire or other emergency. According to *Webster's College Dictionary*, to *train* an individual is ''to give the discipline and instruction, drill, practice, designed to impart proficiency or efficiency;'' *testing* is ''a set of problems, questions, for evaluating abilities, aptitudes, skills, or performance. The means by which the presence, quality, or genuineness of anything is determined.''

Building management, the Fire Safety Director, the Alternate Fire Safety Director, building engineers, security officers, and janitorial and parking staff should be trained in emergency procedures for all shifts they work (including weekend and holiday shifts). (The question of ''Who trains the Fire Safety Director?'' has led to some larger city fire departments—such as New York and San Francisco, for example—requiring that individuals who assume this position attend certified training courses.) The Fire Safety Director generally determines the amount of time necessary to properly equip and prepare other staff members to competently handle their duties and responsibilities.

Some high-rise buildings set up monthly training for emergency staff. During these sessions, staff members review their duties and responsibilities, complete practical exercises, and take written tests to ensure that they are in a constant state of readiness. Aspects of the Building Emergency Plan can be tested using tabletop exercises ''designed to introduce participants to basic plan operations and procedures. The exercise is usually played out at an accelerated pace, with all participants located in the same room and no actual movement of operational resources in the field'' (Reid, 1996, p. 78).

Building Walkthrough

When training new emergency staff members, particularly those who due to their responsibilities have a need to understand all aspects of the building (for example, certain building security staff), it is very helpful to take them on a tour of the building and its fire life safety features. These building walk-throughs should be conducted systematically. A sample outline for touring the hypothetical building Pacific Tower Plaza and inspecting its fire life safety systems and equipment follows:

1. Walk the site.
2. Walk the perimeter of the building and inspect all exits, including exits from the subterranean parking structure.
3. Walk the loading dock area and inspect its layout.
4. Enter the building at street level, inspect the main lobby, and note the configuration of passenger and freight/service elevators.
5. Take an elevator to the subterranean parking structure and walk all levels (take note of roll-down gates and doors with fusible links).
6. In the building tower, take an elevator to several individual floors (one in the low-rise elevator bank, one in the mid-rise elevator bank, and one in the high-rise elevator bank). On each floor, review the posted floor evacuation signs, walk through the common areas and public corridors to become familiar with each floor's configuration, and inspect each stairwell. Note the informational signs indicating floor numbers within the stairwell. Inspect maintenance spaces, including mechanical areas and elevator machine rooms.
7. Access the roof and the heliport.
8. Proceed to the Fire Command Center and inspect the following fire life safety systems and devices:

- Voice communication and building PA system
- Fire department voice communication systems
- Public telephone for fire department use
- Stairwell intercom systems
- Fire detection and alarm system annunciator and control panels, including determining the types of devices and their locations
- Sprinkler control valve, water-flow detector, and fire pump status panels
- Other fire protection equipment and system annunciation or status indicators
- Air-handling system controls and status indicators
- Elevator status panel displaying elevator operations
- Emergency and standby power systems status indicators
- Controls for simultaneously unlocking stairwell doors locked from the stairwell side
- Building and elevator keys
- Fire computer terminal and printer
- The Building Emergency Procedures Manual

9. On a typical floor, inspect the location of manual fire alarm stations and automatic detection devices (smoke, heat, or gas detectors).
10. Inspect the following systems and equipment distributed throughout the building:
    - Fire Pump Room
    - Domestic water valves
    - Emergency and standby power generator
    - Sprinkler control valves (main valve and those located in stairwells)
    - Main electrical panels (power transformer room)
    - Gas mains and shut-off valves
    - Fire department connections on the exterior of the building (for automatic sprinkler and standpipe systems)
    - Locations of elevator pits
    - Elevator car operation (including manual recall, independent service, and ''Fireman's Return Override'' or ''Fireman's By-Pass'')
    - Fire department lock box or rapid entry key vault
    - Any other fire life safety equipment (such as automated external defibrillators)
11. Inspect out-of-building safe refuge areas.

Evacuation Signage

State and local laws require evacuation signs to be posted in high-rise buildings so that a means of egress is clearly visible at all times. The means of egress is defined by the NFPA 101, *Life Safety Code*, as ''a continuous and unobstructed way of travel from any point in a building or structure to a public way consisting of three separate and distinct parts: (a) the exit access, (b) the exit, and (c) the exit discharge.''

NFPA 101, *Life Safety Code*, Section 7.10, ''Marking of Means of Egress,'' states the following concerning signs designating exits or ways of travel:

> Section 7.10.1.2. Exits, other than main exit doors that obviously and clearly are identifiable as exits, shall be marked by an approved sign readily visible from any direction of exit access.

Section 7.10.1.3. Tactile signage shall be located at each door into an exit stair enclosure, and such signage shall read as follows:

EXIT

Signage shall comply with CABO/ANSI A117.1, *American National Standard for Accessible and Usable Buildings and Facilities*, and shall be installed adjacent to the latch side of the door 60 in. (152 cm) above the finished floor to the centerline of the sign. *Exception: This requirement shall not apply to existing buildings, provided that the occupancy classification does not change*.

Section 7-10.1.4. Access to exits shall be marked by approved, readily visible signs in all cases where the exit or way to reach the exit is not readily apparent to all occupants. Sign placement shall be such that no point in an exit access corridor is in excess of 100 ft. (30 m) from the nearest externally illuminated sign and is not in excess of the marked rating for internally illuminated signs. *Exception: Signs in exit access corridors in existing buildings shall not be required to meet the placement distance requirements*.

The Code goes on to address the size, color, design, mounting, and illumination of these signs, yet this is a suggested standard—it is up to the individual authority having jurisdiction to specify what evacuation signage is required.

The ADA classifies exit signs, except for the one at the exit door, in two ways. *Directional* signs read ''EXIT'' with an indicator showing the direction of travel (see Figure 11.18). *Informational* signs are located on stairwell landings and usually indicate the stairwell number, what uppermost and lowermost floor the stairwell serves, including a notation whether the stairwell has or has not roof access. They are likewise in every elevator lobby above and below the ground floor, and in other conspicuous floor locations as required by the authority having jurisdiction such as inside all public entrances of the building. Those in elevator lobbies usually include the following information:

- A building floor plan that shows the building core and perimeter, stairwells, fire escapes, elevators, and every wall that faces every exit route.
- A ''YOU ARE HERE'' direction arrow.
- Exit routes to the appropriate stairwells.
- Symbols depicting locations of fire equipment and manual fire alarm stations.
- Information such as the building name and address, floor number, fire department and building emergency telephone numbers, what stairwells have roof access, and what the building fire alarm looks and sounds like.
- If incorporating language similar to: ''IN CASE OF FIRE USE STAIRWAY FOR EXIT. DO NOT USE ELEVATOR,'' the sign should be installed adjacent to the elevator call station (see Figure 11.19).

Signs inside stairwells also may include details regarding re-entry of occupants from the stairwell onto the floor during a fire.

How to Communicate the Building Emergency Plan to Tenants

According to Lohr (1983), ''In a well-planned fire safety education program, the all-important message must be *concise, positive, relevant and aimed at changing someone's attitude and behavior* . . . making that message come alive

Figure 11.18 Exit sign indicates the stairwell entrance.

and be meaningful is one of the vital aspects of the fire safety educator's program planning . . . . messages must be well-planned, realistic and relevant to particular needs'' (p. 1).

Educational Materials

Fire life safety education can be achieved through a variety of means—lectures, classes, workshops, seminars, panel discussions, live demonstrations, and drills—using a variety of educational materials, both written (books, booklets, brochures, pamphlets, leaflets, flyers, and posters) and audiovisual (films, videotapes, overheads, and slide programs). Adams (1983, p. 149) says that,

> In spite of this overwhelming variety, they all have one focal point: firesafety education materials form a bond of communication between the ''speaker'' and the viewer. The mere presence of materials and a viewer doesn't mean there's always communication. Communication occurs when the viewer ''listens'' to the materials, hears and understands what they say, and remembers their message.

Figure 11.19 Typical sign to indicate that elevators should not be used during fire situations.

Also, as Joseph Sano (1994) of the New York State Public Employees Federation reminds us, "use audiovisual aids but don't overdo it! You do not want to compete for your audience's attention with your own props" (p. 48).

In addition to the use of written and audiovisual materials to communicate information *to* building emergency staff, floor wardens, and occupants, certain information must be received *from* building tenants. For example, tenants always must have trained persons assigned to the positions of floor warden and alternate floor warden, and must immediately inform building management and the building Fire Safety Director of any non-ambulatory individuals or individuals with a disability who may need help in an emergency.

Some buildings facilitate feedback of vital details by including requests for updates of fire life safety information from the tenants with Tenant Manuals and information packages given to new tenants. Others distribute a *Fire Life Safety Information Package* (see sample in Appendix 11-2) at least every quarter or 6 months to remind tenants of the building program and their responsibilities in it. This package could include an explanation of the building fire life safety program and the training available for occupants and floor wardens during the ensuing quarter or 6-month period. It also could supply the current versions of building forms such as *Floor Wardens and Alternates Roster* and *Disabled or Non-Ambulatory Persons List*, with a request that tenants update any changes and return the forms to the building Fire Safety Director. (Samples of these forms appear in Appendix 11-1.)

A computer can be of great assistance in maintaining fire life safety records. A database can be created with names and contact telephone numbers of tenants and building emergency staff and training details of all participants in the program. Also, a word processor vastly simplifies the task of making procedural changes to the Building Emergency Procedures Manual.

Educational Methods

Lectures, classes, workshops, seminars, panel discussions, live demonstrations, and drills can all be used to communicate the Building Emergency Plan to tenants. The entire fire life safety education program, however, should be designed at least 1 year in advance. This ensures that the program is comprehensively planned, allows sufficient time to obtain guest speakers (perhaps from local law enforcement and the fire department), permits timely communication of the upcoming schedule to tenants and others for whom the education is intended, and allows the building Fire Safety Director to properly organize and prepare all aspects of the program. A sample yearly program for training building emergency staff, occupants, and floor wardens, and for updating fire life safety records, is shown in Appendix 11-3.

The actual training conducted may vary according to the requirements of state and local codes, the authority having jurisdiction, the historical and projected patterns of emergencies specific to the building, and the policy and support by the building owner and manager for the fire life safety program.

Building Disaster Exercises

Some buildings, on an annual basis, conduct a full-scale building disaster exercise. A simulated emergency with ''casualties'' is planned in conjunction with local emergency response groups, such as fire department, emergency medical responders, local hospitals and health services, local law enforcement, the American Red Cross, utility company representatives, and other emergency organizations within the community. (Such planning may involve contact with neighboring buildings and lead to mutual aid arrangements that assist in addressing certain emergencies, particularly natural disasters that can affect the entire community.) The media can be notified of the event and invited to participate in news briefings. The event itself may last two to three hours. During the mock disaster, drill monitors are stationed at strategic locations throughout the facility to observe and document the conduct of all participants from the time the simulated incident is first initiated. Afterward, all planners of the event meet to critique the execution of the plan and the overall performance of those participating. If thoroughly prepared and properly executed, the simulation can be of great educational value to building staff, tenants, and all outside agencies and groups who participate.

All fire life safety training is costly to a building in terms of participants' time commitment and the provision of educational materials. However, these financial costs are repaid many times over in terms of the emergency preparedness of the building and in the goodwill that can result among building management, tenants, and local authorities.

How to Communicate the Building Emergency Plan to Fire and Emergency Agencies

It is very important that local fire, law enforcement, and emergency medical services be provided with details of the Building Emergency Plan. In many cities the local authority having jurisdiction, usually the fire department or emergency management agency, requires that the Building Emergency Procedures Manual be approved by them; they then retain a file copy of it. Also, the manual must be updated at least annually, and in some jurisdictions every 6 months, or when changes occur, and resubmitted to the local authority. A copy of the manual is required to be readily available at the building for emergency responders (usually in the building's Fire Command Center).

Some cities are requiring that important data about a building be available electronically. For example, the Chicago Office of Emergency Communications (OEC), which coordinates communications for fire, police, and emergency medical responders, requires that high-rise buildings "provide a compact disc (CD) at least every six months containing detailed floor plans, evacuation routes, text documents for each floor, contact information for the entire building, a file showing occupants needing special evacuation assistance, their specific location and the type of assistance required, and a host of other vital building data, all in standard formats. . . . The OEC is able to transmit textual data to all Chicago Police Department squad cars. More detailed information, including floor plans and other graphics, can be sent to police and fire mobile command units and to emergency medical services (EMS) that would be present at any large-scale disaster" (Archibald, Medby, Rosen, and Schachter, 2002, p. 49).

How to Deal with the Media

When an emergency attracts the attention of the news media, the way in which the building owner or manager handles the press will substantially impact the public's perception of the incident and the building itself. The following gives insight into this important aspect of any emergency plan.

A Reporter's Viewpoint

Jack Popejoy, anchor/reporter for KFWB-AM in Los Angeles, talks about media relations from the media representatives' point of view:

> Our job, as dedicated journalists, is to attract an audience that can be sold to advertisers so that our paychecks will be good at the bank. That is neither cynical nor a joke. If we do not accomplish that, keeping our news organization financially viable, we will be out of a job. Our craft and our skill, then, is to take your emergency and make it audience-attracting: compelling, memorable, understandable, and important. (Popejoy, 1993, p. 8)

When an emergency draws the attention of the news media, the information released to them must be timely and accurate. Misinformation and news leaks of confidential information can be damaging to those involved. Information should be given only by persons authorized to do so and, if possible, only by persons who are experienced in dealing with the media.

It is essential to direct all inquiries from the news media to one individual appointed as spokesperson. All others, unless authorized otherwise, should be instructed not to discuss the situation with outsiders, especially the news media. It is important for the designated spokesperson to ''understand that what they want from you is a quote (*soundbite*) that is understandable, memorable, speaks to the concerns of the audience, and projects emotion. If you accomplish that, you can be almost certain the media will transmit what you gave them in your words instead of theirs'' (Popejoy, 1993, p. 8).

How to Turn a Tragedy into Good Publicity

''Working with reporters gives the organization an opportunity to tell its side of the story. The organization spokesperson can present background information that may give the reporter a different perspective'' (Gardner, July 1997, p. 115). The 1988 Los Angeles First Interstate Bank Building fire is an excellent example of how to successfully handle the media. Despite this tragedy that resulted in the loss of one life, multiple smoke inhalation-related injuries, and an estimated financial loss of $50 million, First Interstate Bank of California (whose corporate headquarters were located in the building) and the Los Angeles Fire Department received very good press from the incident. Although few building owners or managers have the public relations resources of a major bank or a large city fire department, there are lessons to be learned from these organizations' techniques.

> Beginning on the night of the fire, First Interstate Bank's Director of Public Affairs, John Popovich, and senior bank executives gave timely press releases to the media. These releases indicated that the bank had been prepared for such an emergency and would continue to provide for its customers by being open for business the very next day. Such actions avoided the financial impact of stock price falls and customer panic that could have resulted. Within hours of the fire, the bank set up a media center with 20 telephones and a customer ''hot line'' to deal with inquiries. Reporters and camera crews were permitted to take photographs of the damaged building and conduct interviews with key bank personnel. The bank also repeatedly publicized the fact that it had implemented a written Business Recovery Plan that, only weeks before the fire, had been tested by simulation of an earthquake disaster. First Interstate Bank representatives dealt with potential criticism for having no working sprinkler system by raising the point that the bank had made a voluntary decision to install such a system and that it was 85 percent complete at the time of the fire.

The Los Angeles Fire Department, through the fire suppression efforts of its highly trained members, achieved a tremendous operational feat in handling this incident—the largest fire involving a high-rise structure in the city's history. This was made clear to the general public by observing their efforts and through statements given to the media by fire department management, including Chief Donald O. Manning and Deputy Chief Doug Anthony. Accurate facts were released to indicate that 383 personnel (50 percent of the Los Angeles Fire Department's resources), 64 fire suppression companies, 10 fire department ambulances, 17 private ambulances, 4 helicopters, plus support equipment were committed to bringing the situation under control. The department also used this opportunity to publicize the fact that many of the high-rises in the city were unsprinklered and that more stringent sprinkler retrofit laws were needed; it also released information that its fire fighters had communication difficulties during the fire because they had to use an antiquated radio system. Statements such as these helped influence the Los Angeles Council to stiffen legislation regarding sprinkler retrofits for high-rise office buildings, and also led to the Fire Department being given funding to obtain a new radio system.

Within weeks of the incident, First Interstate Bancorp, in conjunction with the Los Angeles Fire Department, made a videotape available to the general public depicting the events, lauding the superb fire fighting efforts of the Los Angeles Fire Department, and explaining how the bank had preplanned for such an emergency.

Basic Principles for Handling the Media

The following are basic principles for effectively handling the media to advantage during and after a major emergency:

1. Preplan how the media will be handled. Consider these questions: What type of information will be released? Is it possible to give the media a marketable story? How can victims and their families be shielded? How can the image of the building or company be protected? Under what circumstances are photographs permitted?
2. Designate a media spokesperson or public information person before an incident occurs. For various reasons, it is best if this person is a member of senior management: ''The media will more readily accept that person who will have better access to the inside story and who will more quickly understand implications of legal issues, corporate recovery, and business'' (Popejoy, 1993, p. 8). Instruct building staff to courteously refer all requests for information or interviews to this designated media spokesperson.
3. Decide how media representatives will be accommodated and what access they will be granted to the facility. Will a staging area for their operations be designated? Will basic amenities be available to them? ''Reporters are people too, and it doesn't hurt to show them a little consideration. At Johnson and Johnson, reporters are ushered into a press room that has amenities to ease their stay. These include coffee and, perhaps more important, bathrooms, an important 'extra' for someone on the road. 'Someone drives here all the way from New York, and the first thing they ask is, ''Can I use the bathroom?'' ' [Steve] Chupa [director of security for Johnson and Johnson] says. These small

services can help make for better relations with the media'' (Peck, October 2000, p. 4).

4. Present timely and accurate information to the media. An underlying reason for dealing with the media is so that the dissemination of information can be controlled and presented in a light that the organization involved wants it to be. Jack Popejoy (1993, p. 9) sums it up this way, ''You can control and manipulate the media if and only if you tell the truth. If you lie or withhold, you're dead meat. In the short term, we will quickly know it because we are always in private contact with our offices, which monitor each other, monitor all police and fire frequencies, and have access to wire services and telephone tipsters.''

Guidelines for handling the media during and after a major emergency should be documented in the Building Emergency Procedures Manual. They should designate the spokesperson or public information person who will address the media, outline how media representatives are to be handled and accommodated, and specify what access these representatives are to be granted.

Keeping the Emergency Plan Up-To-Date

Planning does not end with a written document. A Building Emergency Procedures Manual is only a part of the planning process, and after it has been created it should not be placed on a shelf to gather dust. Because the Building Emergency Staff Organization is changing all the time, the plan must be systematically updated. Changes in personnel will occur, but if new personnel are not thoroughly familiar with the plan, it will not be long before the organization is merely a shell of formalities and the plan itself is no longer effective. Unfortunately, it will only take the next real emergency to reveal the true state of affairs in any high-rise building.

> Plans must be maintained to be effective, indeed they must be ''living'' and dynamic.
>
> —CALIFORNIA STATE OF EMERGENCY SERVICES (1993, p. 40)

Summary

The purpose of establishing, implementing, and maintaining a Building Emergency Plan is to promote a state of readiness within a building. In fact, the value is not only in the plan itself but also in the development process leading up to it and the education of building emergency staff that follows it. Communication with outside agencies—local fire, law enforcement, and emergency management agencies—is essential in both establishing the plan and coordinating planning efforts. Dealing with the media should be included as part of the plan. Also, it is essential that the plan be effectively communicated to all building tenants.

References

Adams, Robert, ''Materials,'' *Firesafety Educator's Handbook* (National Fire Protection Association, Quincy, MA, 1983).

Anthony, Doug, statement made on May 5, 1988, on the First Interstate Bancorp/Los Angeles Fire Department Videotape regarding the May 4, 1988, First Interstate Bank Building Fire.

Archibald, Rae, Jamison Jo Medby, Brian Rosen, and Jonothan Schachter, *Security and Safety in Los Angeles High-Rise Buildings After 9/11*, (RAND Documented Briefing, Santa Monica, CA, April 2002, http://www.rand.org).

Best, Richard, and David Demers, *NFPA Investigation Report*, MGM Grand Hotel, contained in ''Special Data Information Package High-Rise Fires-Hotel and Motel Buildings'' (National Fire Protection Association, One-Stop Data Shop, Quincy, MA, August 1999).

BOMA, ''What is an emergency plan?'' *Emergency Planning Guidebook* (Building Owners and Managers Association International, Washington, D.C., 1994).

California State of Emergency Services, ''Conclusion,'' *Business Resumption Planning Guidelines* (California State of Emergency Services Earthquake Program, June 1993).

Carson, Wayne, ''Chip,'' ''Fire safety and the Americans with Disabilities Act,'' (NFPA *Fire News*, National Fire Protection Association, Quincy, MA, December/January 1993).

Cummings, Robert B., and Thomas W. Jaeger, ''ADA sets a new standard for accessibility,'' (*NFPA Journal*, National Fire Protection Association, Quincy, MA, May/June 1993).

Donoghue, Edward A., ''Building transportation systems,'' *Fire Protection Handbook*, 18th ed. Arthur E. Cote, Editor-in-Chief (National Fire Protection Association, Quincy, MA, 1997).

Feasibility and Design Considerations of Emergency Evacuation by Elevators, NISTIR 4870 (U.S. Department of Commerce Technology Administration and the General Services Administration, September 1992).

''Fire and smoke,'' (*Time* magazine, Washington, D.C., March 8, 1993).

Gardner, Robert A., ''Getting ahead of the headlines'' (*Security Management*, Arlington, VA, July 1997).

Gigliotti, Richard, and Ronald Jason, ''Emergency plan considerations,'' *Emergency Planning for Maximum Protection* (Butterworth–Heinemann, Stoneham, MA, 1991).

Harris, Mel, ''Emergency evacuation of disabled workers,'' Letter to the author dated March 27, 1995 (General Services Administration, Washington, D.C.).

Jennings, Charles, ''High-rise office building evacuation planning: Human factors versus 'Cutting edge' technologies'' (*Journal of Applied Fire Science*, Vol. 4(4) 289-302, 1994-1995, Baywood Publishing Co., Inc.).

Klem, Thomas J, ''Major high-rise fires reveal protection needs,'' (*NFPA Journal*, National Fire Protection Association, Quincy, MA, September/October 1992).

Lohr, Cathy, ''Message,'' *Firesafety Educator's Handbook* (National Fire Protection Association, Quincy, MA, 1983).

Los Angeles Fire Department, *Guideline Format for High-Rise Buildings: Emergency Procedures City of Los Angeles 1993* (prepared by the Los Angeles Fire Department Fire and Safety Education Unit, Disaster Preparedness Division, 1993).

Los Angeles Fire Department and Joni and Friends, ''Emergency Evacuation Procedures for Disabled Individuals'' (obtained from the Los Angeles Fire Department Fire and Safety Education Unit, Disaster Preparedness Division, 1994).

Merritt Company, The, ''Disaster control,'' *Protection of Assets Manual*, vol. 1 (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, 1991).

New Webster Encyclopedic Dictionary of the English Language. Editor-in-Chief Virginia S. Thatcher. (Consolidated Book Publishers, Chicago, 1980.)

NFPA 101, ''Definitions,'' *Life Safety Code*, Section 3.3.121, ''Means of Egress'' (National Fire Protection Association, Quincy, MA, 2000).

NFPA 101, ''General,'' *Life Safety Code*, Section 4.7.2,''Fire Drills'' (National Fire Protection Association, Quincy, MA, 2000).

NFPA 101, ''Means of Egress,'' *Life Safety Code*, Section 7.10: ''Marking of Means of Egress'' (National Fire Protection Association, Quincy, MA, 2000).

NFPA *Glossary of Terms* (National Fire Protection Association, Quincy, MA, 2001).

NFPA 1993 *High-Rise Evacuation* video (National Fire Protection Association, Quincy, MA, copyright 1993).

NFPA 2002 *High-Rise Evacuation* video (National Fire Protection Association, Quincy, MA, http://nfpa catalog@nfpa.org, copyright 2002).

NYFD, *Fire Safety Plan Format and Guidelines* (New York City Fire Department, 1972).

Peck, Michael, '' 'No comment' won't do'' (*Security Management*, Arlington, VA, October 2002). Text quoted from the *Security Management* web site.

Popejoy, Jack, ''Emergency communications,'' *BICEPP News*, 2(1) (Business and Industry Council for Emergency Planning and Preparedness, Los Angeles, 1993).

Prouix, Guylène, and Rita Fahy, *A Comparison of the 1993 and 2001 Evacuations of the World Trade Center*, Presentation to the NFPA World Safety Congress and Exhibition, Minneapolis, May 21, 2002.

RCNY 1625, 6-30-91, 6-01, ''Fire drill and evacuation in office buildings and buildings classified as occupancy group E (business), (d) *Drills* (1)'' (New York).

Reid, Ken E., ''Testing Murphy's Law'' (*Security Management*, Arlington, VA, November 1996).

Routley, J. G., NewYork Bank Building Fire: Compartmentation vs. Sprinklers, Report 071 in Major Fires Investigation Project, United States Fire Administration, Emmitsburg, Maryland, 1993, as reported in ''High-rise office building evacuation planning: Human factors versus 'Cutting edge' technologies'' by Charles Jennings (*Journal of Applied Fire Science*, Vol. 4(4) 289-302, 1994-95, Baywood Publishing Co., Inc.).

Sano, Joseph, ''Speak well, and you'll be heard loudly and clearly,'' *The Firemen's Grapevine* (Los Angeles, March 1994). Reprinted from *The Communicator*, official publication of the New York State Public Employees Federation.

Studer, Craig, ''Safeguarding against building fires'' (*Skylines*, Building Owners and Managers Association International, Washington, D.C., March 1992).

Taubman, Byrna, ''What are your chances of surviving a high-rise fire?'' (*New York* magazine, New York, May 27, 1974).

Webster's College Dictionary, 1992 Edition (From Random House Webster's College Dictionary by Random House, Inc. Copyright © 1995, 1992, 1991 by Random House, Inc. Reprinted by permission of Random House, Inc., New York, 1992.)

Additional Reading

Are Your Tenants Safe? BOMA's Guide to Security and Emergency Planning (Building Owners and Managers Association (BOMA) International, Washington, D.C., 2000).

Appendix 11-1 Sample Documentation Forms

FIRE PREVENTION INSPECTION CHECKLIST

Housekeeping/Maintenance	No	OK
1. ''NO SMOKING'' signs posted.	[ ]	[ ]
2. Smoking areas clearly marked. Equipped with non-tip ashtrays, metal waste receptacles, and fire extinguishers.	[ ]	[ ]
3. ''NO SMOKING'' rules and regulations being observed.	[ ]	[ ]
4. Combustible waste stored in proper/approved containers.	[ ]	[ ]
5. Flammable liquids safely stored in approved containers away from combustibles.	[ ]	[ ]
6. Trash/rubbish removal done on a regular basis.	[ ]	[ ]
7. All electrical plugs, switches (no missing or cracked faceplates), and cords legal and in good repair. (Extension cords not to be used in place of permanent wiring).	[ ]	[ ]
8. Cords are not run across doorways or under carpets or mats where they may be walked on.	[ ]	[ ]
9. No extensive use of cords from outlet (octopus).	[ ]	[ ]
10. Adequate clearance maintained at all switch and sub-panels (3 feet or 1 meter).	[ ]	[ ]
11. Heat-producing appliances are well ventilated.	[ ]	[ ]
12. Electrical equipment turned off when not in use.	[ ]	[ ]
13. Malfunctioning electrical equipment immediately reported or taken out of service.	[ ]	[ ]
14. Accumulations of lint, dust, and grease removed.	[ ]	[ ]
15. Areas kept as clean and neat as possible.	[ ]	[ ]
16. Materials stacked so as not to tip or fall.	[ ]	[ ]
17. Safe storage on top shelves (restrict height, weight, and bulk).	[ ]	[ ]
18. Aisles between shelves are clear.	[ ]	[ ]

Fire/Life Protection Systems	**No**	**OK**
1. Adequate lighting in corridors, exits, and stairwells.	[ ]	[ ]
2. EXIT signs illuminated as required (all lights working).	[ ]	[ ]
3. Evacuation routes adequately posted.	[ ]	[ ]
4. Evacuation signs maintained—none defaced or missing.	[ ]	[ ]
5. Fire doors not wedged or blocked open, especially at stairwell.	[ ]	[ ]
6. Stairwells free of obstacles, storage, debris, etc.	[ ]	[ ]
7. Corridors and exits unobstructed (no storage of files, furniture, etc.).	[ ]	[ ]
8. Stairwells, corridors, and exits free of trip and slip hazards (no holes, loose tiles, torn carpeting, defective mats, etc.).	[ ]	[ ]
9. Fire detection and alarm systems tested regularly.	[ ]	[ ]
10. Fire sprinkler connections and shutoff valves visible/accessible.	[ ]	[ ]
11. Fire sprinkler heads clean and unobstructed (no material stored closer than 18 inches or 0.5 meters from the ceiling).	[ ]	[ ]
12. Adequate clearance (3 feet or 1 meter) for all fire extinguishers and hoses.	[ ]	[ ]
13. Fire equipment in proper locations and undamaged.	[ ]	[ ]
14. Floor warden positions updated, fully staffed.	[ ]	[ ]
15. Tenants/new employees instructed on Building Emergency Plan.	[ ]	[ ]

16. Other observations: ______________________________

____

____

Report submitted by: ______________________

Date: ______________________

Suite/Room Number: ______________________

Checklist compiled with the assistance of the Los Angeles Fire Department Fire and Safety Education Unit.

FLOOR WARDENS AND ALTERNATES ROSTER

FLOOR NUMBER	FLOOR WARDEN NAME	FLOOR WARDEN LOCATION AND TELEPHONE NUMBER	ALTERNATE FLOOR WARDEN NAME	ALTERNATE FLOOR WARDEN LOCATION AND TELEPHONE NUMBER

If any changes occur in the above information, immediately advise the building Fire Safety Director or building management.

DISABLED OR NON-AMBULATORY PERSONS LIST

FLOOR NUMBER	INDIVIDUAL NAME	LOCATION AND TELEPHONE NUMBER	NATURE OF DISABILITY	ASSISTANT MONITORS (2) NAMES

If any changes occur in the above information, immediately advise the building Fire Safety Director or building management.

FIRE DRILL NOTIFICATION

Date: ________________________________

Subject: **Required Building Evacuation Drills**

Dear Tenant:

State and local fire codes require that occupants of high-rise buildings participate in evacuation drills on individual floors. Building Management, in accordance with these requirements, has scheduled dates and times to conduct fire drills at Pacific Tower Plaza. The date and time for your floor is as follows:

Date: _____________________ Time: _____________________

The drill will start with the sounding of the building fire alarm on your floor, followed by an announcement by building security over the PA system directing occupants to proceed to the nearest stairwell. This will be followed by a second announcement directing occupants to enter the stairwell and proceed to their designated safe refuge area. When all occupants have arrived there, they will be asked to sign a Fire Drill Register that shows that they participated; also, building management will conduct a verbal review of the drill before directing participants back to their offices (at which point occupants may use elevators to return to their floor). If the drill is properly carried out, it is expected that the total time from the first sounding of the fire alarm to the return of your employees to their offices will be no longer than 15 minutes.

Drill monitors will be stationed at strategic locations to observe and document on a Fire Drill Checklist the conduct of drill participants from the time the fire alarm is first activated. This documentation will be forwarded to the City of Toluga Hills Fire Department. Occupants who refuse to participate in these drills may be cited for noncompliance by the fire authorities.

In preparation, all employees should be told of the upcoming drill (but not necessarily the exact time of it) and asked to review training materials. Floor wardens should be asked to ensure that their floor response personnel are in place. During the drill they should provide adequate control and direction for evacuating occupants and conduct a thorough search of the floor to ensure that all occupants have evacuated.

Both the City of Toluga Hills Fire Department and the Management of Pacific Tower Plaza thank you for your cooperation and continued support of the building fire life safety program.

Signed by Building Management ____

FIRE DRILL ANNOUNCEMENTS

May I have your attention, please. This is Building Security. This is a fire drill. All occupants please proceed to your nearest stairwell and stand by for further instructions.

Repeat the message loudly, slowly, and clearly.

May I have your attention, please. This is Building Security. All occupants please enter your nearest stairwell and relocate to your designated safe refuge area.

Repeat the message loudly, slowly, and clearly.

May I have your attention, please. This is Building Security. There is a fire drill being conducted on floors above your floor. Floor wardens, please proceed to your nearest stairwell to assist in relocating occupants.

Repeat the message loudly, slowly, and clearly.

These announcements may also be required in a foreign language (for example, Spanish), depending on the proportion of non-English speakers in the building at the time of the drill.

FIRE DRILL CHECKLIST

Name of Building: Pacific Tower Plaza
Building Address: One Poppyfields Drive, Toluga Hills

Drill Monitor: ______________________________
Title/Position: ______________________________
Date of fire drill: ______________________________
Time Fire Department notified of fire drill: ______________________________
Name of Fire Department operator: ______________________________
Fire drill floor: ______________________________
Floor/location to which occupants relocated: ______________________________
Method of activation of fire alarm: ______________________________
Time fire alarm activated: ______________________________
Time all occupants vacated fire drill floor: ______________________________

Floor Response Personnel	*Check the appropriate box* *yes*	*no*	*unobserved*
Floor Warden:	☐	☐	☐
Wearing distinctive marking (arm band, vest, or hard hat)?	☐	☐	☐
Assistant Floor Warden:	☐	☐	☐
Wearing distinctive marking (armband, vest, or hard hat)?	☐	☐	☐
Stairwell Monitors:	☐	☐	☐
Elevator Monitors:	☐	☐	☐
Search Monitors:	☐	☐	☐
Assistants to the Disabled and	☐	☐	☐
Non-Ambulatory:	☐	☐	☐
Interior doors closed but not locked after searched?	☐	☐	☐
Interior doors tagged after searched?	☐	☐	☐
Search Monitors checked public rest rooms?	☐	☐	☐
If the drill involved simulation of a fire, was a portable extinguisher brought to the location of the fire?	☐	☐	☐

Overall response of floor response team: Satisfactory Unsatisfactory

Occupant Response	*yes*	*no*	*unobserved*
	Check the appropriate box		
Occupant initial response on sounding of alarm:	Satisfactory		Unsatisfactory
Occupant noise level:	Satisfactory		Unsatisfactory
Occupants aware of location of stairwells?	☐	☐	☐
Did evacuation proceed in smooth and orderly manner?	☐	☐	☐
Did visitors to building participate in drill?	☐	☐	☐
Name and contact details of any occupants	☐	☐	☐
who would not participate: ______			
Overall response of occupants:	Satisfactory		Unsatisfactory
Building Emergency Systems and Equipment	☐	☐	☐
Fire alarm clear in all areas?	☐	☐	☐
PA system announcement clearly heard in all areas?	☐	☐	☐
Did air conditioning systems shut down?	☐	☐	☐
Did pressurization of stairwells occur?	☐	☐	☐
Did stairwell doors automatically unlock?	☐	☐	☐
If no automatic unlock occurred, did floor wardens on relocation floors manually unlock the stairwell doors?	☐	☐	☐
Did door hold-open devices deactivate and the doors close?	☐	☐	☐
Were exits and corridors free of obstructions?	☐	☐	☐
Were any doors blocked or wedged open?	☐	☐	☐
Condition and accessibility of portable fire extinguishers: ______			
Portable electrical and gas appliances turned off?	☐	☐	☐
Total Performance of the Floor:	*Satisfactory*		*Unsatisfactory*

Comments: ______

______

______

Deficiencies Noted and Actions to be Taken: ______

______

______

Signature of Drill Monitor: ______

FIRE DRILL CHECKLIST TO BE RETAINED IN BUILDING FIRE LIFE SAFETY FILES

FIRE DRILL REGISTER

Date: ___________________

Floor Number: ___________________

THE FOLLOWING PERSONS PARTICIPATED IN THE BUILDING FIRE DRILLS PERFORMED ON THE ABOVE DATE:

NAME OF PERSON (PRINTED)	NAME OF TENANT (PRINT)
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	

FIRE DRILL REGISTER TO BE RETAINED IN BUILDING FIRE LIFE SAFETY FILES

BOMB THREAT CHECKLIST

Exact time of call: ______________________________

Exact words of caller: ______________________________

____

____

Questions to Ask

1. When is bomb going to explode? ______________________________
2. Where is the bomb? ______________________________
3. What does it look like? ______________________________
4. What kind of bomb is it? ______________________________
5. What will cause it to explode? ______________________________
6. Did you place the bomb? ______________________________
7. Why? ______________________________
8. Where are you calling from? ______________________________
9. What is your address? ______________________________
10. What is your name? ______________________________

Caller's Voice (*circle*)

Calm	Stressed	Normal	Squeaky	Accent
Excited	Giggling	Slow	Nasal	Disguised
Angry	Crying	Rapid	Lisp	Slurred
Sincere	Loud	Deep	Stutter	Broken

If the voice is familiar, whom did it sound like? ______________________________

Were there any background noises? ______________________________

Remarks: ______________________________

____

Person receiving call: ______________________________

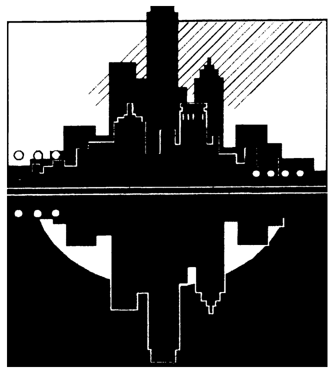
Telephone number at which call received: ______________________________

Date: ______________________________

Reported call immediately to: ______________________________

Reprinted with permission of Bureau of Alcohol, Tobacco and Firearms, an agency of the U.S. Department of the Treasury.

Appendix 11-2 Sample Fire Life Safety Information Package



Date: ______________________________

Subject: **PACIFIC TOWER PLAZA FIRE AND LIFE SAFETY PROGRAM**

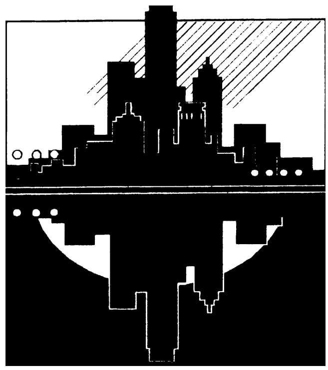
Dear Tenant:

The Management of Pacific Tower Plaza, in cooperation with the City of Toluga Hills Fire Department, has developed a Building Emergency Plan to help ensure the safety of occupants in the event of a fire or other emergency that is likely to occur at this facility. The State Fire Code and the Toluga Hills Fire Code require the material in the plan that pertains to fires. Additional procedures are provided by management for the life safety of building occupants during bomb threats, medical emergencies, workplace violence, power failures, elevator entrapments, natural disasters, hazardous materials incidents, labor disputes, demonstrations, and riots and civil disorder.

Under the Building Emergency Plan, you, as an employer, and we, as building managers, equally share the responsibility for instructing building occupants in the emergency procedures, including evacuation or relocation procedures. The enclosed material explains the fire life safety program in place at Pacific Tower Plaza and provides the means for you to assist us in periodically updating the plan and records pertaining to it. We strongly urge prompt response to ensure compliance with regulations. Failure to comply subjects both you and us to potential prosecution and penalties, including monetary fines.

The Management of Pacific Tower Plaza and the City of Toluga Hills Fire Department thank you for your cooperation and continued support of the building fire life safety program.

Signed by Building Management ______________________________



TENANT FIRE LIFE SAFETY PROGRAM

PACIFIC TOWER PLAZA

The fire life safety program for tenants consists of three major parts:

1. Occupant Documentation and Instruction
   The State Fire Code and the Toluga Hills Fire Code Emergency Planning and Evacuation requirements mandate that all high-rise building occupants be instructed annually on the procedures to be followed in the event of fire or other emergencies likely to occur in the building. All new occupants must be given this instruction within 14 days of assuming occupancy. Documentation of the instruction will be maintained by the building Fire Safety Director and available for inspection by the Chief of the Toluga Hills City Fire Department.
   To meet this requirement, Pacific Tower Plaza has the following publications available:
   - An Occupant Safety Brochure to be given to every occupant in your tenant space.
   - A Certificate of Occupant Training to be filled out by each occupant after each he or she has received fire life safety training. This certificate should then be returned to the Office of the Building or the building Fire Safety Director.

   The Building provides training classes twice each month for occupants, particularly new employees, to be trained in fire life safety. These classes are conducted from 2:00 PM to 3:00 PM on the scheduled days in the Office of the Building. The schedule of classes for the next quarter is as follows:

October 7	October 21	November 4
November 18	December 2	December 16
December 30		

   All occupants must receive fire life safety training. If necessary, additional classes can be conducted in your tenant space. Please communicate any requests for these classes to the building Fire Safety Director.
2. Floor Warden Manual and Training
   The State Fire Code and the Toluga Hills Fire Code Emergency Planning and Evacuation requirements mandate that a responsible person on each floor of every high-rise building be designated as a floor warden, with alternates. Floor wardens, in cooperation with the building Fire Safety Director, are to be thoroughly familiar with the Building Emergency Plan and oversee and ensure safe and complete evacuation or relocation of occupants during a fire or other emergency, or a fire drill.
   Usually each floor has a floor warden and a designated alternate floor warden; if a floor is particularly large or has many individual tenants, there may be several floor wardens (each

individual suite having a suite warden). Each of these persons can be identified by an armband, vest, or hardhat that is worn whenever they are called to duty. Floor wardens should be selected for their ability to make sound decisions during emergency situations, provide direction, and maintain order. They also should be persons whose work responsibilities do not require extensive absences from the office.

The duties of floor wardens and alternate floor wardens, which include overseeing the training and instruction of occupants in their care, are outlined in the Floor Warden Manual that building management provides for every floor warden. Training for these persons is conducted using the manual, meetings, and fire drills. The schedule of activities for the next quarter is as follows:

- October 28: Floor Warden Training for Natural Disasters and Fire Drills. Classes are conducted in the Building Auditorium from 10:30 AM to noon and from 2:00 PM to 3:30 PM (floor wardens are required to attend one of these sessions).
- November 5, 6, 12, & 13: Building Fire Drills. All floor wardens will be notified of the exact time and day on which their individual floor will be drilled.
- December 3 & 4: Fire Extinguisher Training. Classes are conducted on the roof of the Pardee Lane Parking Structure from 11:00 AM to noon and from 2:00 PM to 3:00 PM

3. Fire Drills

The State Fire Code and the Toluga Hills Fire Code Emergency Planning and Evacuation requirements mandate that occupants of high-rise buildings participate in evacuation drills on individual floors. A, minimum of two fire drills on individual floors is required annually. Total evacuation of the building is not mandated. Documentation of all fire drills is maintained by the building Fire Safety Director.

Building management, in accordance with these requirements, has scheduled dates and times to conduct fire drills at Pacific Tower Plaza. The fire drills are scheduled for the next quarter on November 5, 6, 12, & 13. All floor wardens will be notified of the exact time and day on which their individual floor will be drilled.

The drill will commence with the sounding of the building fire alarm on your floor, followed by an announcement by building security over the PA system to direct occupants to proceed to their nearest stairwell. This will be followed by a second announcement to direct occupants to enter the stairwell and proceed to their designated safe refuge area. When all occupants arrive at the safe refuge area, they will be asked to sign a Fire Drill Register that shows that they participated. Also, building management will conduct a verbal review of the drill before directing participants back to their offices (at which point occupants may use building elevators to return to their floors). If the drill is properly carried out, it is expected that the total time from the first sounding of the fire alarm to the return of your employees to their offices will be no longer than 15 minutes.

Drill monitors will be stationed at strategic locations to observe and document the conduct of drill participants from the time the fire alarm is first activated. This documentation will be forwarded to the City of Toluga Hills Fire Department. Any occupants who refuse to participate in these code-mandated drills may be cited by the fire authorities for noncompliance.

In preparation, all employees should be told of the upcoming drill and asked to review occupant training material. Floor wardens should be asked to ensure that their floor response personnel are in place. During the drill they should provide adequate control and direction for evacuating occupants and conduct a search of the floor to ensure that everyone has left.

Attachments: Disabled or Non-Ambulatory Persons List
Floor Wardens and Alternates Roster
Fire Prevention Inspection Checklist

PLEASE RETURN THE COMPLETED LIST, ROSTER, AND CHECKLIST WITHIN TWO WEEKS TO THE OFFICE OF THE BUILDING OR THE BUILDING FIRE SAFETY DIRECTOR.

Appendix 11-3 Calendar of Annual Events

January

Building Emergency Staff——Training for Fires and Fire Alarms
Occupants——Building Fire Life Safety Training
Floor Wardens——Training for Fire Life Safety
All Building Occupants——''Safety Reminder of the Month'' Bulletin

February

Building Emergency Staff——Power Failure and Elevator Safety Training
Occupants——Building Fire Life Safety Training
All Building Occupants——''Safety Reminder of the Month'' Bulletin

March

Building Emergency Staff——Explosions, Bombs, and Bomb Threats Training
Occupants——Building Fire Life Safety Training
Floor Wardens——Update of Floor Warden Rosters and Disabled and Non-Ambulatory Persons List
All Building Occupants——''Safety Reminder of the Month'' Bulletin

April

Building Emergency Staff——Training for Fires and Fire Alarms and May Fire Drills
Occupants——Building Fire Life Safety Training
Floor Wardens——Training for Explosions, Bombs, and Bomb Threats and May Fire Drills
All Building Occupants——''Fire Drills'' Bulletin

May

Building Emergency Staff——Chemical/Hazardous Material Training
Occupants——Building Fire Life Safety Training
All Building Occupants——Fire Drills and ''Safety Reminder of the Month'' Bulletin

June

Building Emergency Staff——Violence in the Workplace and Hostage and Barricade Training
Occupants——Building Fire Life Safety Training
All Building Occupants——''Safety Reminder of the Month'' Bulletin

July

Building Emergency Staff——Training for Fires, Fire Alarms, and Aircraft Collisions
Occupants——Building Fire Life Safety Training
Floor Wardens——Training for Violence in the Workplace Incidents
All Building Occupants——''Safety Reminder of the Month'' Bulletin

August

Building Emergency Staff——Labor Disputes, Demonstrations, Riots and Civil Disorder Training
Occupants——Building Fire Life Safety Training
All Building Occupants——''Safety Reminder of the Month'' Bulletin

September

Building Emergency Staff——Natural Disaster and Water Leak Training
Occupants——Building Fire Life Safety Training
Floor Wardens——Update of Floor Warden Rosters and Disabled and Non-Ambulatory Persons List
All Building Occupants——''Safety Reminder of the Month'' Bulletin

October

Building Emergency Staff——Training for Fires and Fire Alarms and November Fire Drills
Occupants——Building Fire Life Safety Training
Floor Wardens——Training for Natural Disasters and November Fire Drills
All Building Occupants——''Fire Drills'' Bulletin

November

Building Emergency Staff——Medical Emergency Training
Occupants——Building Fire Life Safety Training
All Building Occupants——Fire Drills and ''Safety Reminder of the Month'' Bulletin

December

Building Emergency Staff and Floor Wardens——Fire Extinguisher Training
Occupants——Building Fire Life Safety Training
All Building Occupants——''Safety Reminder of the Month'' Bulletin

This Page Intentionally Left Blank

12 *Laws, Codes, and Standards*[*]

As defined by *Black's Law Dictionary*, the *law*, "in its generic sense, is a body of rules or action or conduct prescribed by the controlling authority, and having binding legal force; that which must be obeyed and followed by citizens subject to sanctions or legal consequences is a law." A *code* is "a systematic collection; a private or official compilation of all permanent laws in force consolidated and classified according to subject matter." A *standard* is "a model, type, or gauge used to establish or verify what is commonly regarded as acceptable or correct" (*Webster's* definition as stated in POA, 1999, p. 1-35).

Laws, codes, and standards applicable to high-rise office buildings aim to enhance public safety for building users through guidelines established for the manufacture and use of various materials and equipment, the methods of construction, and the provision of various services for building operation.

Building inspectors, fire marshals, testing laboratories, manufacturers, architects, engineers, builders, installers, consultants, owners, managers, risk managers, insurance agents, security directors, fire safety directors, maintenance departments, contract security firms, investigators, legal counsel, professional societies, trade associations, and tenants all have codes and standards to follow in their particular areas of expertise or responsibility. These regulations also provide a format for quality and standardization throughout the industry.

Types of Standards

There are two main types of standards relevant to the security and fire life safety operations of high-rise buildings.

Statutory or Regulatory Standards

Statutory or *regulatory standards* are enacted under the law. Some come from federal sources such as the Occupational Safety and Health Act (OSHA), the Americans with Disabilities Act (ADA), and the National Institute

[*]The article "Standards in Security," in the *Protection of Assets Manual*, was invaluable in understanding laws, codes, and standards. (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright 1991, pp. 1-41–1-57.)

of Standards and Technology (NIST). Others, such as the licenses and regulations governing private security firms and certain building and fire codes, are adopted by state and local legislatures.

Consensus or Private Standards

Consensus or *private standards* are advisory recommendations applied by consent or agreement rather than required by law. Some of these standards have been developed or sponsored by the federal government, such as those created by the Law Enforcement Assistance Administration (LEAA). Others were developed by private sources (professional societies, trade associations, insurance companies, equipment manufacturers, etc.); examples include the National Fire Protection Association (NFPA), Underwriters Laboratories Inc. (UL), the American Society for Testing Materials (ASTM), the American Institute of Architects (AIA), the American Society of Mechanical Engineers (ASME), the American Society of Civil Engineers (ASCE), the Security Industry Association (SIA), the National Association of Security Companies (NASCO), the National Burglar and Fire Alarm Association (NBFAA), the Illuminating Engineering Society (IES), the National Electrical Manufacturers Association (NEMA), the National Conference of States on Building Codes and Standards (NCSBCS), the Institute of Real Estate Management (IREM), and the Building Owners and Managers Association (BOMA) International.

American National Standards Institute

The American National Standards Institute (ANSI) is a private organization that does not develop or enforce standards, but reviews and validates the voluntary standards already prepared by private groups, designating the best of them as American National Standards. These standards represent a general agreement among manufacturers, distributors, and consumers on the best practices over a wide area of the building industry. ANSI reviews standards every 5 years to ensure they are up to date with current technology and practice.

The following sections review various organizations and their laws, codes, and standards. However, it is not within the scope of this book to list comprehensively all regulations applied in the United States. Even if such a list were provided, it would need to be customized for each facility, as Schum (1989, p. 205) points out:

> In your personal experience, you will be faced with codes and standards not listed therein, and you may never have to deal with many of those listed. Code use tends to be regional, and every state, county, and city must be dealt with individually for local approvals and restrictions. However, most codes are based on national code publications.

Laws

Occupational Safety and Health Act

Congress passed the Occupational Safety and Health Act to provide a legislative basis for safety activities. On April 28, 1971, Public Law 91.596 became effective, and the Occupational Safety and Health Administration (OSHA) was established within the Department of Labor. Each employer in the United States is now responsible for meeting the minimum requirements of the published OSHA standards. In addition, each employer must maintain injury and illness records. As POA (1999, p. 29-14) comments:

> The law also requires each employee to comply with safety and health standards as well as with all rules, regulations and orders which are applicable to the employee's own actions and conduct. But no penalties are provided for employees who fail to do so. One way the language might be applied would be in mitigation of damages in any civil suit brought against an employer by an employee who had been non-complying. But most workplace accidents and injuries are dealt with under state Workers' Compensation law which, typically, doesn't recognize a ''contributory'' or ''comparative negligence'' type defense.

Generally speaking, OSHA requires that an employer provide a safe and healthful place for employees to work. The ''General Duty'' clause summarizes the act and states that each employer ''shall furnish to each of his [or her] employees a place of employment free from recognized hazards that are causing or likely to cause death or serious physical harm to his [or her] employees'' (OSHA, 1974). ''Much of the rest of the act deals with procedures and standards of safety and is in places difficult to follow. It speaks of free and accessible means of egress, of aisles and working areas free of debris, of floors free from hazards. It gives specific requirements for machines and equipment, materials, and power sources. It specifies fire protection by fixed or portable systems, clean lunchrooms, environmental health controls, and adequate sanitation facilities'' (Fischer and Green, 1998, p. 283).

The means of egress requirements (sections .35 through .37 of OSHA's Title 29 of the Code of Federal Regulations, Part 1910, General Industry Standard) include standards on emergency plans and fire prevention plans. From 1970 to 1972, however, appropriate national consensus standards were adopted, including specific portions of NFPA 101, *Life Safety Code*. Because ''OSHA did not adopt all of the Life Safety Code, just specific portions of it, OSHA's standards on means of egress are incomplete at best'' (Carson, 1993, p. 48). OSHA has attempted to solve this problem by allowing one of the comprehensive and frequently updated NFPA standards to meet the requirements for a corresponding OSHA standard—not only in this area, but also in many others. Fischer and Green (1998, pp. 283, 284) note:

> In 1988, OSHA issued the Hazard Communication Standard, which states that all employees have the right to know what hazards exist in their place of employment and what to do to protect themselves from the hazards. Simple labels and warnings on containers are not enough. Employers must have a program to communicate more

detail on all hazards, including a Material Safety Data Sheet (MSDS) that must be available for each chemical at the worksite. Each MSDS contains seven sections:

1. Product identification and emergency notification instructions
2. Hazardous ingredients list and exposure limits
3. Physical and chemical characteristics
4. Physical hazards and how to handle them (that is, fire, explosion)
5. Reactivity data—what the product may react with and whether it is stable
6. Health hazards—how the product can enter the body, signs and symptoms of problems, and emergency first-aid steps
7. Safe handling procedures

At the federal level, the Department of Labor has the responsibility for enforcing the standards and regulations of OSHA. The standards also can be enforced at the state level using local laws, if they meet the minimum requirements of the federal legislation. Compliance officers inspect places of business to investigate adherence to OSHA standards. If a facility is not in compliance, these officers may issue citations and penalties and fines may be levied against the employer.

Americans with Disabilities Act

The Americans with Disabilities Act (ADA) was signed into law in 1990. The protection it provides to specified classes of individuals is similar to that afforded by the Civil Rights Act of 1964, which prohibited discrimination on the basis of race, color, religion, sex, or national origin. The ADA provides comprehensive civil rights protection to ''individuals with a disability'' (the previous term ''handicapped individual'' has been replaced). The term *disability* (Title 42, United States Code, Chapter 126, Section 12102) means, with respect to an individual, ''(A) a physical or mental impairment that substantially limits one or more of the major life activities of such individual; (B) a record of such an impairment; or (C) being regarded as having such an impairment.'' The term *reasonable accommodation* may include (Title 42, United States Code, Chapter 126, Subchapter 1, Section 12111): ''(A) making existing facilities used by employees readily accessible to use and usable by individuals with disabilities; and (B) job restructuring, part-time or modified work schedules, reassignment to a vacant position, acquisition or modification of equipment or devices, appropriate adjustment or modifications of examinations, training materials or policies, the provision of qualified readers or interpreters, and other similar accommodations for individuals with disabilities.''

The ADA has superseded the Architectural Barriers Act of 1968 and the Rehabilitation Act of 1973. Both these laws were directed toward assisting individuals with a disability. However, they were applied primarily to firms doing business with or receiving monetary assistance from the federal government. The ADA applies to almost every type of business. The act is intended to ensure comprehensive civil rights protection to individuals with a disability with regard to employment, state and local government services, transportation, new and existing public accommodations, new commercial facilities, and telecommunications. It places certain obligations on employers and businesses and has a far-reaching impact on the security and fire life safety operations of buildings. Atlas (1992) notes, ''ADA will affect architecture, life safety design, and building security technology dramatically. Some of the most critical impacts on building security will be building access, door hardware, fire egress, and system controls, including card readers used for entrance and exit access control, elevator controls'' (p. 37), emergency intercoms, fire and life safety devices such as manual fire alarm stations, and evacuation signage. The government has published two technical manuals, *Uniform Federal Accessibility Standards* and *ADA Accessibility Guidelines*, which give detailed information regarding these issues. The ADA consists of five parts or titles:

Title I: Employment—This title prohibits discrimination in employment against qualified individuals with disabilities. It went into effect July 26, 1992, for employers with 25 or more employees. On July 26, 1994, it became effective for employers with 15 or more employees.

Title II: Public Services—This title states that ''no qualified individual with a disability shall, by reason of such disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of a public entity, or be subject to discrimination by any such entity'' (Title 42, United States Code, Chapter 126, Subchapter II, Section 12132). The term *public entity* includes any state or local government or their departments, agencies, special purpose districts, or other instrumentalities, including public transportation.

Title III: Public Accommodations and Services Operated by Private Entities—This title deals with the accessibility requirements in public buildings and commercial facilities. ''No individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation'' (Title 42, United States Code, Chapter 126, Subchapter III, Section 12182).

This regulation applies to both the occupants of a building and any visitors to the facility. New buildings are required to comply fully with Title III. Existing buildings must comply to the extent that the changes required are *readily achievable*. This term means ''easily accomplishable and able to be carried out without much difficulty or expense'' (Title 42, United States Code, Chapter 126, Subchapter III, Section 12181). The Architectural Transportation Barriers Compliance Board (ATBCB) developed ADA Accessibility Guidelines for Buildings and Facilities (ADAAG) as specific Title III standards. Title III went into effect on January 26, 1992, for existing facilities, and on January 26, 1993, for all new construction.

Title IV: Telecommunications—This title requires all common carriers to provide a telephone service (Telecommunications Relay Service) that permits individuals with hearing or speech difficulties to use the telephone.

Title V: Miscellaneous Provisions—This title contains some of the technical information pertaining to the Act.

The ADA applies to new building construction and major alterations carried out in existing buildings. When a building owner or manager makes alterations in compliance with ADA there are some financial and tax benefits to the building.

Codes and Regulatory Standards

National Institute of Standards and Technology

The National Institute of Standards and Technology, a unit within the U.S. Department of Commerce, was formerly called the National Bureau of Standards. NIST creates the Federal Information Processing Standards Publications (FIPS PUB), which are used both in the government and the private sector. It also produces standards and technical reports, which cover equipment such as control units for intruder alarm systems, and a Building Science Series, which ''disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems'' (NIST, 1991).

The NIST also houses the Building and Fire Research Laboratory (BFRL), which compiles data regarding the characteristics of materials and their behavior when subjected to fire. The objective of the research conducted by the BFRL is to improve fire life safety codes and standards.

Licensing and Regulation of Private Security Firms

State and local governments frequently license and regulate private security* firms. To obtain a license to operate in some areas, both state and local requirements must be met. According to Cunningham, Strauchs, and Van Meter (1990, pp. 153, 154),

> Approximately 75% of the states regulate some aspect of private security and its employees. In addition (or sometimes in place of state regulation), municipal or county governments often have ordinances regulating private security. Because laws pertaining to security licensing have changed often, it is nearly impossible to delineate the regulatory requirements of local and state governments. However, the table [Table 12.1] provides an overview of state regulatory activity. In addition to security business and personnel regulation, an estimated 2,000 local governments have enacted alarm ordinances.

State and Local Building and Fire Codes†

Building Codes

According to Cote and Grant (1997, p. 1–43),

> A building code is a law or regulation that sets forth minimum requirements for design and construction of buildings and structures. These minimum requirements, established to protect the health and safety of society, generally represent a compromise between optimum safety and economic feasibility. Although builders and building owners often establish their own requirements, the minimum code

*Appendix 12-1, *Security and the Law*, is a study of criminal and civil law.

†The article ''Building and Fire Codes and Standards'' by Arthur E. Cote and Casey C. Grant was used to help compile this information (*Fire Protection Handbook*, 18th ed. Arthur E. Cote, Editor-in-Chief, National Fire Protection Association, Quincy, MA, 1997, pp. 1-42–1-54).

Table 12.1 State Regulation of Private Security Firms*

TYPE OF FIRM	NUMBER OF STATES
Guard and Patrol	
Licensing of businesses	39
Registration	25[1]
Private Investigators	37
Alarm	25
Armored Car	9[2]

[1]Plus District of Columbia.
[2]Does not include Public Utility Commissions or Interstate Commerce Commission.
*Reprinted with permission from William C. Cunningham, John J. Strauchs, and Clifford W. Van Meter, *The Hallcrest Report II: Private Security Trends 1970–2000* (Butterworth–Heinemann, Stoneham, MA, 1990), p. 153.
Sources: (1) ''Security data bank,'' *Security*, June 1990, p. 55; (2) *Security Letter Source Book*, 1990–1991, Section H.H.6, Robert McCrie, Editor, Butterworths, Stoneham, MA, March 1990; (3) ''Regulations vary by state,'' *Security Distributing and Marketing*, September 1989, p. 82; (4) Truett Ricks, Gill Tillett, Clifford Van Meter, *Principles of Security* (Second Edition), Anderson Publishing Co., 1988, pp. 168–171; (5) ''Regulation of the Private Security Industry,'' National Institute of Justice, U.S. Department of Justice, (unpublished), January 1981.

requirements of a jurisdiction must be met. Features covered include structural design, fire protection, means of egress, light, sanitation, and interior finish.

There are two general types of building codes. Specification or prescriptive codes spell out in detail what materials can be used, the building size, and how components should be assembled. Performance codes detail the objective to be met and establish criteria for determining if the objective has been reached; thus, the designer and builder are free to select construction methods and material as long as it can be shown that the performance criteria can be met.

There are a small number of model building code groups that have been largely responsible for building code development in the United States.

American Insurance Services Group (AISG)

In 1905, National Board of Fire Underwriters (NBFU; later known as the American Insurance Association [AIA], and now as the American Insurance Services Group [AISG]) first published what was later known as the *National Building Code* (NBC). The NBC was designed as an archetype for cities to adopt and as a means of grading the building regulations of cities and towns. The NBFU ''began to emphasize safe building construction, control of fire hazards, and improvements in both water supplies and fire departments. As a result, the new tall buildings constructed of concrete and steel conformed to specifications that helped limit the risk of fire. These buildings were called Class A buildings'' (Cote and Grant, 1997, p. 1-43).

Permission to use the term *National Building Code* was transferred to the Building Officials and Code Administrators in 1982.

Building Officials and Code Administrators, International

The Building Officials and Code Administrators (BOCA), International was first established as the Building Officials Conference of America, and published the *Basic/Building Code* (BBC) in 1950. BOCA began publishing this code as the *National Building Code* (NBC) after acquiring rights to the term from AISG. The NBC is republished every 3 years.

In addition, the BOCA publishes fire prevention, plumbing, and mechanical codes. Its membership primarily covers the northeastern United States and includes building officials, architects, engineers, and industry representatives. BOCA is a service organization that provides its members with technical and educational information aimed toward developing safe and efficient building codes.

International Conference of Building Officials (ICBO)

The International Conference of Building Officials (ICBO) first published the *Uniform Building Code* (UBC) in 1927. ''The *Uniform Building Code* is the most widely adopted model building code in the world. Published every three years, it provides complete regulations covering all major aspects of building design and construction relating to life and fire safety and structural safety'' (ICBO, 1993, p. 1).

With the International Fire Code Institute (IFCI), the ICBO co-publishes the *Uniform Fire Code*, which is a fire prevention code endorsed by the Western Fire Chiefs Association, a division of the International Association of Fire Chiefs (IAFC), and a *Uniform Mechanical Code*. The ICBO also co-publishes the *International Plumbing Code* (IPC) with its sister model code organizations, BOCA and SBCCI. The ICBO membership primarily covers the western half of the United States and includes local government agencies, building professionals, and trade associations.

Southern Building Code Congress International (SBCCI)

The Southern Building Code Congress International (SBCCI) first published the *Southern Standard Building Code* in 1945. It is now called the *Standard Building Code* (SBC) and provides minimum construction standards to safeguard life, health, and public welfare in all types of buildings and structures, including high-rises. The SBC ''addresses life safety issues such as height and area requirements, fire protection, alarm systems, and means of egress. It provides design information such as minimum design loads, wind loads, snow loads, and earthquake loads. In addition, it gives information on specific construction materials such as masonry, steel, concrete, wood or gypsum'' (SBCCI, 1993, p. 2). The SBCCI publishes this code every 3 years and also provides a comprehensive commentary to assist in its interpretation. The SBCCI membership covers roughly the southeastern section of the country as far west as Texas and Oklahoma; it consists mainly of building officials, with an associate membership of fire officials and industry representatives.

Council of American Building Officials (CABO)

BOCA, ICBO, and SBCCI formed an organization called the Council of American Building Officials (CABO). Its Board for the Coordination of the Model Building Codes (BCMC) has attempted to coordinate the provisions of the NBC, UBC, and SBC, plus various NFPA codes and standards (mainly NFPA 101, *Life Safety Code*).

International Code Council (ICC)

Established in 1995, the International Code Council (ICC) consists of representatives from BOCA, ICBO, and SBCCI. ''The purpose of the ICC is to combine the codes of the three model building code organizations into single national models'' (Cote and Grant, 1997, p. 1-45).

National Fire Protection Association

The National Fire Protection Association (NFPA) was organized in 1896 as an independent, voluntary, nonprofit organization. Its mission, as stated in the *Fire Protection Handbook* (1997, p. C-1), is to ''reduce the burden of fire on the quality of life by advocating scientifically-based consensus codes and standards and research and education for fire and related safety issues.'' According to information obtained from *Building Life Safety with Codes* (Lathrop and Birk, 1992, p. 46), in 1913, the NFPA formed the Committee on Safety to Life. This committee was responsible in 1927 for publishing the *Building Exits Code*, which addressed exits and fire life safety features in all occupancy classes. There were many revisions of and new additions to this code. In 1966, its name was changed to the *Code for Safety to Life from Fire in Buildings or Structures*, more commonly known as NFPA 101, *Life Safety Code*.

As Cote and Grant (1997, p. 1-44) explain,

> NFPA 101, *Life Safety Code*, establishes minimum requirements necessary for providing a reasonable degree of life safety from fire. The *Life Safety Code* addresses those construction, protection, and occupancy features necessary to minimize danger to life from fire, smoke, fumes, or panic. It also identifies the minimum criteria for design of egress facilities to permit prompt escape of occupants from buildings or, where preferable, evacuation into safe areas within the building. The *Life Safety Code* does not attempt to address those general fire prevention or building construction features that normally are functions of fire prevention and building codes.

This code is revised and published by the NFPA every 3 years. ''To date, approximately half the states in the United States have adopted the NFPA, *Life Safety Code*, and many others use it as a model for local legislation dictating life safety standards for new construction, existing buildings, and renovations'' (Garboden, 1994, p. 35).

Presently the NFPA creates and updates over 300 standards and codes, including the *Life Safety Code*, that are published as the *National Fire Codes* (NFC). They address virtually every aspect of fire protection, including prevention, detection, and suppression. These standards and codes are widely used and adopted as law by many state and local governments and overseas countries. They are used as a reference by many agencies of the federal government, such as OSHA, in their own regulations. Insurance agencies use them as a basis for risk evaluation and premium ratings. The NFPA also performs investigations of major fires; conducts research on important fire protection issues; collects and analyzes fire data and statistics; and produces educational brochures, videos, reference books and textbooks, training programs, and school curricula to assist people in learning how to protect themselves from fire. In addition, NFPA administers certification programs ''designed to raise the level of professionalism throughout the fire protection community'' (Wilson, 2001, p. 100).

NFPA 5000, *Building Code*™

''NFPA 5000 is the first building code being developed through an American National Standards Institute (ANSI)-accredited process. . . . NFPA is currently developing NFPA 5000, *Building Code*, the first consensus-based building code'' (NFPA web site, 2002). ''The purpose of the *Code* is to provide minimum design regulations to safeguard life, health, property, and public welfare and to minimize injuries by regulating and controlling the permitting, design, construction, quality of materials, use and occupancy, location, and maintenance of buildings and structures within the jurisdiction and certain equipment specifically regulated herein'' (NFPA 5000, May 2002, 1-3).

''One aspect that sets NFPA 5000 apart from other building codes in the United States is the way it's set up. Like the *Life Safety Code*, NFPA 5000 is organized by occupancy rather than design feature, giving users the fundamental requirements for everything from occupant load factors to means of egress and related hazard requirements right from the start of the project. From there, the user is directed to related chapters that deal with structural design and interior environments'' (Wolf, March/April 2002, p. 58).

Model Building Codes are Not Laws until Enacted

Model building codes are not laws in themselves. They must be adopted into law by the appropriate state and local legislatures before they can be enforced. ''Building code requirements usually apply to new construction or to major alterations to buildings. Retroactive application of code requirements is rare. Building code applicability usually ends with the issuance of an occupancy permit or certificate of occupancy'' (Cote and Grant, 1997, p. 1-49).

Fire Prevention Codes

In addition to building codes, there are fire prevention codes. A fire code or fire prevention code usually deals with fire hazards that exist in a building after occupancy has been granted. In the United States the model fire codes or fire prevention codes are:

1. The *Fire Prevention Code* of the AISG (this code has not been revised or published since 1976)
2. The BOCA *National Fire Prevention Code*
3. The ICBO *Uniform Fire Code*
4. The SBCCI *Standard Fire Prevention Code*
5. The *Fire Prevention Code* of the NFPA. Often local authorities adopt the NFPA standards but do not update the standard when the NFPA does. Therefore, it is important to check the actual standard adopted rather than referring to the most up-to-date NFPA standard.

"NFPA 1, *Fire Prevention Code*, and the *Uniform Fire Code* (UFC), the two most widely adopted fire codes in the U.S., are being merged in 2003 to become NFPA 1, *Uniform Fire Code*, addressing basic fire prevention requirements necessary to establish a reasonable level of fire safety and property protection from the hazards created by fire and explosion" (NFPA web site, 2002).

Who Enforces Building and Fire Prevention Codes?

The building department having jurisdiction usually enforces building codes; a fire official such as the fire marshal usually enforces fire prevention codes.

Authority Having Jurisdiction

To determine the laws and codes that apply to a particular facility, one must determine exactly which ones the *authority having jurisdiction* (AHJ) has adopted. The *National Fire Code* defines this term:

> The "authority having jurisdiction" is the organization, office or individual responsible for approving equipment, materials, an installation, or a procedure.
>
> The phrase "authority having jurisdiction" is used in NFPA documents in a broad manner, since jurisdictions and approval agencies vary, as do their responsibilities. Where public safety is primary, the authority having jurisdiction may be a federal, state, local, or other regional department or individual such as a fire chief; fire marshal; chief of a fire prevention bureau, labor department, or health department; building official; electrical inspector; or others having statutory authority. For insurance purposes, an insurance inspection department, rating bureau, or other insurance company representative may be the authority having jurisdiction. In many circumstances, the property owner or his designated agent assumes the role of the authority having jurisdiction.

Interpretation of Laws, Codes, and Standards

Laws, codes, and standards are interpreted and enforced by human beings, and therefore one should keep in mind that:

> If you feel that an error has been made, contact the agency in writing and seek a clarification of that interpretation. Never assume that an agency official is correct. If

> a summons or a violation is issued to you, accept it, but advise the official that you are accepting it under protest. If the summons requires your signature, sign it, but also note that you are signing it under protest. (Cassidy, 1992, p. 73)

Private Standards

Law Enforcement Assistance Administration

The former Law Enforcement Assistance Administration (LEAA), which was part of the U.S. Department of Justice, developed two sets of standards. The first was prepared by LEAA's Private Security Advisory Council (PSAC). As Cunningham, Strauchs, and Van Meter (1990, p. 3) summarize:

> Among the publications prepared by the PSAC, and published by the LEAA, were model statutes for burglar alarms, and for state licensing of security guards; a code of ethics for security management and operating personnel; and standards for armored car and armed courier services. Additionally, the PSAC published documents outlining the scope of legal authority of security personnel and areas of conflict between law enforcement and private security.

The second set of standards, called the *Report of the Task Force on Private Security* (PSTF), was issued in 1976. According to Cunningham, Strauchs, and Van Meter (1990), ''The Task Force suggested development of comprehensive standards in the following areas: selection of personnel, training, conduct and ethics, alarm systems, environmental security, law enforcement agencies, consumers of security services, higher education and research, and government regulation. In the 14 years since the release of that report, probably not more than 10 of the [83] standards have been universally implemented by the contract security industry, proprietary security, and law enforcement'' (p. 151).

Underwriters Laboratories, FM Global, and Wernock Hersey International

Organizations, such as Underwriters Laboratories Inc. (UL), FM Global,* and Wernock Hersey International (WHI), conduct research, test products, and document the results, then create standards from this information.

UL, established in 1894, is one of the most widely recognized and accepted testing laboratories in the United States. FM Global has a national testing laboratory that has been in existence for over 100 years. WHI was established in Canada in 1888 and provides fire testing and technical services to industry and government. These laboratories' testing consists of determining whether a particular product presents any safety hazard to the public and whether it performs as specified for its intended use. The actual areas of investigation may vary from laboratory to laboratory. Also, local codes may specify the laboratory by which a product must be tested. As with building codes, testing requirements tend to vary on a regional basis.

---

*Formerly known as Factory Mutual.

The major commercial insurance companies often require listing by these particular laboratories or conformity to their standards as a prerequisite for obtaining casualty insurance. In fact, two of these organizations were created for this purpose: UL was originally founded by the fire insurance industry, and FM Global today is made up of three large mutual property insurance companies. The influence of these laboratories is considerable, then, because meeting their standards is of critical importance for businesses seeking to obtain adequate insurance.

American Society for Testing Materials

The ASTM Publications 1994 catalog states that ''from the work of 131 technical standards-writing committees, the American Society for Testing Materials (ASTM) publishes standard specifications, tests, practices, guides, and definitions for materials, products, systems, and services. ASTM also publishes books containing reports on state-of-the-art testing techniques and their possible applications'' (ASTM, 1994).

The ASTM F-12 Committee on Security Standards and Equipment, according to Cumming (1992), is involved in ''the harmonization, extension, codification, and production of new standards for the protection of people and property. It is probably the only organization in the security field that is taking a global view of minimum manufacturing, installation, and maintenance standards for systems. It is also involved in producing guidelines for the methods by which protection can be provided'' (p. 25).

Other Building Institutes, Associations, and Societies

Groups whose quality criteria affect building standards include the American Institute of Architects (AIA); the Construction Specifiers Institute (CSI); the American Iron and Steel Institute (AISI); the American Institute of Steel Construction (AISC); the American Concrete Institute (ACI); the National Association of Architectural Metal Manufacturers; the Architectural Aluminum Manufacturers Association (AAMA); the American Plywood Association (APA); the Architectural Woodworking Institute (AWI); the Builders Hardware Manufacturers Association; the National Wood Window and Door Association (NWWDA); the Air Conditioning and Refrigeration Institute (ARI); the American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE); the National Association of Plumbing-Heating-Cooling Contractors (PHCC); the American Society of Mechanical Engineers (ASME); the American Society of Civil Engineers (ASCE); and the Steel Door Institute (SDI). The SDI, for example, proposes that fire-rated openings specify an appropriately labeled fire doorframe and fire door, an approved door closer, an approved latching device, and appropriate steel hinges. ''Elevator Safety Features'' (see Chapter 6) explains how the ASME's safety codes have positively affected the nation's elevator and escalator safety records.

Security Associations

Security Industry Association

In the words of Nesse and Williams (1994),

> The Security Industry Association (SIA) is a national trade association comprised of manufacturers, distributors and service companies in the security industry. SIA works to further the growth, expansion and professionalism of the industry through various programs, including the development of standards. SIA operates an ANSI-approved Standards Program, which develops consensus standards directly through subcommittees and provides liaison to and from other standards-writing bodies. SIA develops product performance, application, and communication standards relating to the alarm industry.

National Association of Security Companies

The National Association of Security Companies (NASCO) was founded in 1972 as the Committee of National Security Companies (CONSCO). ''Today NASCO is at the forefront of efforts to set meaningful standards for the private security industry, and monitors state and federal legislation proposed for laws and regulations that might affect the quality and effectiveness of private security services'' (NASCO, 1994). The organization's goals clearly state its mission:

1. To maintain and upgrade standards within the industry.
2. To participate in the formulation and revision of legislation affecting the industry and the public.
3. To foster uniformity of regulation throughout the United States.
4. To increase public awareness of the distinction between private security and public law enforcement, as well as the complementary and cooperative functions they share.
5. To publicize the valuable services provided by hundreds of thousands of private security officers across the country.

ASIS International

ASIS International is the preeminent global organization for professionals responsible for security, including managers and directors of security. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security practices by developing educational programs and materials that address broad security concerns. ASIS also advocates the role and value of the security management profession to government, business, the media, and the public.

ASIS has chapters, which provide networking and professional development opportunities for security practitioners in a local setting. ASIS' councils provide support to, and enhancement of, ASIS educational programs and materials designed to meet the needs of professionals with specific security concerns and issues inherent to a specific industry. In particular, the ASIS Commercial Real Estate Council ''investigates and reports on security problems in offices and multiresidential dwellings. The council encourages communication among building designers, construction personnel, and security personnel'' (ASIS *Dynamics*, 2002, p. 41).

In addition, ASIS administers the Certified Protection Professional (CPP) Board credential, which indicates that an individual has been Board Certified in Security Management. It is the security profession's highest recognition of practitioners and provides an objective measure of an individual's knowledge and competency in security management. Certification is awarded based upon experience and passing of an examination that tests broad-based security knowledge. Ongoing professional development is required to maintain the credential. The Professional Certification Board (PCB) is responsible for development and implementation of the CPP program. Commencing in 2003, the PCB will also administer certification programs for physical security professionals and investigation professionals.

Fire Alarm and Burglar Alarm Trade Associations

The National Burglar and Fire Alarm Association (NBFAA) and the Automatic Fire Alarm Association (AFAA) represent fire alarm equipment installers and dealers; the NBFAA also represents burglar alarm installers.

Lighting and Electrical Associations

The Illuminating Engineering Society (IES) is concerned with lighting standards and practices. Electrical components and products are the focus of the Electronic Industries Association (EIA). The Institute of Electrical and Electronic Engineers (IEEE), the world's largest technical professional society, develops standards and directs its attention to advancing the theory and practice of electrical, electronics, and computer engineering. The National Electrical Contractors Association (NECA) is concerned with electrical standards for contractors.

The National Electrical Manufacturers Association (NEMA) has a division entitled Signaling, Protection and Communications, which maintains close liaison with related organizations, professional societies, trade associations, and approval and code writing agencies such as NFPA and NECA. It develops industry manufacturing standards on nomenclature ratings, performance and testing aimed at providing input to UL, FM Global, NFPA, WHI, authorities having jurisdiction, model building code organizations, and ANSI. It also has a continuing program for the definition and distribution of industry manufacturing standards and publications that address specific industry or user needs. Particular emphasis is placed on fire protective signaling systems and devices, security signaling systems and devices, and paging systems and devices (NEMA, 1994).

National Conference of States on Building Codes and Standards, Inc.

The National Conference of States on Building Codes and Standards, Inc. (NCSBCS, 1994, p. vii) states that it:

> Promotes the development of an efficient, cooperative system of building regulation in order to ensure the public's safety in all residential and commercial

> buildings. The Conference also works for the acceptance of new building construction technologies; a uniform, national system of education and certification for building regulatory personnel; accountability in the design, construction, and inspection of buildings; public awareness of building regulatory personnel and the work they do; and interstate acceptance of modular and industrialized buildings. As a membership organization, NCSBCS provides state and local building officials, architects and engineers, building contractors, manufacturers of building materials and equipment, national associations and corporations, federal government officials, consumers, and its governor-appointed delegate members with a forum for coordinating their building code and public safety interests and for discussing construction codes and regulations.

NCSBCS publishes the *State Directory of Building Codes and Regulations*. This directory ''is a guide to the building codes and regulations that are adopted and enforced in the 50 United States and the District of Columbia for new construction and alterations'' (NCSBCS, 1994, p. 1). It lists building, mechanical, plumbing, electrical, energy, gas, fire prevention, life safety, and accessibility codes with their technical basis (the model code or standard on which the state code is based), their applicability—the types of buildings to which the code applies, their preemptive application—whether the code is mandatory or voluntary, and whether local amendments are allowed, the state agency responsible for administering the code, and the state agency responsible for enforcing the code. Also included are a brief summary of the state's code, the code change cycle, and a list of locations where state codes can be purchased.

Management-Related Associations

Institute of Real Estate Management

The Institute of Real Estate Management (IREM), an affiliate of the National Association of Realtors, is an organization, founded in the 1933, of property and asset managers in the United States and Canada. It produces books, courses, seminars, periodicals, audiovisuals, and other educational activities and materials. The Institute offers courses that teach a full range of property management duties, from carrying out basic functions to owning and operating a management company. Through its property manager certification program, IREM sets widely adopted standards of professional conduct and ethics for its members.

Building Owners and Managers Association International

Founded in 1907, the Building Owners and Managers Association (BOMA) International is the oldest and largest trade association serving commercial real estate professionals. It is a federation of over 100 local associations in the United States, Canada, and the world. Its members include a wide cross-section of the building community including owners and managers of high-rise office buildings. Other members plan, develop, market, and lease office buildings and provide the goods and services to operate those properties. ''The mission of BOMA is to actively and responsibly represent and promote the interests of the commercial real-estate industry through effective leadership and advocacy through the collection, analysis and dissemination of information, and through professional development'' (BOMA International, 1994, p. 4).

Other Societies and Organizations

In addition to the professional societies and organizations already mentioned, there are various other groups in the United States that contribute to the development and maintenance of security and fire life safety standards. In the security field, these include the Academy of Security Educators and Trainers, the International Foundation for Protection Officers, the International Society of Crime Prevention Educators, the National Crisis Prevention Institute, the National Council of Investigation and Security Services, and the International Association of Chiefs of Police. In the fire life safety field, the National Fire Academy (NFA) and the United States Fire Administration (USFA) both report to the Federal Emergency Management Agency (FEMA) and make contributions to public fire safety. NFA, through its National Emergency Training Center, provides extensive training in fire-related disciplines and the application and enforcement of fire codes. The USFA, among other federal fire policy and coordination efforts, maintains an extensive fire data and analysis program.

The purpose of the Society of Fire Protection Engineers (SFPE, 2002) is ''to promote and advance the science of fire protection engineering and its allied fields, to maintain the high ethical and professional standards among our members, and to foster and develop fire protection engineering education.'' The Society publishes *The Journal of Fire Protection Engineering*, *Fire Protection Engineering* magazine, technical reports, reference books, and conference proceedings.

The National Institute for Certification in Engineering Technologies (NICET) is a nonprofit organization sponsored by the National Society of Professional Engineers. NICET is an examining body whose objective ''is to provide nationally applicable, widely recognized certification programs by which engineering technicians and technologists can demonstrate competence and achievement in their areas of technical expertise'' (NICET, 1992). By doing this, it promotes high standards of safety and codes of responsibility for NICET-certified persons working in the engineering field.

The University of Maryland and the Worcester Polytechnic Institute are two other institutions that indirectly have made considerable contributions to the development of laws, codes, and standards by providing degree programs in fire protection engineering. In addition, organizations like the National Crime Prevention Institute, and various universities that offer security-related degree courses, have contributed greatly to the professionalism of the security industry.

Applicability of Laws, Codes, and Standards

The laws, standards, and codes mentioned in this chapter can apply to both security and fire life safety in high-rise buildings; however, fire life safety operations are more strictly regulated than security operations. For example, building codes address security as well as fire life safety issues, but, in the United States, ''more than 50 percent of a modern building code usually refers in some way or another to fire protection'' (Cote and Grant, 1997, pp. 1-43, 1-44).

Fire Life Safety Measures

Many of the fire life safety requirements for high-rise buildings are governed by state and local codes; the widely accepted NFPA codes and standards; and requirements (particularly by building insurers) to use equipment listed, recognized, or certified by recognized testing groups such as NIST and UL. For example, modern high-rise buildings are required by the authority having jurisdiction to install and maintain adequate fire protection systems and to establish and maintain a pre-fire plan that includes the training of occupants as to what they should do in case of a fire or other emergency. Any building owner and manager not complying is at considerable risk of sanctions and fines and to significant liability risk if injuries, deaths, or property loss result from inadequate safety measures.

Also, OSHA clearly holds building owners and managers responsible to ensure that adequate life safety precautions are taken to provide a safe and healthful working environment and to keep the premises reasonably safe for business visitors.

Security Measures

Private security firms—those providing guard and patrol services, private investigators, alarm services, and armored car services—are frequently regulated by state and local governments. However, ''America has very few national *mandatory* laws, statutes, or standards relating to security in the commercial, industrial, and private sectors'' (Cumming, 1992, p. 24). As Post and Kingsbury (1991) remind us, ''It is also generally recognized that the security field does not have what might be classified as 'generally accepted security practices' comparable to the 'generally accepted accounting practices' that guide the accounting profession'' (p. 222).

There have been attempts to promote standards at the state and national levels, but this has met with resistance, particularly within the contract security industry. *The Hallcrest Report II* states, ''Many smaller security firms view standards and regulation as a means to promote increased market share for larger firms that are better able to meet the requirements'' (Cunningham, Strauchs, and Van Meter, 1990, p. 152). This report further notes that in the United States, only 14 of the 50 states require any training for unarmed security staff. (The vast majority of security personnel working in high-rise office buildings are unarmed.) Also, there are no standardized minimum screening standards for private security officers who work throughout the 50 states.

For security, ''It is difficult to protect against legal actions regardless of what measures of protection are taken unless there is a basic agreement about what constitutes *enough* security.... There has not, however, been a national effort developed to undertake the process of developing standards for the security industry as a whole because of the complexity of the issue'' (Post, 1991, p. 221). The security profession itself is divided over the question of whether developing additional standards will allow an objective determination of ''adequate security.''

In the high-rise environment, part of the problem lies in the fact that virtually every building is different and no two security professionals will always agree on what constitutes adequate security for a particular facility. So many recommendations are *subjective* determinations by individuals with varying opinions about the value of particular security measures. For example, one security professional may rely heavily on using closed-circuit television systems to observe security violations, whereas another may prefer concentrated deployment of security personnel; one may emphasize the use of access cards to control entry to a facility, whereas another may prefer security staff to screen tenants and visitors. Even if security professionals were able to agree on what an adequate security level is for a particular facility, inevitably budgetary considerations still must be taken into consideration. A fully occupied, financially sound building in a thriving business district will be more likely to invest money in its security program than a partially occupied building that can only charge lower-than-market rents because the facility has deteriorated and is in an area many businesses have vacated. The dilemma for the building owner or manager is that the latter building may actually have a greater need for security than the former.

References

ASIS *Dynamics* (ASIS International, Alexandria, VA, 2002).

ASTM Publications 1994 Catalog (American Society for Testing and Materials, Philadelphia, 1994).

Atlas, Randall, ''Will ADA handicap security?'' (*Security Management*, Arlington, VA, March 1992).

Black's Law Dictionary, 6th ed. (West Publishing, St. Paul, 1990).

BOMA International, ''Cornerstone of the commercial real estate industry,'' *Building Owners and Managers Association International* (BOMA International, Washington, D.C., 1994).

Carson, Wayne G. ''Chip,'' ''Who sets means of egress standards?'' (*NFPA Journal*, (National Fire Protection Association, Quincy, MA, September/October 1993).

Cassidy, Kevin A., ''Conflicting codes and how to deal with them,'' *Fire Safety and Loss Prevention* (Butterworth–Heinemann, Stoneham, MA, 1992).

Cote, Arthur E., and Casey C. Grant, ''Building and fire codes and standards,'' *Fire Protection Handbook*, 18th ed. Arthur E. Cote, Editor-in-Chief (NFPA, Quincy, MA, 1997).

Cumming, Neil, ''Stages of system design, selection, and installation,'' *Security: A Guide to Security System Design and Equipment Selection and Installation*, 2nd ed. (Butterworth–Heinemann, Stoneham, MA, 1992).

Cunningham, William C., John J. Strauchs, and Clifford W. Van Meter, ''Introduction,'' *The Hallcrest Report II: Private Security Trends 1970–2000* (Butterworth–Heinemann, Stoneham, MA, 1990). Information obtained from the Private Security Advisory Council to the Law Enforcement Assistance Administration, U.S. Department of Justice, 1973–1977.

Cunningham, William C., John J. Strauchs, and Clifford W. Van Meter, ''Security personnel issues,'' *The Hallcrest Report II: Private Security Trends 1970–2000* (Butterworth–Heinemann, Stoneham, MA, 1990). Information obtained from the Private Security Advisory Council to the Law Enforcement Assistance Administration, U.S. Department of Justice, 1973–1977.

Fire Protection Handbook, 18th ed. Arthur E. Cote, Editor-in-Chief (National Fire Protection Association, Quincy, MA, 1997).

Fischer, Robert J., and Gion Green, ''Fire protection, safety, and emergency planning,'' *Introduction to Security*, 6th ed. (Butterworth–Heinemann, Stoneham, MA, 1998).

Garboden, Clif, ''The life safety code: responding to change,'' (*NFPA Journal*, National Fire Protection Association, Quincy, MA, March/April 1994).

ICBO, *Publications List* (International Conference of Building Officials, Whittier, CA, 1993).

Lathrop, James K., and David Birk, ''Building life safety with codes,'' *NFPA Journal* (National Fire Protection Association, Quincy, MA, May/June 1992).

NASCO, *Information Brochure* (National Association of Security Companies, Memphis, TN, 1994).

NCSBCS, *State Directory of Building Codes and Regulations* (National Conference of States on Building Codes and Standards, Inc., Herndon, VA, 1994).

NEMA, *Signaling, Protection and Communications Section Roster* (National Electrical Manufacturers Association, Washington, D.C., 1994).

Nesse, Ted, and Virginia Williams, *Putting Security Product Standards to Work for You* (presentation by the Security Industry Association to the International Security Conference in Las Vegas, January 1994).

NFPA web site, http://www.nfpa.org, NFPA 5000™, *Building Code* (National Fire Protection Association, Quincy, MA, 2002).

NICET, *General Information Booklet*, Engineering Technician and Technologist Certification Programs (National Institute for Certification in Engineering Technologies, Alexandria, VA, 1992).

NIST, *List of Publications by Subject Category*, SP305-22 Abridged (U.S. Department of Commerce, National Institute of Standards and Technology, Washington, D.C., revised July 1991).

OSHA, *General Industry: Safety and Health Regulations*, Title 29 of the Code of Federal Regulations, Part 1910 (U.S. Department of Labor, Washington, D.C., 1974).

POA, ''The security aspects of OSHA,'' *Protection of Assets Manual*, Vol. I, Timothy L. Williams, editor (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, 1991).

POA, ''Standards in asset protection,'' definition from *Webster's New Universal Unabridged Dictionary*, 2nd ed. (Used with permission of POA Publishing, LLC, Los Angeles, CA, 323/663-4887. Original copyright from the Merritt Company, 1991).

Post, Richard S., and Arthur A. Kingsbury (revised by Richard S. Post with Arthur A. Kingsbury and David A. Schachtsiek), *Security Administration: An Introduction to the Protective Services*, 4th ed. (Butterworth–Heinemann, Stoneham, MA, 1991).

SBCCI, *1993 Products Catalog* (Southern Building Code Congress International, Birmingham, AL, 1993).
Schum, John L., ''Codes and Standards,'' *Electronic Locking Devices: Toolbook Guides for Security Technicians* (Butterworth–Heinemann, Stoneham, MA, 1989).
SFPE, *Your Guide to the Society, Benefits of Membership, Canon of Ethics, Committees and Task Groups, Chapters, Corporate 100 Program* (Society of Fire Protection Engineers, Bethesda, MD, 2002).
Wilson, Dean K., ''Certifying competency'' (*NFPA Journal*, National Fire Protection Association, Quincy, MA, May/June, 2001).
Wolf, Alisa, ''NFPA 5000 full-service building code'' (NFPA *Journal*, National Fire Protection Association, Quincy, MA, March/April 2002).

Additional Reading

Protection of Assets Manual, Timothy L. Williams, editor (POA Publishing, LLC, Los Angeles, CA, 323/663-4887).

Appendix 12-1 Security and the Law*

The pursuit of security itself involves contact with others. In each such contact, there is a delicate consideration of conflicting rights. Whereas public police and protection services derive their authority to act from a variety of statutes, ordinances, and orders enacted at various levels of government, private police function essentially as private citizens. Their authority to so function is no more than the exercise of the right of all citizens† to protect their own property. Every citizen has common law and statutory powers that include arrest, search, and seizure. The security officer has these same rights, both as a citizen and as an extension of an employee's right to protect their employer's property. Similarly, this common-law recognition of the right of defense of self and property is the legal underpinning for the right of every citizen to employ the services of others to protect property against any kind of incursion by others.

The broad statement of such rights, however, in no way suggests the full legal complexities that surround the question. In common law, case law, and state statutes, as well as in the basic authority of the U.S. Constitution, privileges and restrictions further defining these rights abound. The body of law covering the complex question of individual rights of defense of person and property contains many apparent contradictions and much ambiguity. In their efforts to create a perfect balance between the rights of individuals and the needs of society, the courts and the legislatures have had to walk a narrow path. As the perception of society's needs changed or as the need for the protection of the individual became more prominent, a swing in the attitudes of the courts and the legislatures became apparent. This led to some confusion especially among those with little or no knowledge of the law.

It is of enormous value, therefore, for everyone engaged in security to pursue the study of both criminal and civil law. Such a study is aimed neither at acquiring a law degree nor certainly at developing the skills to practice law. It is directed toward developing a background in those principles and rules of law that will be useful in the performance of the complex job of security. [*Author's Note*: The following study of criminal and civil law is purposely aimed at the private security officer. The reason for this approach is that in a high-rise office building the primary agent for implementing the security program, which provides for the protection of lives and property, is the security staff. For simplicity, the term *security officer* represents *security staff*.]

---

*This entire appendix is reprinted, with some modifications and additions, from Chapter 6 in *Introduction to Security* by Robert J. Fischer and Gion Green, 6th ed. (used with permission of Butterworth–Heinemann, Woburn, MA, 1998). Definitions were largely obtained from *Black's Law Dictionary*, 6th ed., by The Publisher's Editorial Staff and co-authors Joseph R. Nolan and Jacqueline M. Nolan-Haley (West Publishing, St. Paul, 1990).

†In the high-rise setting such citizens may include building owners, managers, security directors, fire safety directors, building maintenance departments, security officers, and the individual tenants themselves. A *security officer* is a person who has been commissioned or authorized to perform duties primarily concerned with protection of the lives and property of people working within the private sector.

Without some knowledge of the law, security officers frequently cannot serve their clients' interests. They may subject themselves or their employers to ruinous lawsuits through well-meaning but misguided conduct.

Since for the purposes of this review of *Security and the Law* we are primarily interested in civil and criminal law—both have major implications for the security officer and the industry—it is useful to distinguish between them.

Criminal Law

Criminal law deals with offenses against society (corporations are of course part of society and can be either criminals or victims). Every state has its criminal [or penal] code that classifies and defines criminal offenses [and prescribes the punishment to be imposed for such conduct]. Criminal law is the result of a jurisdiction either using common law, which was adopted from English traditions, or passing specific legislation called *statutory law*. (In some jurisdictions both are used.) When criminal offenses are brought into court, the state takes an active part, considering itself to be the offended party.

Civil Law

Civil law, on the other hand, has more to do with the personal relations and conflicts between individuals, corporations, and government agencies. Broken agreements, sales that leave a customer dissatisfied, outstanding debts, disputes with a government agency, accidental injuries, and marital breakup all fall under the purview of civil law. In these cases, private citizens, companies, or government agencies are the offended parties, and the party found at fault is required to directly compensate the other party.

Security, Public Police, and the U.S. Constitution

The framers of the U.S. Constitution with their grievances against England uppermost in mind when they were creating a new government were primarily concerned with the manner in which the powerless citizen was or could be abused by the enormous power of government. The document they created was concerned, therefore, not with the rights of citizens against each other but rather with those rights with respect to federal or state action.

Breaking and entering by one citizen on another may be criminal and subject to tort action (a civil wrong not involving a breach of contract), but it is not a violation of any constitutional right. Similar action by public police is a clear violation of Fourth Amendment rights and, as such, is expressly forbidden by the Constitution.

The public police have substantially greater powers than do security personnel to arrest, detain, search, and interrogate. Where security people are, as a rule, limited to the premises of their employer, public police operate in a much wider jurisdiction.

At the same time, the public police are limited by various restrictions imposed by the Constitution. Although the issue is not entirely clear, private police are not as a rule touched by these same restrictions.

Public police are limited by federal statutes that make it a crime for officials to deny others their constitutional rights. The Fourth and Fourteenth Amendments are most frequently invoked as the cornerstones of citizen protection against arbitrary police action. The exclusion of evidence from court action is one penalty paid by public police for violation of the search provision of the Fourth Amendment. For the most part private police are not affected by these restrictions.

Sources of Law

All law, whether civil or criminal, has its source in common law, statutory law, or case law (judge-made). The following discussion can be applied to either civil or criminal law. Although today's criminal law is primarily statutory, civil law, particularly tort law, is essentially judge-made and created in response to changing social conditions.

Common Law

At one time, the principal source of law in the United States was English common law. Although common law may also refer to judge-made (as opposed to legislature-made) law, to law that originated in England and grew from ever-changing custom, or to written Christian law, the term is most commonly used to refer to the English common law that has been changed to reflect specific U.S. customs.

Some states have preserved the status of common-law offenses for their criminal codes, while others have abolished common law and written most of the common-law principles into statutes. Some states are still using both common and statutory law.

Case Law

When a case goes to court, the outcome is usually governed by prior court opinions of similar nature. Those preceding cases have usually been resolved in such a way as to put to rest any doubts as to the meaning of the governing statutes or common-law principles as well as to clarify the attitude of the courts regarding the legal issue involved. The court opinions used have established precedent that will guide other courts in subsequent cases based on the same essential facts. Since the facts in any two cases are rarely precisely the same, opposing attorneys cite preceding cases whose facts more readily conform to their own theory or argument in the case at hand. They, too, build their case on precedents, or case law already established. It is up to the court to choose one of the two sides or to establish its own theory. This is a very significant source of our law essentially becoming common law.

Because society is in a constant state of change, it is essential that the law adapt to these changes. At the same time, there must be stability in the law if it is to guide behavior. People must know that the law as it appears today will be the same tomorrow, that they will not be punished tomorrow for behavior that was permitted today. They need to know that each decision represents a settled statement of the law and they can conduct their affairs accordingly. So the published decisions of the appellate courts become guides to the meaning of the law and in effect become the law itself. Their judgments flesh out legislative enactments to give them clear outlines. Such interpretations based on precedents are never regarded lightly and in legal terms are ''*stare decisis*'' or ''let the decision stand.''

This does not mean that each decided case locks the courts forever into automatic compliance. Conditions that created the climate of the earlier decision may have changed, rendering the precedent invalid. And there are cases decided in such a narrow way that they cannot be applied beyond that case. Further, there is nothing that prevents review of a decision at the time of a later case. If the court agrees that the earlier case was in error, it may not be bound by the earlier precedent.

So it can be seen that case law is an important source of the law; it provides a climate of legal stability without closing the law to responsiveness to changing needs.

Statutory Law

Federal and state legislatures are empowered to enact laws that describe crimes. The authority to do so emanates from the U.S. Constitution and from the individual state constitutions. These constitutions do not specifically establish a body of criminal law. In general, they are more concerned with setting forth the limitations of governmental power over the rights of individuals. But they do provide both for the authority of legislative action in establishing criminal law and for a court system to handle these as well as civil matters.

Much criminal law is, in fact, the creation of the legislatures. The legislatures are exclusively responsible for making and defining laws. The courts may find some laws unconstitutional or vague and thus set them aside, but they may not create statutes. Only the legislatures are empowered to do that.

The Power of Security Personnel

Security personnel are generally limited to the exercise of powers possessed by every citizen. There is no legal area where the position of a security officer as such confers any greater rights, powers, or privileges than those possessed by every other citizen. A few states go contrary to this norm and confer additional arrest powers for security personnel after the completion of a designated number of hours of training.[1] As a practical matter, if officers are uniformed they will very likely find that in most cases people will comply with their requests. Many people are aware neither of their own rights nor of the limitations of the powers of a security officer. Thus security officers can obtain compliance to directives that may be, if not illegal, beyond their power to command. In cases where security officers have unwisely taken liberties with their authority, the officers and their employers may be subject to the penalties of civil action. The litigation involved in suing security officers and their employers for a tort is slow and expensive, which may make such recourse improbable for the poor and for those unfamiliar with their rights. But the judgments that have been awarded have had a generally sobering effect on security professionals and have probably served to reduce the number of such incidents. Criminal law also regulates security activities. Major crimes such as battery, manslaughter, kidnapping, and breaking and entering—any one of which might be encountered in the course of security activities—are substantially deterred by criminal sanctions.

Further limitations may be imposed on the authority of a security force by licensing laws, administrative regulations, and specific statutes directed at security activities. Operating contracts between employers and security firms may also specify limits on the activities of the contracted personnel.

Classes of Crimes

A crime has been defined as a voluntary and intentional violation by a legally competent person of a legal duty that commands or prohibits an act for the protection of society.[2]

Since such a definition encompasses violations from the most trivial to the most disruptive and repugnant, efforts have long been made to classify crimes in some way. In common law, crimes are classified according to seriousness from treason (the most serious) to misdemeanors (the least serious). Most states do not list treason separately and deal with felonies as the most serious crimes and misdemeanors as the next in seriousness, with different approaches to the least serious crimes, those known as infractions in some jurisdictions, less than misdemeanors in others, and petty offenses in still others. It will become apparent why security specialists should understand the nature of a given crime and its classification since such considerations will be important in determining

- Power to arrest
- The need to use force in making the arrest
- Whether to and what to search
- Various other considerations that must be determined under possibly difficult circumstances and without delay

Serious crimes like murder, rape, arson, armed robbery, and aggravated assault are felonies. Misdemeanors include charges such as disorderly conduct and criminal damage to property.

Felonies

Felonies comprise the more serious crimes. This is true in modern U.S. law as far as it goes, but clearly the definition of felony must be pinned down more precisely than that if it is to be used as a classification of crime and if courts are to respond differently to felons than they would to another type of law breaker. The definition of a felony is by no means standard throughout the United States. In some jurisdictions, there is no distinction between felonies and misdemeanors.

The federal definition of a felony is an offense punishable by death or by imprisonment for a term exceeding one year. The test, then, for a felony is the length of time that punishment is imposed on the convicted person.

A number of states follow the federal definition. In those states, a felony is a crime punishable by more than a year's imprisonment. The act remains a felony whatever the ultimate sentence may actually be. Other states provide that, ''[a] felony is a crime punishable with death or by imprisonment in the state prison.'' This definition hinges on the place of confinement rather than, as in the federal description, the length of confinement.

Some states bestow broad discretionary powers on the judge by providing that certain acts may be considered either a felony or a misdemeanor depending on the sentence. The penalty clauses in the statutes thus involved specifically state that if the judge should sentence the defendant to a state prison, the act for which he was convicted shall be a felony (under the state definition of a felony) but if the sentence be less than such confinement the crime shall be a misdemeanor.

The distinction can be very important. In states where arrest by private citizens (for example, security personnel) is covered by statute, an arrest may be made only where the offense is committed in the presence of the arrester. In the case of arrest for a felony, the felony must in fact have been committed (though not necessarily in the presence of the arrester), and there must be reasonable grounds to believe the person arrested committed it. In other words, security employees, unlike police officers, act at their own peril.

A police officer has the right to arrest without a warrant where he or she reasonably believes that a felony has been committed and that the person arrested is guilty, even if, in fact, no felony occurred. A private citizen, on the other hand, is privileged to make an arrest only when he or she has reasonable grounds for believing in the guilt of the person arrested and a felony has in fact been committed.[3]

Some states, however, do allow for citizen arrest in public-order misdemeanors. Making a citizen's arrest, which must be recognized as the only kind of arrest that can be made by a security officer, is a privilege, not a right, and as such is carefully limited by law. Such limitation is enforced by the ever-present potential for either criminal prosecution or tort action against the unwise or uninformed action of a security professional.

Private Security Powers

Arrest

Arresting a person is a legal step that should not be taken lightly. A citizen's power to arrest another is granted by common law and in many jurisdictions by statutory law. In most cases, it is best to make an arrest only after an arrest warrant* has been issued. Most citizens' arrests occur, however, when the immediacy of a situation requires arrest without a warrant. The exact extent of citizen's arrest power varies, depending on the type of crime, the jurisdiction (laws), whether the crime was committed in the presence of the arrester, or the status of the citizen (strictly a private citizen or a commissioned officer).

In most states, warrantless arrests by private citizens are allowed when a felony has been committed and reasonable grounds exist for believing that the person arrested committed it. Reasonable grounds means that the arrester acted as would any average citizen who, having observed the same facts, would draw the same conclusion. In some jurisdictions, a private citizen may arrest without reasonable grounds as long as a felony was committed.

Most states allow citizen's arrest for misdemeanors committed in the arrester's presence. A minority of states, however, adhere closely to the common-law practice of allowing misdemeanor arrests only for offenses that constitute a breach of the peace and that occur in the arrester's presence.

Although the power of citizen's arrest is very significant in the private sector because it allows security officers to protect their employer's property, there is little room for errors of judgment. The public police officer is protected from civil liability for false arrest if the officer has probable cause to believe a crime was committed, but the private officer (citizen) is liable if a crime was not committed regardless of the reasonableness of the belief. This liability is because a citizen's arrest generally can be made only if a crime has definitely been committed.

Detention

Detention is a concept that has grown largely in response to the difficulties faced by merchants in protecting their property from shoplifters and the problems and dangers they face when they make an arrest. Generally detention differs from arrest in that it permits a merchant to detain a suspected shoplifter briefly without turning the suspect over to the police. An arrest requires that the arrestee be turned

---

***Black's Law Dictionary* defines an *arrest warrant* as ''a written order of the court which is made on behalf of the state, or United States, and is based upon a complaint issued pursuant to statute and/or court rule and which commands [a] law enforcement officer to arrest a person and bring him before [a] magistrate.''

over to the authorities as soon as practicable and in any event without unreasonable delay.

The privilege of detention is, however, subject to some problems. There must be probable cause to believe theft already has taken place, or is about to take place, before a merchant may detain anyone. Probable cause is an elusive concept and one that has undergone many different interpretations by the courts. It is frequently difficult to predict how the court will rule on a given set of circumstances that may at the time clearly indicate probable cause to detain. Second, reasonableness must exist both in time and manner of the detention or the privilege will be lost.

Interrogation

No law prohibits a private person from engaging in conversation with a willing participant. For public law enforcement, should the conversation become an interrogation, the information may not be admissible in a court of law. The standard is whether the statements were made voluntarily.

A statement made under duress is not regarded as trustworthy and is therefore inadmissible in court. This principle applies equally to police officers and private citizens. A confession obtained from an employee by threatening loss of job or physical harm would be inadmissible and would also make the interrogator liable for civil and criminal prosecution.

The classic cases involving interrogation, generally applied to only public law enforcement officers, are *Escobedo v. State of Illinois*[4] and *Miranda v. Arizona*.[5] Today the *Miranda* case has become the leading case recognized by most American citizens in reference to ''their rights.'' On March 13, 1963, Ernesto Miranda was arrested at his home and taken to a Phoenix police station. There he was questioned by two police officers who during Miranda's trial admitted that they had not advised him that he could have a lawyer present. After two hours of interrogation, the officers emerged with a confession. According to the statement, Miranda had made the confession ''with full knowledge of my legal right, understanding any statement I make may be used against me.'' His confession was admitted into evidence over defense objections during his trial. He was convicted of kidnapping and rape. On appeal, the Arizona Supreme Court upheld the conviction indicating that Miranda did not specifically request counsel. The U.S. Supreme Court reversed the decision based on the fact that Miranda had not been informed of his right to an attorney, nor was his right not to be compelled to incriminate himself effectively protected.

Although the principle behind the *Miranda v. Arizona* decision was the removal of compulsion from custodial questioning (questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of freedom), it generally only applies to public law enforcement officers. The police officer must show that statements made by the accused were given after the accused was informed of the facts that speaking was not necessary, that the statements might by used in court, that an attorney could be present, and that if the accused could not afford an attorney, one would be appointed for the accused prior to questioning. These Miranda warnings are not necessary unless the person is in custody or is deprived of freedom. Based on this distinction, most courts agree that private persons are not generally required to use Miranda warnings because they are not public law-enforcement officers.

Search and Seizure

A search may be defined as an examination of persons and/or their property for the purpose of discovering evidence of guilt in relation to some specific offense. The observation of items in plain view is not a search as long as the observer is legally entitled to be in the place where the observation is made. This includes public property and private property that is normally open to the public, for example, shopping malls, retail stores, hotel lobbies, and so on.

Common law says little about searches by private persons and is inconclusive. Searches by private persons, however, have been upheld by the courts where consent to search was given and where searches were made as part of a legal citizen's arrest. The best practice to follow is to contact police officials who can then ask for a search warrant* to search as part of an arrest. Since searches often need to be conducted on short notice without the aid of a police officer; however, it is important to understand several factors.

First, in a consent search, the searcher must be able to show that the consent was given voluntarily. Second, the search cannot extend beyond the area for which consent to search was given. It is advisable to secure a written agreement of the consent to search. Third, the consent must be given by the person who possesses the item. Possession, not ownership, is the criterion for determining whether a search was valid. Although many firms issue waivers to search lockers and other work areas, an [a security] officer must remember that the consent to search may be withdrawn at any time. If the consent is withdrawn, continuing a search might make the officer and the company liable for invasion of privacy. Some companies have solved this problem by retaining control over lockers in work areas. In this situation, workers are told that the lockers are not private and may be searched at any time.

A search made as a part of an arrest is supported by case law. In general, the principle of searching the arrestee and the immediate surroundings, defined as the area within which one could lunge and reach a weapon or destroy evidence, has been repeatedly held as constitutional. The verdict on searches incident to arrest by security officers is still mixed. In *People v. Zelinski*,[6] the California court disapproved of searches made incident to an arrest but did approve of searches for weapons for protective reasons. New York courts tend to support searches, indicating that private [security] officers, like their public counterparts, have a right to searches incident to an arrest. In general, it appears that unless the security officer fears that a weapon may be hidden on the arrestee, the officer should wait until the police arrive to conduct a search unless permission is given for such a search.

Even in the statutes governing retail shoplifting, the area of search is limited. Some states neither forbid nor condone searches; rather, they allow security personnel to investigate or make reasonable inquiries as to whether a person possesses unpurchased merchandise. In other states, searches are strictly forbidden, except looking for objects carried by the suspected shoplifter. Courts, however, generally favor protective searches where officers fear for their own safety.

***Black's Law Dictionary* defines a *search warrant* as ''an order in writing, issued by a justice or other magistrate, in the name of the state, directed to a sheriff, constable, or other officer, authorizing him to search for and seize any property that constitutes evidence of the commission of a crime, contraband, the fruits of a crime, or things, otherwise criminally possessed; or, property designed or intended for use or which is or has been used as a means of committing a crime.''

Exclusionary Rule

In a historic decision, the Supreme Court ruled that any and all evidence uncovered by public law enforcement agents in violation of the Fourth Amendment will be excluded from consideration in any court proceedings. That means all evidence, no matter how trustworthy or indicative of guilt, will be inadmissible if it is illegally obtained.

Unlike illegal searches conducted by public law enforcement officers, evidence secured by a private security officer conducting an illegal search is still admissible in either criminal or civil proceedings. In *Burdeau v. McDowell*,[7] the U.S. Supreme Court said, ''[i]t is manifest that there was no invasion of the security afforded by the Fourth Amendment against unreasonable searches and seizures, as whatever wrong was done was the act of individuals in taking property of another.'' If such evidence is admissible, why should private sector employees concern themselves with the legality of searches? Even though the evidence is admissible, security officers who conduct illegal searches may be subject to liability for other actions, including battery and invasion of privacy.

In summary, although public police are clearly limited by constitutional restrictions, generally private security personnel are not so limited. Provided that they act as private parties and are in no way involved with public officials, they are limited by criminal and civil sanctions but are not bound at this time by most constitutional restrictions.

Use of Force

On occasion, security personnel must use force to protect someone or to accomplish a legitimate purpose. In general, force may be used to protect oneself or others, to defend property, and to prevent the commission of a criminal act. The extent to which force may be used is restricted; no more force may be used than is reasonable under the circumstances. This means that deadly force or force likely to create great bodily harm will not be allowable unless the force being used by the assailant is also deadly force or force likely to create great bodily harm. If the force exceeds what is deemed reasonable, [security] officers and their employers are liable for the use of excessive force, which can range from assault and battery to homicide. This is the same degree of power extended to the ordinary citizen.

Self-defense

In general people may use reasonable force to protect themselves. The amount of force may be equal to, but not greater than, the force being used against them. In most states, a person can protect herself, except when that person was the initial aggressor. Most states allow self-defense to be used by a person against whom force is used.

Defense of Others

Security officers may protect others just as they protect themselves. However, two different approaches to defense of others are evident. In the first approach, the officer must try to identify with the attacked person. In this position, the officer is entitled to use whatever force would be appropriate if she were the person being attacked. If the officer happens to protect the wrong person—that is, the aggressor—the officer is liable regardless of his or her good intentions. In the second approach, the defender may use force when it is reasonable to believe that such force is necessary. In this case, the defender is protected from liability as long as he or she acted in a reasonable manner.

Defense of Property

In defense of property, force may be applied, but it must be short of deadly force, which is generally allowable only in cases involving felonious attacks on property during which loss of life is likely. As noted by Schnabolk, ''one may use deadly force to protect a home against an arsonist but the use of deadly force against a mere trespasser would not be permitted.''[8] Security officers acting in the place of their employers are empowered to use the same force that their employers are entitled to use.

Force Used during Arrest or Detention

Like the police, the private citizen security officer has the right to use reasonable force in detaining or arresting someone. Many states still follow the common-law principles that allow deadly force in the case of fleeing felons, but many others have restricted the use of deadly force. This restriction allows the use of deadly force only in cases where the felony is both violent *and* the felon is immediately fleeing.

Prevention of Crimes

To determine the amount of force a security officer may use to prevent crimes, the courts have considered the circumstances, the seriousness of the crime prevented, and the possibility of preventing the crime by other means. Under common law a person can use force to prevent a crime. The courts have ruled, however, that the use of force is limited to situations involving felonies or a breach of the peace and nonviolent misdemeanors do not warrant the use of force. Deadly force is justifiable in preventing a crime only if it is necessary to protect a person from harm.

Use of Firearms

Most states regulate the carrying of firearms by private citizens. Almost all states prohibit the carrying of concealed weapons, whereas only half of them prohibit carrying an exposed handgun. Although all states excuse police officers from these restrictions, some states also exempt private security officers. Even in states that prohibit carrying concealed or exposed handguns, there are provisions for procuring a license to carry weapons in this manner.

Civil Law: The Controller for Private Security

Tort Law: Source of Power and Limits

A *tort* is a civil action based on the principle that one individual can expect certain behavior from another individual. When the actions of one of the parties do not meet reasonable expectations, a tort action may result. In security applications, a [security officer] may take some action to interfere with the free movement of some person. There is a basis for a suit no matter whether the [security officer] knows the actions are wrong, or is unaware that the actions are wrong but acts in a negligent manner.

Thus tort law may be invoked for either an intentional or negligent act. In some cases, liability may be imposed even though an individual is not directly at fault. One branch of this doctrine is ''strict liability,'' and does not generally affect the security officer. Strict liability applies to the provider of defective or hazardous products or services that unduly threaten a consumer's personal safety. [In the high-rise setting, strict liability may be applicable to the incorrect installation and maintenance of security and fire life safety systems and equipment.] Vicarious liability, however, is of concern to enterprises that contract or employ security services. Vicarious liability is an indirect legal responsibility; for example, the liability of an employer for the actions of an employee.

Negligence: The Restatement of Torts[9] states that ''[it] is negligence to use an instrumentality, whether a human being or a thing, which the actor knows, or should know, to be incompetent, inappropriate or defective and that its use involves an unreasonable risk of harm to others.'' This statement has particular importance to security employers and supervisors in hiring, supervision, and training of employees.

In all cases of negligence, the plaintiff (the person who brings an action, the party who complains or sues) must prove the case by a preponderance of the evidence (more than 50 percent or ''more likely than not'') in all of the following areas:

1. An act or failure to act (an omission) by the defendant
2. A legal duty owed to the plaintiff by the defendant, the person defending or denying, and/or the party against whom relief or recovery is sought
3. A breach of duty by the defendant
4. A foreseeable injury to plaintiff
5. Actual harm or injury to the plaintiff

A relatively new concept in the area of negligence is comparative fault. This concept accepts the fact that the plaintiff may have contributed to her own injury, such as being in a restricted area or creating a disturbance or some hazard. In the past, the theory of contributory negligence prevented the plaintiff from collecting for injuries and so forth if she contributed somehow to his or her own injury. In comparative negligence, the relative negligence of the parties involved is compared, and the plaintiff who may have contributed to the injury may get some award for part of the injury for which she is not responsible.

Cases involving negligence in providing adequate security on the part of firms have been increasing. Recent cases have resulted in awards to plaintiffs in individual cases of over $1 million. More will be said about this issue in the next section entitled ''Security and Liability.''

Intentional Torts: An intentional tort occurs when the person who committed the act was able to foresee that the action would result in certain damages. The actor intended the consequences of the actions or at least intended to commit the action that resulted in damages to the plaintiff. In general, the law punishes such acts by punitive measures that exceed those awarded in common negligence cases.

The most common intentional torts are:

- *Assault:* Intentionally causing fear of harmful or offensive touching but without touching or physical contact. In most cases, courts have ruled that words alone are not sufficient to place a person in fear of harm and that the danger is imminent.
- *Battery:* Intentionally harmful or otherwise offensive touching of another person. The touching does not have to be direct physical contact but may instead be through an instrument such as a cane or rock. In addition, the courts have found battery to exist if ''something'' closely connected to the body, but not actually a part of the body, is struck.[10]
- *False imprisonment or false arrest:* Intentionally confining or restricting the movement or freedom of another. The confinement may be the result of physical

restraint or intimidation. False imprisonment implies that the confinement is for personal advantage rather than to bring the plaintiff to court. This is one of the torts most frequently filed against security personnel.

- *Defamation:* Injuring the reputation of another by publicly making untrue statements. Slander is oral defamation, while libel is defamation through the written word. The classic case of a security officer yelling ''Stop thief!'' in a crowded store has all the necessary elements for slander if the accused is not a thief. Although it is generally true that truth is an absolute defense in defamation issues, the courts may also look at the motivation. True statements published with malicious intent can be prosecuted in some jurisdictions.
- *Malicious prosecution:* Groundlessly instituting criminal proceedings against another person. To prove malice, the plaintiff must show that the primary motive in bringing about criminal proceedings was not to bring the defendant to justice.
- *Invasion of privacy:* Intruding on another person's physical solitude, disclosing private information about another person, or publicly placing someone in false light.
- *Trespass and conversion:* Trespass is the unauthorized physical invasion of property or remaining on property after permission has been rescinded. Conversion means taking personal property in such a way that the plaintiff's use or right of possession of chattel is restricted. In simpler terms, conversion is depriving someone of the use of personal property.
- *Intentional infliction of mental distress:* Intentionally causing mental or emotional distress to another person. The distress may be either mental or physical and may result from highly aggravating words or conduct.

Security and Liability

In the past few years, the number of suits filed against security officers and companies has increased dramatically. Predictions for the next ten years indicate no further increase. One possible reason for the leveling off of suits is that security management has a better understanding of the problems associated with liability situations today. The earlier increase may be partly attributed to the growth of the security industry and to the public's demand for accountability and professionalism in the security area. Most of the cases filed against private security officers and operations belong in the tort category as was mentioned earlier.

In most cases of negligence, the jury considers awarding damages to compensate the plaintiff [the injured party, whether it be a person, a corporation, or an association]. The awards generally take into account the physical, mental, and emotional suffering of the plaintiff, and future medical payments may be allowed for.

Punitive damages are also possible but are more likely to be awarded in cases of intentional liability. Punitive damages are designed to punish the *tortfeasor* [the individual who commits a tort] and to deter future inappropriate behavior. Punitive damages are also possible in negligence cases where the actions of the tortfeasor were in total disregard for the safety of others.

Duty to Protect from Third-Party Crime

The area of civil liability is of great importance to the security industry because the courts have been more willing to hold the industry legally responsible for protection in this area than in others. This trend is particularly noticeable in the hotel and motel industry where owners are liable for failure to adequately protect guests from foreseeable criminal activity. In some circumstances, a landlord or hotel or motel owner might be held accountable for failure to provide adequate protection from criminal actions. In *Klein v. 1500 Massachusetts Avenue Apartment Corporation*,[11] a tenant who was criminally assaulted sued the corporation. The decision centered on the issue that the landlord had prior notice of criminal activity (including burglary and assault) against his tenants and property. In addition, the landlord was aware of conditions that made it likely that criminal activities would continue. The court ruled that the landlord had failed in an obligation to provide adequate security and was thus liable. A similar case was made against Howard Johnson's by the actress, Connie Frances.[12] Frances alleged that the hotel had failed to provide adequate locks on the doors. The jury awarded Frances over $1 million.

[Other] decisions (*Philip Aaron Banks, et al. v. Hyatt Corporation* and *Refco Poydras Hotel Joint Venture* and *Allen B. Morrison, et al. v. MGM Grand Hotel, et al.*) have followed earlier landmark cases.[13] In the *Banks* case, the court held the hotel liable for foreseeable events that led to the murder of Banks by a third party. Banks was shot only four feet from the hotel door. The suit alleged that the hotel failed to provide adequate security and to warn Banks of the danger of criminal activity near the hotel entrance. The jury awarded the plaintiffs $975,000, even though evidence was introduced that showed that the hotel had made reasonable efforts to provide additional protection in the area. The court stated that ''the owner or operator of a business owes a duty to invitees to exercise reasonable care to protect them from injury,'' noting that ''the duty of a business to protect invitees can extend to adjacent property, particularly entrances to the business premises, if the business is aware of a dangerous condition on the adjacent property and fails to warn its invitees or to take some other reasonable preventive action.''

In the Morrison case, a robber followed Morrison from the hotel desk into the elevator after Morrison had cashed in his chips and withdrew his jewelry and cash from the hotel's safe. The robber took Morrison's property at gun point and then knocked him unconscious. Morrison brought suit against the hotel for failing to provide adequate security, noting that a similar robbery had recently occurred. The appellate court supported Morrison's contention saying, ''a landowner must exercise ordinary care and prudence to render the premises reasonably safe for the visit of a person invited on his premises for business purposes.'' In *McCarty v. Pheasant Run, Inc.*,[14] however, the court recognized that invitees who fail to take basic security precautions may not have cause for action against the hotel.

In determining foreseeability, another factor to take into account is the nature and condition of the premises at the time the incident occurred. The following case was reported in *Premises Liability: Legal Considerations for the Industrial and Retail Manager*.

In a case, *Gomez v. Ticor*,[15] involving a murder in a parking garage of a commercial office building the court commented that the very nature of a parking structure to be such that criminal activity was something that could be anticipated:

> [W]e note the unique nature of a parking complex, which invites acts of theft and vandalism. In such structures, numerous tempting targets (car stereos, car contents, the cars themselves) are displayed for the thief; high walls, low ceilings and the absence of cars' owners allow the thief or vandal to work in privacy and give him time to complete his task. Such circumstances increase the likelihood of criminal misconduct. In addition, the deserted, labyrinthine nature of these structures, especially at night, makes them likely

> places for robbers and rapists to lie in wait. Robbery, rape, and violent consequences to anyone who interrupts these crimes, may thus also be foreseeable.

In fact, the concept of foreseeability has been expanded beyond the narrow opinion that foreseeability is implied in failure to provide security for specific criminal behavior. This concept implies that, since certain attacks have occurred in or near the company, the company should reasonably be expected to foresee potential security problems and provide adequate security. In a recent Iowa Supreme Court decision, the court abolished the need for prior violent acts to establish foreseeability. In *Galloway v. Bankers Trust Company and Trustee Midlands Mall*,[16] the court ruled foreseeability could be established by ''all facts and circumstances,'' not just prior violent acts. Therefore prior thefts may be sufficient to establish foreseeability since these offenses could lead to violence. In another case, *Polly Suzanne Paterson v. Kent C. Deeb, Transamerica Insurance Co., W. Fenton Langston, and Hartford Accident & Indemnity Co.*,[17] a Florida court held that the plaintiff may recover for a sexual assault without proof of prior similar incidents of the premises.

According to Thomas,[18]

> Property and business owners should always remember that courts will review their duty of care in a given situation on a case-by-case basis. ''If the place or character of the landowner's business, or his past experience, is such that he should reasonably anticipate careless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it and to use such means of protection as are available to afford reasonable protection'' *Nola M. v. U.S.C.*, 16 Cal. App. 4th 421 (1993).

Nondelegable Duty

Another legal trend is to prevent corporations from divesting themselves of liability by assigning protection services to an independent contractor. Under the principle of agency law, such an assignment transferred the liability for the service from the corporation to the independent contractor. The courts, however, have held that some obligations cannot be entirely transferred. This principle is called *nondelegable duty*. Based on this principle, contractual provisions that shift liability to the subcontractors have not been recognized by the courts. These contractual provisions are commonly called *hold harmless* clauses.

Imputed Negligence

Imputed negligence simply means that, ''by reason of some relation existing between A and B, the negligence of A is to be charged against B, although B has played no part in it, has done nothing whatever to aid or encourage it, or indeed has done all that he possibly can to prevent it. This is commonly called 'imputed contributory negligence.' ''[19]

Vicarious Liability

One form of imputed negligence is *vicarious liability*. The concept of vicarious liability arises from agency law in which one party has the power to control the actions of another party involved in the contract or relationship. The principal is thus responsible for the actions of a servant or agent. In legal terms, this responsibility is called *respondeat superior*. In short, employers are liable for the actions of their employees while they are employed on the firms' business. Employers are liable for the actions of their agents even if the employers do nothing to cause the actions directly. The master is held liable for any intentional tort committed by the servant where the servant's purpose, however misguided, is wholly or partially to further the master's business.

If security officers are acting within the scope of their employment and commit a wrongful act, the employer is liable for the actions. The matter then turns on the scope of the officer's employment and the employer-employee relationship. One court described the scope of employment as depending on

(1) The act as being of the kind the employee is employed to perform
(2) The act occurring substantially within the authorized time and space limits of the employment
(3) The offender being motivated, at least in part, by a purpose to serve the master.[20]

Liability then is a function of the control exercised or permitted in the relationship between the security officer and the hiring company. If the hiring company maintains a totally hands-off posture with respect to personnel supplied by the agency, it may well avoid liability for wrongful acts performed by such personnel. On the other hand, there is some precedent for considering the hiring company as sharing some liability simply by virtue of its underlying rights of control over its own premises, no matter how it wishes to exercise that control. Many hiring companies are, however, motivated to contractually reject any control of security personnel on their premises in order to avoid liability. This, as was pointed out in *The Private Police*, works to discourage hiring companies from regulating the activity of security employees and ''the company that exercises controls, e.g., carefully examines the credentials of the guard, carefully determines the procedures the guard will follow, and pays close attention to all his activities, may still be substantially increasing its risk of liability to any third persons who are in fact, injured by an act of the guard.''[21]

It is further suggested in this excellent study that there may be an expansion of certain nondelegable duty rules into consideration of the responsibilities for the actions of security personnel. As was discussed previously, the concept of the nondelegable duty provides that there are certain duties and responsibilities that are imposed on an individual and for which that individual remains responsible even though an independent contractor is hired to implement them. Such duties currently encompass keeping the workplace safe and the premises reasonably safe for business visitors. It is also possible that the courts may find negligence in cases where the hiring companies, in an effort to avoid liability, have neglected to exercise any control over the selection and training of personnel, and they may further find that such negligence on the part of the hiring company has led to injury to third-party victims.

Criminal Liability

Criminal liability is most frequently used against private security personnel in cases of assault, battery, manslaughter, and murder. Other common charges include burglary, trespass, criminal defamation, false arrest, unlawful use of weapons, disorderly conduct, extortion, eavesdropping, theft, perjury, and kidnapping. Security officers charged with criminal liability have several options in defending their actions. First, they might try to show that they were entitled to use force in self-defense or that they made a reasonable mistake, which would negate criminal intent. Other defenses include entrapment, intoxication, insanity, consent (the parties involved concurred with the actions), and compulsion (the officer was forced or compelled to commit the act). As has been already noted in previous discussions, a corporation or an association could be charged with criminal liability as well as an individual officer.

The reporting of crime is an area in which security officers are liable for criminal prosecution. In general, private citizens are no longer obliged to report crime or to prevent it. But some jurisdictions still recognize the concept of misprision of felony—that is, concealing knowledge of a felony. Such legislation makes it a crime to not report a felony. To be guilty of misprision of felony, the prosecution must prove beyond a reasonable doubt that (1) the principal committed and completed the alleged felony, (2) the defendant had full knowledge of that fact, (3) the defendant failed to notify the authorities, and (4) the defendant took affirmative steps to conceal the crime of the principal.

Security officers may also be liable for failure to perform jobs they have been contracted or employed to perform. If guards fail to act in a situation in which they have the ability and obligation to act, the courts suggest that they could be criminally liable for failure to perform their duties, assuming a criminal act is committed. At the minimum the guard is subject to tort liability.

Another issue in security work involves undercover operations. Many times security operatives are accused of soliciting an illegal act. Where security officers clearly intended for crimes to be committed, they may be charged with solicitation of an illegal act or conspiracy in an illegal act. This is in contrast to the public sector, where most police officers are protected by statute from crimes they commit in the performance of their duty. Thus only the private citizen may be charged with such an offense, and the only issue that can be contested is the defendant's intent.

Entrapment, which is solicitation by police officers, is another charge that may be leveled against security officers. While entrapment does not generally apply to private citizens (the case of *State v. Farns*[22] is frequently cited to prove that entrapment does not apply to private citizens), several states have passed legislation that extends entrapment statutes to cover private persons as well as police officers. Until the issue is resolved in the courts in the next few years, security officers involved in undercover operations should be careful to avoid actions that might lead to entrapment charges.

Security and the Law References

1. Michigan Revised Statutes, Section 338.1051-338.1083.
2. Robert D. Pursley, *Introduction to Criminal Justice*, 5th ed. (Macmillan, New York, 1991), p. 35.
3. *U.S. v. Hillsman*, 522 F.2d 454, 461 (7 Cir. 1975).
4. *Escobedo v. State of Illinois*, (378 U.S. 478, 32 Ohio Op 92d) 31, 84 S.Ct. 1758 12 L.Ed(2d)977 (1964).
5. *Miranda v. Arizona*, 384 U.S., 486 86 S.CT 1602, 16L.Ed.2d.691.
6. *People vs. Zelinski*, 594 P 2d 1000 (1979).

7. *Burdeau v. McDowell*, 256 U.S. 465 (1921).
8. Charles Schnabolk, *Physical Security: Practices and Technology* (Butterworth Publishers, Stoneham, MA, 1983), p. 74.
9. Restatement of Torts, Second Edition 307.
10. *Fisher v. Carrousel Motor Hotel, Inc*., 424 SW2d 627 (Texas 1976).
11. *Klein v. 1500 Massachusetts Avenue Apartment Corporation*, 439 F 2d 477 DC Cir (1970).
12. *Garzilli v. Howard Johnson's Motor Lodge, Inc*., 419 F Supp. 1210 U.S. DCT EDNY (1976).
13. *Philip Aaron Banks, et al. v. Hyatt Corporation and Refco Poydras Hotel Joint Venture*, 722 F.2d 214 (1984); and *Allen B. Morrison, et al. v. MGM Grand Hotel, et al*., 570 F. Supp. 1449 (1983).
14. *McCarty v. Pheasant Run, Inc*., F.2d 1554 (1987).
15. *Gomez v. Ticor*, 145 Cal. App. 3d 622, 193 Cal. Rptr. 600, 1983 (as reported in ''Premises Liability: Legal Considerations for the Industrial and Retail Manager,'' p. 6, Mary Ann Alsnauer, Laura D. Wolpow, Howarth and Smith, Los Angeles, California).
16. *Galloway v. Bankers Trust Company and Trustee Midlands Mall*, No. 63/86-1879 Iowa Supreme Court.
17. *Polly Suzanne Paterson v. Kent C. Deeb, Transamerica Insurance Co., W. Fenton Langston, and Hartford Accident & Indemnity Co*., 472 S. 2d 1210.
18. Thomas, Michael, Paul, ''Duty to protect against attacks is narrow but real'' (*California Real Estate Journal*, Los Angeles, CA, April 22, 2002, p. 12), with reference to *Nola M. v. U.S.C*., 16 Cal. App. 4th 421 (1993).
19. William L. Prosser, *Handbook of the Law of Torts*, 4th ed., Hornbook Series (St. Paul, Minn.: West, 1970), p. 458.
20. *Fornier v. Churchill Downs-Latonia*, 292 Ky. 215, 166 SW 2d 38 (1942).
21. James S. Kakalik and Sorrel Wildhurn, *The Private Police* (New York: Crane, Russak & Co., 1977).
22. *State vs. Farns*, 542 P.2d 725 Kan. (1975).

Additional Reading

Kaminsky, Alan, *A Complete Guide to Premises Security Litigation*, 2nd ed. (American Bar Association, Tort and Insurance Practice Section, 750 North Lake Shore Drive, Chicago, IL, 2001).

13 *Liaison with Law Enforcement and Fire Authorities*

For a high-rise office building to have a successful security and fire life safety program, it is essential for the building owner or manager, the Director of Security, or the Fire Safety Director, to liaise with various agencies in the public sector, including law enforcement and fire authorities. Developing and maintaining strong lines of communication and cooperation with these authorities will lead to a successful working relationship.

Liaison with Law Enforcement

Law enforcement authorities are concerned primarily with crime prevention and control. This involves the protection of the lives, property, and general welfare of the public community. Police, funded by public monies, achieve this protection largely through the enforcement of laws. High-rise buildings interact with public law authorities such as police and sheriff's departments and state or federal agencies.

Police and Sheriff's Departments

The *police department* is the primary law enforcement agency in a city. The *sheriff's department* serves a similar function outside city limits or if no municipal police department exists. Both departments are the points of origin for reporting all crimes. Although other agencies may have final jurisdiction over many classes of crime, initial authority almost always rests with the local police department.

Police and sheriff's departments handle tasks such as taking reports and investigating crimes; maintaining arrest, missing persons, and identification records; keeping records of lost and stolen property; taking reports of vehicle accidents (but not those that occur on state roads); issuing gun permits; and transporting and maintaining custody of prisoners. Local police also may provide traffic control support for special events. A local marshal or constable may serve criminal and bench warrants and handle service of process.

State Law Enforcement Agencies

State agencies—the State Police, the State Patrol, the Department of Justice, the Department of Public Safety, and so on—have authority that varies from state to state but may include enforcement of traffic laws, conducting investigations, gathering intelligence, and providing protection of public figures.

Federal Law Enforcement Agencies

Federal agencies have jurisdiction over areas as defined by their charters. The Department of Justice (DOJ) includes the following organizations:

Federal Bureau of Investigation (FBI). The FBI has jurisdiction over federal crimes and offenses such as bank robbery, kidnapping, white collar crime, public corruption, and terrorism. It has concurrent jurisdiction with the Drug Enforcement Administration in drug enforcement.

Drug Enforcement Administration (DEA). The DEA has jurisdiction over federal narcotics offenses and provides special training and laboratory services to law enforcement.

U.S. Marshal's Office. The U.S. Marshal's Office handles federal service of process.

Immigration and Naturalization Service (INS). The INS handles immigration-related matters.

The DOJ, along with the Architectural Transportation Compliance Board (ATCB), the Equal Employment Opportunity Commission (EEOC), and the Federal Communications Commission (FCC), has responsibility for exacting compliance with various parts of the Americans with Disabilities Act (ADA).

The Treasury Department includes the Secret Service, which provides protection for the President and public figures and has jurisdiction over counterfeiting and credit card and wire frauds; the Bureau of Alcohol, Tobacco and Firearms (ATF) enforces laws pertaining to alcohol, tobacco, firearms, and explosives and conducts investigations; the Customs Service enforces customs laws and regulations, including anti-smuggling; and the Internal Revenue Service (IRS) handles tax collection. The Department of Labor includes the Occupational Safety and Health Administration (OSHA), which regulate safety in the workplace. The Department of Defense includes the Defense Investigative Service, which regulates the protection of government contractors' classified information. The Federal Emergency Management Agency (FEMA) provides disaster relief and manages the civilian response to national security crises.*

In addition, the U.S. Office of Homeland (OHS) Security, established on October 8, 2001, by executive order of the President of the United States, is mandated ''to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.''

---

*Information obtained from *Liaison: Who's What in Law Enforcement and Regulatory Agencies* (Polek and Crowl, 1994) was helpful in understanding law enforcement agencies.

Liaison with Fire Authorities

Fire authorities are primarily concerned with the preservation of people's lives and properties, including the enforcement of local and state fire codes. Municipal, county, and state fire personnel who enforce fire codes and conduct arson investigations may have police officer status to assist them in carrying out their duties.

Building fire life safety systems and fire prevention inspections, as well as fire investigations, commonly are conducted in conjunction with the local fire department inspector or the fire marshal who has jurisdiction over the building. Frequently, state or federal agencies, such as OSHA, conduct inspections and investigations related to occupant safety.

Fostering Relationships with Law Enforcement and Fire Authorities

The building security representative can foster relationships with law enforcement by formal and informal communication. There is a strong underlying reason such a relationship is of mutual benefit to both law enforcement and the private security representative: the common objective of crime prevention. During criminal investigations conducted within a high-rise building, for example, a successful working relationship with law enforcement can greatly improve the outcome. Such investigations commonly are conducted in conjunction with the local police or sheriff's department or federal agency, whose support and assistance must be obtained to bring the effort to a satisfactory conclusion. It is important to remember that the authority of a private investigator is comparable only to that of a private citizen in areas such as detaining suspects and obtaining access to information. (See ''Private Sector and Public Law Enforcement Investigations'' in Chapter 9 for details on this subject.)

The building safety representative can also foster relationships with fire authorities. These agencies are only too anxious to assist buildings in establishing and maintaining sound fire life safety programs for building users. Fire departments in large cities—such as New York, Chicago, and Los Angeles—have even established specialized high-rise divisions and units to help in this endeavor.

The following sections describe ways to initiate positive interaction with local law enforcement and the fire authority having jurisdiction; these mostly have to do with mutual respect and planned coordination of efforts.

Communication

It is vital to establish a clear line of communication with law enforcement and the fire department and, wherever possible, involve them in implementing the building's security and fire life safety program. Most city police agencies and some sheriff's departments have a community affairs manager or a contact officer. It is important for the building representative to become familiar with that individual and learn of offered services and also ways to help support these agencies. Likewise, with the fire department, establish contact and learn ways for mutual cooperation. ''Some jurisdictions around the country have local associations or formal alliances comprised of police [fire] [building managers] and security professionals for the express purpose of addressing their mutual problems [and concerns]. If there isn't one in your area start one'' (Vail, 2002, p. 50).

Any public service education programs appropriate to the building offered by these agencies should be supported by the building.

Reporting Crimes

Whenever possible, provide law enforcement with statistics of criminal acts, particularly crimes of larceny, that have occurred at the building. Encourage tenants to report crimes to law enforcement. Public reports such as Uniform Crime Reports and the National Incident-Based Reporting Systems are based on data generated at the local level. By reporting crimes to law enforcement, such data will more accurately indicate what types of crimes are being committed in the community. This will provide a clearer picture of crime and may assist law enforcement in justifying requests for additional law enforcement personnel.

Complying with Laws, Regulations, and Codes

Always comply willingly with state and local laws, particularly as they pertain to maintaining a safe workplace for building occupants. Maintain up-to-date self-inspections and maintenance of building fire life safety systems and equipment. Keep fire protection test records and log sheets current—including emergency generator tests, tests of fire detection and suppression systems, portable fire extinguisher checks, and equipment service invoices. Maintain documentation according to the guidelines of the authority having jurisdiction.

When state or local fire officials conduct inspections, escort the inspector on the tour of the building. The inspector will offer acceptable ways to correct deficiencies and will give advice that will be invaluable in preparing for the next inspection. Prompt correction of violations within established time frames, and to the satisfaction of the inspector, will assist in developing a good relationship.

Enlisting Public Agency Support

Consult the appropriate authority when problems exist that the building cannot satisfactorily handle. For example, if a tenant fails to respond to the building Fire Safety Director's repeated requests to correct improper storage of material that constitutes a fire hazard, solicit the support of the local fire authority. The local fire inspector may decide to carry out an ''unannounced'' fire prevention inspection with particular emphasis on that tenant. The inspector thus takes building management out of what can be a sensitive and potentially confrontational situation.

Also, consult with law enforcement regarding any serious theft problem within a building. When appropriate, involve law enforcement in security investigations.

Hospitality

Invite law enforcement agencies for a tour of the building to view the security program, and acquaint them with the security operation. This will give them a better understanding of the building and its security objectives. Offer law enforcement the use of the building for periodic training operations, such as hostage simulations.

Invite members of the fire department to tour the building and view the fire life safety program. Also, encourage them to conduct familiarization drills of the building.

If fire and law enforcement officials invite building representatives to tour their operations, such offers should always be graciously accepted.

Taking local law enforcement and fire representatives to lunch, at least annually, is also strongly encouraged.

Disaster Exercises

Conduct a full-scale building disaster exercise in conjunction with local emergency response groups—the local fire department's fire suppression crews and emergency medical responders, local hospitals and health services, local law enforcement, the American Red Cross, and other emergency organizations within the community. If thoroughly prepared and properly executed, such exercises can be of great educational value to building staff, tenants, and all outside agencies and groups who participate, and it can greatly assist in developing working relationships with local fire and law enforcement agencies.

Public Agency Presentations

Invite law enforcement and fire department representatives to give presentations to building tenants. For example, representatives of police bomb squads and the ATF can provide very informative, interesting, and helpful information regarding bombs and bomb threats; the FBI can do the same regarding white-collar crime and terrorism. Fire departments, particularly in larger cities where generally more staff are available, are willing to do special presentations on fire life safety. Some will even provide tabletop and live demonstrations and hands-on portable fire extinguisher training for building occupants. Fire department representatives always should be invited to attend building fire drills and evacuation exercises.

Presentations by law enforcement and fire departments can benefit not only the building concerned but can also assist these public agencies in their efforts to control crime and promote public safety.

Professional Security and Fire Life Safety Organizations

Support private organizations such as ASIS International and the National Fire Protection Association (NFPA).

ASIS has local chapters, and some law enforcement representatives attend these monthly meetings. Also, its Law Enforcement Liaison Council provides guidelines and recommendations as to how private security can interact with law enforcement agencies. Annual events like ''Law Enforcement Appreciation Day,'' when local members of law enforcement are invited by members of ASIS to a special luncheon, is an opportunity to express gratitude to members of law enforcement.

NFPA, among its myriad of activities, sponsors public fire safety education and awareness events such as the annual National Fire Prevention Week. In 1920, October 9—a significant date because the Great Chicago Fire occurred on that day in 1871—was declared National Fire Prevention Day by President Woodrow Wilson. In 1922, the observance was extended to one week by the NFPA when it assumed sponsorship of the event. In 1925, the entire week containing October 9 was officially proclaimed Fire Prevention Week by President Calvin Coolidge (''Fire tech update,'' 1994, p. 127).

In addition there are various other groups that help facilitate communication between the private and public sectors. These include the International Association of Chiefs of Police (IACP), the National Sheriff's Association (NSA), and the Joint Council of Law Enforcement and Private Security Association (comprising representatives of IACP, NSA, and ASIS International).

Community Service

It is a good practice to sponsor community service programs that are offered through local law enforcement or fire department agencies. Sponsoring youth sports teams and assisting in volunteer fund-raisers can help considerably in a building's efforts to work effectively with local law enforcement and fire authorities.

Summary

In addressing security, high-rise buildings focus on loss prevention, whereas public law enforcement agencies are primarily concerned with crime control and public safety.

Building management is concerned with the life safety of all its building users. Fire authorities are concerned with the preservation of people's lives and properties, and with the enforcement of local and state fire codes.

Representatives of a high-rise office building can find many opportunities to cooperate with public agencies. The result of these efforts will be an enhanced building security and fire life safety program and a safer community at large.

References

''Fire tech update'' (*Security Sales*, Vol. 16, No. 10, Bobit Publishing Company, Redondo Beach, CA, October 1994).

Polek, Victor, and Larry Crowl, *Liaison: Who's What in Law Enforcement and Regulatory Agencies* (presentation for CPP Review Class, ASIS Los Angeles Chapter, October 15, 1994).

Vail, Chris, ''Successful partnering of police and private forces'' (*Security Technology & Design*, Cumming, GA, March 2002).

This Page Intentionally Left Blank

14 *Apartment and Residential Buildings, Hotels and Motels, and Hospitals and Health-Care Facilities*

As outlined in the opening chapter of this book, with reference to high-rise buildings, ''in terms of reported fires, there are actually four property classes that dominate the statistics. Office buildings and hotels and motels are among them, but so are apartment buildings and hospitals (and other facilities that care for the sick)'' (Hall, 2001, p. 3). Primarily, this book addressed office buildings; but these other high-rise occupancies are also very important. This chapter touches upon the fire life safety of these occupancies, but is by no means an in-depth treatise.

Apartment and Residential Buildings

''Apartment buildings are identified as those structures containing three or more living units with independent cooking and bathroom facilities, whether designated as apartment houses, tenements, condominiums, or garden apartments. Apartments differ from multi-unit residential occupancies that are not considered homes, such as hotels and boarding homes, by the provision of individual cooking facilities, the number of sleeping rooms, and the less transient nature of the occupants'' (Bush, 1997, p. 9-67).

All new high-rise apartment buildings are required by code to have automatic fire detection and suppression systems and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes and automatic smoke control systems to restrict the spread of smoke. Existing high-rise apartment buildings are required to have automatic detection and manual alarm systems, and most* are required to be protected by an approved, supervised, automatic sprinkler

*For example, the city of Chicago does not require sprinkler systems in residential high-rises built before 1975 (Bush and Ferkenhoff, 2002, p. 6).

system. However, fire remains an ever-present danger in these facilities. National statistics based on surveys by the National Fire Incident Reporting System (NFIRS) and NFPA Fire Analysis & Research indicate for the period 1985–1998 that ''most high-rise building fires and associated losses occur in apartment buildings. This may seem surprising, but it shouldn't. Homes dominate the U.S. fire problem'' (Hall, 2001, p. 4).

''The occupancy hazards of apartment buildings include all risk factors that may arise in particular segments of the population. Preschoolers and older adults, if present, have a higher risk of dying in fires because of the mental or physical limitations associated with their age. Older children and younger adults may be at risk if they are physically or mentally handicapped, or as a result of drug or alcohol abuse. And fatal fires are more common at night, when people are asleep'' (Bush, 1997, p. 9-67).

It is vital that occupants in a residential occupancy know how to react when a fire emergency occurs. This is particularly important because usually after normal business hours these facilities do not have many building emergency staff present to assist residents to evacuate. ''Occupants of each living unit must be given emergency instructions on a yearly basis, indicating the location of alarms, exiting paths, and actions to be taken in response to a fire in the living unit and in response to the sounding of an alarm'' (Bush, 1997, p. 9-71).

Hotels and Motels

Hotels and motels differ from apartment and residential buildings in that occupants are primarily temporary guests. According to Bell (1997, p. 9-64),

> Hotels are buildings or groups of buildings under the same management having more than sixteen sleeping accommodations primarily used by transients who are lodged, with or without meals, for a period of less than 30 days. These facilities may be designated as hotels, inns, clubs, motels, guest quarters, suite hotels, or by other names. So-called apartment hotels also are classified as hotels, because they are subject to transient occupancies like those of hotels. . . . These facilities are unique in that they almost always combine several different occupancies under one roof. In addition to guest rooms or guest suites, which are residential occupancies, hotels usually provide space for assembly occupancies such as ballrooms, meeting rooms, exhibition halls, and restaurants; or mercantile occupancies such as shopping areas, gift shops, and other retail areas; and offices and commercial establishments, or business occupancies.
>
> Since hotel guests are transients, special consideration must be given to the potential threat to their life safety from fire. For example, occupants of the residential portion of a hotel sleep in unfamiliar surroundings and could possibly become disoriented when trying to evacuate under heavy smoke conditions. Likewise, persons in ballrooms, lounges, [casinos,] and restaurants could become disoriented due to low-level lighting, crowd size, and unfamiliarity with evacuation routes.

Serious Hotel and Motel Fires

Since 1980, the following serious high-rise hotel fires* have occurred in the United States and Puerto Rico.

MGM Grand Hotel

November 21, 1980, Las Vegas, Nevada—The MGM Grand Hotel fire resulted in the death of 85 persons,† injury to about 600, and over $30 million in property damage. The fire started at approximately 7:10 AM in a restaurant in the Main Casino and resulted in considerable smoke spread throughout the 23-story hotel building. There were approximately 3400 registered hotel guests. Of the 79 body locations identified, 61 were in the high-rise tower and 18 were on the Casino level. The most probable cause of the fire was heat caused by an electrical fault in the restaurant.

According to the NFPA's analysis of the fire, the major contributing factors in this fire and significant additional findings included the following:

- Rapid fire and smoke development on the Casino level due to available fuels, building arrangement, and the lack of fire-resistant barriers
- Lack of fire sprinklers and fire-resistant barriers in the incipient stage of the fire
- Unprotected vertical openings contributing to vertical smoke spread to the high-rise tower
- Distribution of smoke throughout the high-rise tower through HVAC equipment
- Smoke spread through elevator hoistways to the high-rise tower
- There was no evidence of a fire emergency plan being carried out, and there was some delay in notifying hotel occupants and the fire department
- The number of exits and capacity of exits from the Casino at the time of the fire were deficient
- There was no evidence of manual fire alarm pull stations located in the natural path of escape on the Casino level
- There was no automatic way to return elevators to the main floor in the event of fire
- An estimated 300 persons were evacuated from the roof of the high-rise tower by helicopter

Favorable factors in the MGM helicopter evacuation operation included clear weather, daylight hours, and the unusual availability of participating Air Force helicopters (NFPA *Investigation Report*, January 1982, p. 31).

---

*Details of the MGM Grand Hotel, the Dupont Plaza Hotel and Casino, and the Las Vegas Hilton Hotel fires were obtained from NFPA investigation reports (David Demers was the principal investigator for the Las Vegas Hilton fire, and Richard Best and David Demers conducted the investigation of the MGM Grand fire) contained in ''Special Data Information Package High-Rise Fires-Hotel and Motel Buildings'' (National Fire Protection Association, One-Stop Data Shop, Quincy, MA, August 1999).

†''The death toll of 85 people made this the second most deadly fire in U.S. history (119 people died in the Winecoff Hotel in Atlanta, Georgia, in 1946)'' (Klaene and Sanders, 2000, p. 386).

Dupont Plaza Hotel and Casino

> *December 31, 1980, San Juan, Puerto Rico*—The Dupont Plaza Hotel and Casino fire resulted in the death of 86 persons and over 140 being injured. The fire, discovered at approximately 3:22 PM, resulted in smoke that spread to the 17-story hotel portion. Many of those trapped on upper floors were able to obtain fresh air on balconies. Three people died in elevators and one in a 4th-floor guest room. The majority of fatalities occurred when fleeing guests were trapped inside the casino. The fire burned for almost five hours before fire authorities extinguished it. The ATF and local authorities determined that the fire was deliberately lit among guest room furniture temporarily stored in the ballroom.

According to the NFPA's analysis of the fire, ''the major contributing factors to the loss of life in the Dupont Plaza Hotel and Casino [were]:

- Lack of automatic sprinklers in the South Ballroom (room of fire origin)
- Rapid fire growth and spread
- There were no automatic fire detection systems present in the Dupont Plaza Hotel complex to alert occupants of the fire in its incipient stage
- The vertical opening between the ballroom and casino level[s] created by the ballroom foyer allowed smoke and fire to move to the casino level and then into the casino itself. As a result, smoke and fire spread to the hotel lobby, effectively blocking the exit paths for the casino guests and high-rise occupants
- Smoke movement to the high-rise tower by way of vertical penetrations'' (NFPA *Interim Investigation Report*, pp. 10, 11)

Las Vegas Hilton Hotel

> *February 10, 1981, Las Vegas, Nevada*—The Las Vegas Hilton Hotel fire resulted in the death of eight persons and 350 being injured. The main fire that started at 8:05 PM on the 8th floor spread vertically up the exterior of the building, floor by floor, until it reached the top floor. Smoke also spread through the 30-story hotel. Four victims were found in guest rooms whose doors were open or had been opened. No guests died who kept the door to their room closed until they were rescued or the fire stopped.

According to excerpts from the NFPA's analysis of the fire, ''the most significant factors that contributed to the fire spread and subsequent fatalities, injuries and damage at the Las Vegas Hilton were:

- Failure to extinguish the fire in its incipient stage
- The presence of highly combustible carpeting on the walls and ceilings of the involved elevator lobbies, which contributed to the exterior fire spread. The resulting fire spread exposed a large number of the building's occupants on multiple floors to the blaze.

The person who initially called in the fire alarm to the security dispatcher was arrested, charged, and indicted on eight counts of homicide and arson. He was a hotel room-service busboy who had been employed by the Hilton for only a few weeks'' (NFPA *Investigation Report*, January 1982, pp. 53, 62).

The above hotel fires have in common that there were no automatic sprinklers in the area of fire origin. As has been stated earlier in this book, sprinkler systems have proven to be a most effective means of controlling fires. There is a substantial reduction of the chances of death or extensive property damage in a fully sprinklered building. According to Hall and Cote (1997, pp. 1-19, 1-20),

> The 1980 MGM Grand Hotel fire, in Las Vegas, NV, inspired an industry response that combined unprecedented widespread code compliance with fire safety provisions that often ran ahead of code requirements. The result has been a dramatic change both in the fire death toll in hotels and motels and in the use of proven fire protection in that industry. . . .
>
> In 1980, the year of the MGM Grand Hotel fire, sprinklers were reported present in only one of nine hotel or motel fires reported to U.S. fire departments. Detectors were reported present in just over one-fourth of reported hotel or motel fires.
>
> By 1993, sprinklers were reported present in one-third of hotel and motel fires and in three-fourths of high-rise hotel fires. An industry-sponsored study of sprinkler usage in 1988 found sprinklers present in roughly half of all properties, suggesting the percentage today is much higher still. By 1993, detectors were reported present in three-fourths of all hotel or motel fires. And for both detectors and sprinklers, it is reasonable to assume that the new level of built-in fire protection had much to do with the dramatic drop in the number of hotel and motel fires since 1980.

Of course, in addition to automatic fire detection and suppression systems and other fire protection features—automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes and automatic smoke control systems to restrict the spread of smoke—it is essential that each hotel and motel has an effective emergency organization in a constant state of readiness to react to an emergency, particularly one that involves fire, in a way that will help assure the safety of hotel guests. When a fire occurs it is essential that emergency staff, in conjunction with responding fire fighters, assist occupants to evacuate and conduct a thorough search of every hotel guest room. In searching hotel rooms it needs to be kept in mind that guests may be asleep at any time of day. They also may be in a deep sleep due to the use of alcohol, sleeping pills, or other substance.

Hospitals and Health-Care Facilities

''Health care facilities are used for the treatment or care of persons suffering from physical or mental illness, disease, or infirmity, and for the care of infants, convalescents, or aged persons. These facilities provide sleeping accommodations for occupants who may be incapable of self-preservation because of physical or mental disability or age. Some buildings that house health-care occupants have security measures that limit freedom of movement. . . . A significant percentage of occupants in hospitals and nursing homes are incapable of self-evacuation or are ambulatory but incapable of perceiving a fire threat and choosing a rational response'' (Jaeger, 1997, p. 9-49).

Threat of Fire

As with all high-rise occupancies, one of the greatest threats to the life safety of health-care occupants is fire. Because some patients are not capable of evacuation or would be very slow to evacuate, health-care facilities utilize a ''defend in place'' strategy that means ''it is better to keep the fire from the patient than to remove the patient from the fire. . . . As a result, health care facility design and operation must incorporate methods by which a fire can be detected early, contained, and fought rapidly and successfully. Accomplishing this requires careful planning of the health care facility and its day-to-day operation. . . . Total building fire protection for life safety is more necessary in health care facilities than in other occupancies because of the nature of the occupants'' (Jaeger, 1997, pp. 9-49, 9-50).

As stated in NFPA 101, *Life Safety Code*,

> All health care facilities shall be designed, constructed, maintained, and operated to minimize the possibility of a fire emergency requiring the evacuation of occupants. Because the safety of health care occupants cannot be ensured adequately by dependence on evacuation of the building, their protection from fire shall be provided by appropriate arrangement of facilities, adequate, trained staff, and development of operating and maintenance procedures composed of the following:
>
> (1) Design, construction, and compartmentation
> (2) Provision for detection, alarm, and extinguishment
> (3) Fire prevention and the planning, training, and drilling programs for the isolation of fire, transfer of occupants to areas of refuge, or evacuation of the building (Section 18.1.1.3)

''Since hospitals are required to comply with NFPA 101, *Life Safety Code*, to receive reimbursement Medicare and Medicaid, other provisions of NFPA 101 are undoubtedly also in nearly universal use. This helps explain why, in the latest available statistics, hospitals averaged fewer than seven civilian fire deaths per year between 1989 and 1993'' (Hall and Cote, 1997, p. 1-19).

Other High-Rise Occupancies

In closing, it is noteworthy that in addition to office buildings, apartment and residential buildings, hotels and motels, and hospitals and health-care facilities, there are other high-rise occupancies. These include detention and correctional facilities, lodging or rooming houses, board and care facilities, library and museum collections, and educational institutions. The fire life safety needs of each of these individual occupancies are determined by ''identifying specific *assets*, the *threats* against those assets, and the *risk* of those threats materializing. Also of vital importance, if selected solutions are going to be effective, is an understanding of the possible constraints (for example, culture, operations, economic factors, and codes and standards)'' (Aggleton, 2001).

Summary

In addition to office buildings there are other types of high-rise occupancies. These include apartment and residential buildings, hotels and motels, hospitals and health-care facilities, detention and correctional facilities, lodging or rooming houses, board and care facilities, library and museum collections, and educational institutions. The fire life safety needs for each of these occupancies will vary according to the assets being protected; the threats to those assets; the risks of those threats occurring; cultural, operational, and economic factors; and the laws, codes, and standards that govern that specific occupancy.

References

Aggleton, David G., comments in ''Review of Proposal for Revisions to *High-Rise Security and Fire Life Safety*'' (November 2001).

Bell, James R., ''Hotels,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Best, Richard, and David Demers, NFPA *Investigation Report*s of the Dupont Plaza Hotel and Casino, the MGM Grand Hotel, and the Las Vegas Hilton Hotel fires, ''Special Data Information Package High-Rise Fires–Hotel and Motel Buildings'' (National Fire Protection Association, One-Stop Data Shop, Quincy, MA, August 1999). (David Demers was the principal investigator for the Las Vegas Hilton fire, and Richard Best and David Demers conducted the investigation of the MGM Grand fire.)

Bush, Kenneth, ''Apartment buildings,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Bush, Rudolph, and Eric Ferkenhoff, ''1 killed, 11 injured in Gold Coast fire'' (*Chicago Tribune*, Chicago, January 22, 2002, p. 6).

Hall, John R. Jr., ''High-rise building fires'' (National Fire Protection Association, Quincy, MA, September 2001).

Hall, John R. Jr., and Arthur E. Cote, ''America's fire problem and fire protection'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Jaeger, Thomas W., ''Health care occupancies,'' *Fire Protection Handbook*, 18th ed. (National Fire Protection Association, Quincy, MA, 1997).

Klaene, Bernard J., ''Ben,'' and Russell E. Sanders, *Structural Fire Fighting* (National Fire Protection Association, Quincy, MA, 2000).

NFPA 101, ''New health care occupancies,'' *Life Safety Code*, Section 18.1.1.3 (National Fire Protection Association, Quincy, MA, 2000).

Additional Reading

Beaudry, Mark H., *Contemporary Lodging Security* (Butterworth–Heinemann, Newton, MA, 1996).

Colling, Russell L., *Hospital and Healthcare Security*, 4th ed. (Butterworth–Heinemann, Woburn, MA, 2001).

Colling, Russell L., *Security Keeping the Health Care Environment Safe* (Joint Commission on Accreditation of Healthcare Organizations, Oakbrook Terrace, IL, 1996).

Fire Protection Handbook (National Fire Protection Association, Quincy, MA) contains chapters that individually address detention and correctional facilities, health-care occupancies, board and care facilities, hotels, apartment buildings, lodging or rooming houses, library and museum collections, and educational occupancies.

Index

(n after a page number indicates a footnote)