PART

I

Introduction to Security and Loss Prevention

1

The History of Security and Loss Prevention: A Critical Perspective

Objectives

After studying this chapter, the reader will be able to:

1. Explain the purpose of critical thinking and how to think critically.
2. Define security and loss prevention.
3. List the benefits of studying the history of security and loss prevention.
4. Trace the early development of security and policing.
5. Describe the growth of security companies in the United States.
6. Explain the convergence of IT and physical security and the convergence of enterprise security.
7. Describe 21st century/post-9/11 security challenges.

KEY TERMS

- critical thinking
- security
- loss prevention
- Chief Security Officer (CSO)
- Great Wall of China
- Hammurabi, King of Babylon
- polis
- Praetorian Guard
- vigiles
- feudalism
- comitatus
- posse comitatus
- Posse Comitatus Act
- frankpledge system
- tithing
- Magna Carta
- Statute of Westminster
- watch and ward
- Henry Fielding
- Bow Street Runners
- Sir Robert Peel
- Metropolitan Police Act
- Allan Pinkerton
- Henry Wells
- William Fargo
- William Burns
- Washington Perry Brink
- Edwin Holmes
- George Wackenhut
- first wave societies
- second wave societies
- third wave societies
- convergence of IT and physical security
- convergence of enterprise security

Why Critical Thinking?

September 11, 2001, marked a turning point in the history of security. In a devastating terrorist onslaught, knife-wielding hijackers crashed two airliners into the World Trade Center in New York City, creating an inferno that caused the 110-story twin skyscrapers to collapse. About 3,000 people were killed, including responding firefighters and police. During the same morning, another hijacked airliner crashed into the Pentagon, causing additional deaths and destruction. A fourth hijacked airliner failed to reach its target and crashed when heroic passengers learned of the other attacks and struggled with hijackers to control the airliner. The attacks were immensely successful and cost-effective for the terrorists. With a loss of 19 terrorists and expenses between $400,000 and $500,000, the attackers were able to kill thousands, cause hundreds of billions of dollars in economic damage and spending on counterterrorism, and significantly affect global history. With such a huge kill ratio and investment payoff for the terrorists, governments and the private sector must succeed in controlling terrorism.

Because of these devastating attacks, not only have homeland defenses, military strategies, public safety, and private sector security changed, but also our way of thinking has changed. We cannot afford to have failures in our planning and imagination of what criminals can do. To improve security, we must seek new tools to assist us in our thinking processes.

Here we begin with critical thinking skills to counter “business as usual.” **Critical thinking** helps us to become active learners: to not only absorb information, but to probe and shape knowledge. The critical thinker cuts through “hype” and emotion and goes beyond collecting “facts” and memorizing information in an effort to understand causes, motives, and changes. Critical thinking skills provide a foundation for creative planning while helping us to anticipate future events.

The critical thinker asks many questions, and the questions are often easier to formulate than the answers. Critical thinking requires us to “jump out of our own skin” to see the world from the perspective of others. Although this is not an easy process, we are much better informed before we make our conclusions and decisions.

Critical thinking is not to be used as a tool to open up the floodgates of criticism in the workplace. It is to be applied discreetly to understand the world and to meet challenges.

A professional’s success depends on his or her thinking process applied to everyday duties and long-range planning. Critical thinking adds an extra edge to the repertoire of tools available to security and loss prevention practitioners.

Safi and Burrell (2007: 54) write:

> *Theorists have hypothesized that critical thinking is correlated with internal motivation to think. Cognitive skills of analysis, interpretation, explanation, evaluation and correcting one’s ownreasoning are at the heart of critical thinking.*
>
> *Critical thinking can be learned with practice and guidance by changing the actions involved in making decisions so that they become part of permanent behavior in homeland security intelligence analysis, threat protection and security planning.*

Security challenges have become increasingly complex because as we plan for protection and face a multitude of threats in a rapidly changing environment, we must expect the unexpected, while staying within our budgets. The security practitioner should be creative, have an excellent imagination, apply critical thinking skills, and carefully prioritize security strategies to produce the best possible security program.

Although critical thinking skills are applied to a critical perspective of history in this chapter, students and practitioners are urged to continue this thinking process throughout this book. It is hoped that your conclusions and decisions will be enhanced to improve security and loss prevention.

To prime the reader's mind for the explanation of critical thinking, Chapter 3 applies critical thinking to security planning by suggesting that all security strategies be placed under one of the following three models: it protects people and assets; it accomplishes nothing; or it helps offenders.

How Can We Think Critically?

Our world is filled with many efforts to influence our thinking. Examples are the media, advertisers, politicians, educators, and writers. This author is biased just like other writers, and within these pages is a North American interpretation of security. Although an effort has been made to write an objective book here, it is impossible for any writer, and biases surface. Objectivity is fostered in this book through an introduction to critical thinking skills, a multidisciplinary approach, international perspectives, boxed topics and questions, a variety of references, Web exercises, and case problems at the end of chapters that bridge theory to practice and ask the reader to make decisions as a practitioner.

With so much competition seeking to influence us, choices become difficult and confusing. And, as we think through complex challenges, we need a method of sorting conflicting claims, differentiating between fact and opinion, weighing "evidence" or "proof," being perceptive to our biases and those of others, and drawing logical conclusions. Ellis (1991: 184–185) suggests a four-step strategy for critical thinking:

Step 1: Understand the point of view.

- Listen/read without early judgment.
- Seek to understand the source's background (e.g., culture, education, experience, and values).
- Try to "live in their shoes."
- Summarize their viewpoint.

Step 2: Seek other views.

- Seek viewpoints, questions, answers, ideas, and solutions from others.

Step 3: Evaluate the various viewpoints.

- Look for assumptions (i.e., an opinion that something is true, without evidence), exceptions, gaps in logic, oversimplification, selective perception, either/or thinking, and personal attacks.

Step 4: Construct a reasonable view.

- Study multiple viewpoints, combine perspectives, and produce an original viewpoint that is a creative act and the essence of critical thinking.

Why Think Critically about the History of Security and Loss Prevention?

The intent here is to stimulate the reader to go beyond memorizing historical events, names, and dates. If you have read several books in this field, the history chapters sound very similar. Did the writers, including this one, become complacent and repeat what has been written repeatedly about the history of this field? How do you know that the history of security and loss prevention as presented in this book and in others is objective?

Recorded history is filled with bias. Historians and scholars decide what subjects, events, innovations, countries, ethnic groups, religions, men, and women should be included or excluded from recorded history. In reference to the history of security and loss prevention, what have we missed? What subjects have been overemphasized? (A case problem at the end of this chapter asks the reader to critically think about the history of security and loss prevention.) In the policing field, for example, Weisheit, Baker, and Falcone (1995: 1) note that history and research reflect a bias toward urban police, at the expense of rural police. Do security researchers and writers overemphasize large proprietary security programs and large security service firms? What about the thousands of proprietary security programs at small companies and the thousands of small security service firms? Another question is what role did women and minorities play in the history of this field?

What country do you think has had the most impact on police and security in the United States? Our language, government, public and private protection, law, and many other aspects of our lives have deep roots in England. However, what about the role of other countries in the development of police and private security methods? Stead (1983: 14–15) writes of the French as innovators in crime prevention as early as the 1600s under King Louis XIV. During that time, crime prevention was emphasized through preventive patrol and street lighting. Germann, Day, and Gallati (1974: 45–46) write of early Asian investigative methods that used psychology to elicit confessions.

A critical thinking approach "opens our eyes" to a more objective perspective of historical events. The author is not seeking to rewrite history, or to change the basic strategies of security and loss prevention. Rather, the aim is to expand the reader's perception and knowledge as a foundation for smarter protection in a complex world.

Security and Loss Prevention Defined

Within our organized society, security is provided primarily by our armed forces, law enforcement agencies, and private security. The 9/11 attacks resulted in several changes in the way in which we organize public and private security. Post-9/11 security changes are covered in subsequent chapters.

During the last decades of the 20th century, the methods of private security became more specialized and diverse. Methods not previously associated with security emerged as important components of the total security effort. Security officers, fences, and alarms have been the hallmark of traditional security functions. Today, with society becoming increasingly complex, additional specialization—auditing, safety, fire protection, information technology (IT) security, crisis management, executive protection, terrorism countermeasures, to name a few—continuously are being added to the security function. Because of the increase in diverse specializations within the security function, many practitioners favor a broader term for all of these functions, known as *loss prevention.*

Another reason for the growing shift in terminology from security to loss prevention involves the negative connotations of security. Saul Astor (1978: 27) points out:

> *In the minds of many, the very word "security" is its own impediment.*
> *… Security carries a stigma; the very word suggests police, badges, alarms, thieves, burglars, and some generally negative and even repellent mental images…. Simply using the term "loss prevention" instead of the word "security" can be a giant step toward improving the security image, broadening the scope of the security function, and attracting able people.*

Because of additional specialization included in the security function and the frequently negative connotations associated with the term *security*, the all-encompassing term for describing the contents of this book is *loss prevention*. The security function and other specialized fields (auditing, safety, fire protection, etc.) are subsumed in loss prevention.

Security is narrowly defined as traditional methods (security officers, fences, and alarms) used to increase the likelihood of a crime-controlled, tranquil, and uninterrupted environment for an individual or organization in pursuit of objectives.

Loss prevention is broadly defined as almost any method (e.g., security officers, safety, auditing) used by an individual or organization to increase the likelihood of preventing and controlling loss (e.g., people, money, productivity, materials) resulting from a host of adverse occurrences (e.g., crime, fire, accident, natural disaster, error, poor supervision or management, bad investment). This broad definition provides a foundation for the loss prevention practitioner whose innovations are limited only by his or her imagination. It is hoped that these concepts not only will guide the reader through this book but also reinforce a trend in the use of these definitions.

Various employment titles are applied to individuals who perform security and loss prevention duties within organizations. The titles include Vice President, Director, or Manager of Security, Corporate Security, Loss Prevention, or Assets Protection.

Another title receiving attention is the **Chief Security Officer** (**CSO**). The *Chief Security Officer Guideline* (ASIS International, 2004) is designed "… as a model for organizations to utilize in the development of a leadership function to provide a comprehensive, integrated security risk strategy to contribute to the viability and success of the organization." This guideline is a response to an increasingly serious threat environment, and it recommends that the CSO report to the most senior level executive of the organization. The guideline lists specific risks, job duties and services, and skills required. The CSO designation and the guideline supporting it provide an excellent reference from which the security profession and senior management can draw on to improve the protection of people and assets and help organizations survive in a world filled with risks.

CSO (2004) defines the CSO position as follows:

> *The title Chief Security Officer (CSO) was first used principally inside the information technology function to designate the person responsible for IT security. At many companies, the term CSO is still used in this way. CISO, for Chief Information Security Officer, is an equivalent term, and today the CISO title is becoming more prevalent for leaders with an exclusive infosecurity focus.*
>
> *The CSO title is also used at some companies to describe the leader of the "corporate security" function, which includes the physical security and safety of employees, facilities and assets. More commonly, this person holds a title such as Vice President or Director of Corporate Security. This function has historically been distinct from information security.*
>
> *Increasingly, Chief Security Officer means what it sounds like: The CSO is the executive responsible for the organization's entire security posture, both physical and digital.*

Research conducted by Booz Allen Hamilton (2005) for ASIS International, the Information Systems Security Association, and the Information Systems Audit and Control Association, found that placing all security functions under one individual ("the strongest or most powerful of the various security elements") may not be beneficial ("an obvious and flawed option") for all organizations because it can reduce the influence of important managers in enterprisewide security. The study recommended a "business-focused council of leaders" consisting of representatives from various specializations—such as risk management, law, safety, and business continuity—who "come together using the corporate strategy as a common element on which to focus."

Security **is narrowly defined;** ***loss prevention*** **is broadly defined.**

History

Why Study the History of Security and Loss Prevention?

We should study the history of security and loss prevention because

- We learn of the origins of the profession and how it developed.
- We can see how voids in security and safety within society were filled by the private sector.

- We can learn of noted practitioners and theorists and their challenges, failures, and successes.
- We can compare security in the past to security in the present to note areas of improvement and areas requiring improvement.
- We can learn how security services and systems have been controlled and regulated.
- We can learn of the interaction of private security and public police over time.
- History repeats itself. We should strive to avoid the mistakes of the past and continue with successes.
- We can learn how social, economic, political, and technological forces have affected security over time.
- The past assists us in understanding the present, and it offers us a foundation to anticipate future events.

Early Civilizations

Prehistoric human beings depended on nature for protection because they had not learned how to build strong houses and fortifications. In cold climates, caves provided protection and shelter, whereas in the tropics, trees and thickets were used. Caves were particularly secure because rocky walls guarded tribes on all sides except at the cave mouth. To protect the entrance, redundant (i.e., duplicating to prevent failure) security was employed: large rocks acted as barriers when they were rolled in front of entrances; dogs, with their keen sense of smell, served to alarm and attack; and fires added additional defense. By living on the side of a mountain with access via a narrow, rocky ledge, cave dwellers were relatively safe from enemies and beasts. Early Pueblo Indians, living in what is now New Mexico and Arizona, ensured greater protection for themselves in their dwellings by constructing ladders that could be pulled in, and this defense proved useful until enemies attacked with their own ladders. *In fact, in early civilizations, as today, security measures have never been foolproof, and adversaries typically strive to circumvent (i.e., to go around) defenses.*

Throughout history, redundant security has been used to block adversaries attempting to circumvent defenses.

The **Great Wall of China** is the longest structure ever built. It was constructed over hundreds of years beginning in the 400s BC. Hundreds of thousands of workers lived their lives near the wall and participated in this huge project that stretched 4,000 miles and reached heights of 25 feet. Unfortunately, the wall provided protection only from minor attacks; when a major invasion force struck, the defense could not withstand the onslaught. The army of Mongol leader Genghis Khan swept across the wall during the AD 1200s and conquered much of China. Since 1949, the Chinese government has restored some sections of the mostly collapsed wall, which is a major tourist attraction (Feuerwerker, 1989: 373–374).

It is interesting to note the changing character of security through history. In earlier years, huge fortifications could be built with cheap labor, and a king could secure a perimeter with many inexpensive guards. Today, physical barriers such as fences and walls are expensive, as is the posting of security forces at physical barriers. One 24-hour post can cost over $100,000 annually for security personnel and physical security systems.

As societies became more complex, the concepts of leadership, authority, and organization began to evolve. Mutual association created social and economic advantages but also inequities, so people and assets required increased protection. Intergroup and intragroup conflicts created problems whose “solutions” often took the form of gruesome punishments, including stoning, flaying, burning, and crucifying. A person's criminal record was carried right on his or her body, through branding and mutilation. By 1750 BC the laws of **Hammurabi, King of Babylon**, not only codified the responsibilities of the individual to the group and the rules for private dealings between individuals, but also discussed retributive penalties (Germann, Day, and Gallati, 1974: 43).

Ancient Greece

Between the ninth and third centuries BC, ancient Greece blossomed as an advanced commercial and culturally rich civilization. The Greeks protected their advancing civilization with the **polis**, or city-state, which consisted of a city and the surrounding land protected by a centrally built fortress overlooking the countryside. A stratified society brought the ruling classes constant fear of revolution from below. Spartans, for example, kept their secret agents planted among the lower classes and subversives. *During the time of the Greek city-states, the first police force evolved to protect local communities, although citizens were responsible for this function.* The Greek rulers did not view local policing as a state responsibility, and when internal conflicts arose, they used the army. During this era, the Greek philosopher Plato introduced an advanced concept of justice, in which an offender not only would be forced to pay a sort of retribution, but also would be forced into a method of reform or rehabilitation.

Ancient Egyptians sealed the master locksmith in the tomb to prevent security leaks.

Ancient Rome

The civilization of ancient Rome also developed both commercially and culturally before the birth of Christ. Rome was located only 15 miles from the sea and could easily share in the trade of the Mediterranean. This city sat on seven hills overlooking the Tiber River, which permitted ease in fortification and defense. A primitive but effective alarm system was used by placing geese at strategic locations so their very sensitive hearing would trigger squawking at the sound of an approaching army.

The Roman regime was well designed to carry on the chief business of the Roman state, which was war. A phalanx of 8,000 foot-soldiers became the basic unit of a Roman army equipped with helmets, shields, lances, and swords. Later, a more maneuverable legion of 3,600 men armed in addition with iron-tipped javelins was used. These legions also were employed to maintain law and order. The first emperor of Rome, Augustus (63 BC–AD 14), created the **Praetorian Guard** to provide security for his life and property. These urban cohorts of 500 to 600 men were deployed to keep the peace in the city. Some believe that after about AD 6 this was the most effective police force until recent developments in law enforcement. Modern-day coordinated patrolling and preventive security began with the subsequent nonmilitary **vigiles**, night watchmen who were active in both policing and firefighting (Post and Kingsbury, 1977; Ursic and Pagano, 1974).

The Romans have an interesting history in fire protection. During the 300s BC, slaves were assigned firefighting duties. Later, improved organization established divisions encompassing hundreds of people, who carried water in jars to fires or brought large pillows so victims trapped in taller structures could jump with improved chances for survival. The completion of the aqueducts to Rome aided firefighting by making water easier to obtain. Hand pumps and leather hoses were other innovations.

The Middle Ages in Europe

During the Dark Ages, the period in history after the destruction of the ancient Greek and Roman empires, **feudalism** gradually developed in Europe. Overlords supplied food and security to those who farmed and provided protection around castles fortified by walls, towers, and a drawbridge that could be raised from its position across a moat. Even then, security required registration, licensing, and a fee—Henry II of England (reigned AD 1154–1189) destroyed more than 1,100 unlicensed castles that had been constructed during a civil war (Brinton, et al., 1973: 167).

Another mutual arrangement was the war band of the early Germans, the **comitatus**, by which a leader commanded the loyalty of followers, who banded together to fight and win booty. To defend against these bands of German barbarians, many landowners throughout Europe built their own private armies. (The term **posse comitatus** denotes a body of citizens that authority can call on for assistance against offenders. The **Posse Comitatus Act** is a Civil War–era act that generally prohibits the military from engaging in civilian law enforcement. This law has been labeled as archaic because it limits the military from responding to disasters.)

Much of the United States' customs, language, laws, and police and security methods can be traced to its English heritage. For this reason, England's history of protection is examined here.

Between the 7th and 10th centuries, the frankpledge system and the concept of tithing fostered increased protection. The **frankpledge system**, which originated in France and spread to England, emphasized communal responsibility for justice and protection. The **tithing**, or group of 10 families, shared the duties of maintaining the peace and protecting the community.

In 1066, William, Duke of Normandy (in present-day France), crossed the English Channel and defeated the Anglo-Saxons at Hastings. A highly repressive police system developed under martial law as the state appropriated responsibility for peace and protection. Community authority and the tithing system were weakened. William divided England into 55 districts, or *shires*. A *reeve*, drawn from the military, was assigned to each district. (Today, we use the word *sheriff*, derived from *shire-reeve*.) William is credited with changing the law to make a crime an offense against the state rather than against the individual and was instrumental in separating police from judicial functions. A traveling judge tried the cases of those arrested by the shire-reeves.

In 1215 King John signed the **Magna Carta**, which guaranteed civil and political liberties. Local government power increased at the expense of the national government, and community protection increased at the local level.

Another security milestone was the **Statute of Westminster** (1285), issued by King Edward I to organize a police and justice system. A **watch and ward** was established to keep the peace. Every town was required to deploy men all night, to close the gates of walled towns at night, and to enforce a curfew.

What similarities can you draw between security strategies of earlier civilizations and those of today?

More Contemporary Times

England

For the next 500 years, repeated attempts were made to improve protection and justice in England. Each king was confronted with increasingly serious crime problems and cries from the citizenry for solutions. As England colonized many parts of the world and as trade and commercial pursuits brought many people into the cities, urban problems and high crime rates persisted. Merchants, dissatisfied with the protection afforded by the government, hired private security forces to protect their businesses.

By the 18th century, the Industrial Revolution compounded urban problems. Many citizens were forced to carry arms for their own protection, because a strong government policing system was absent. Various police and private security organizations did strive to reduce crime; **Henry Fielding**, in 1748, was appointed magistrate, and he devised the strategy of preventing crime through police action by helping to form the famous **Bow Street Runners**, the first detective unit. The merchant police were formed to protect businesses, and the Thames River police provided protection at the docks. During this period, more than 160 crimes, including stealing food, were punishable by death. As pickpockets were being hanged, others moved among the spectators, picking pockets.

Do you think policing and justice were impotent during the early Industrial Revolution in England? Do you think we have a similar problem today in the United States?

Peel's Reforms

In 1829, **Sir Robert Peel** worked to produce the **Metropolitan Police Act** that resulted in a revolution in law enforcement. Modern policing was born. Peel's innovative ideas were accepted by Parliament, and he was selected to implement the act that established a full-time, unarmed police force with the major purpose of patrolling London. Peel is credited also with reforming the criminal law by limiting its scope and abolishing the death penalty for more than 100 offenses. It was hoped that such a strategy would gain public support and respect for the police. Peel was very selective in hiring his personnel, and training was an essential part of developing a professional police force. Peel's reforms are applicable today and include crime prevention, the strategic deployment of police according to time and location, a command of temper rather than violent action, record keeping, and crime news distribution.

Although Sir Robert Peel produced a revolution in law enforcement in 1829, crime and the private security industry continued to grow.

Early America

The Europeans who colonized North America had brought with them the heritage of their mother countries, including various customs of protection. The watchman system and collective responses remained popular. A central fortification in populated areas provided increased security from hostile threats. As communities expanded in size, the office of sheriff took hold in the South, whereas the functions of constable and watchman were the norm in the Northeast. The sheriff's duties involved apprehending offenders, serving subpoenas, and collecting taxes. Because a sheriff was paid a higher fee for collecting taxes, policing became a lower priority. Constables performed a variety of tasks such as keeping the peace, bringing suspects and witnesses to court, and eliminating health hazards. As in England, the watch system had its share of inefficiency, and to make matters worse, those convicted of minor crimes were sentenced to serve time on the watch.

The watch also warned citizens of fire. In colonial towns, each home had to have two fire buckets, and homeowners were subject to a fine if they did not respond to a fire, buckets in hand. A large fire in Boston in 1679 prompted the establishment of the first paid fire department in North America (Bugbee, 1978: 5).

The Growth of Policing

The period of the middle 1800s was a turning point for both law enforcement and private security in America, as it had been in England. Several major cities (e.g., New York, Philadelphia, San Francisco) organized police forces, often modeled after the London Metropolitan Police. However, corruption was widespread. Numerous urban police agencies in the Northeast received large boosts in personnel and resources to combat the growing militancy of the labor unions in the late 1800s and early 1900s. Many of the large urban police departments originally were formed as strikebreakers (Holden, 1986: 23). Federal policing also experienced growth during this period. The U.S. Treasury had already established an investigative unit in 1864. As in England, an increase in public police did not quell the need for private security.

The History of Loss Prevention in a Nutshell

Loss prevention has its origin in the insurance industry. Before the Civil War, insurers gave minimal attention to the benefits of loss prevention. For instance, in the fire insurance business, executives generally viewed fires as good for business. Insurance rates were based on past loss experience, premiums were paid by customers, losses were paid to unfortunate customers, and a profit was expected by the insurer. When excessive fire losses resulted in spiraling premiums, the changing nature of the fire insurance business created a hardship for both the insurer and the insured. Insurance executives were forced to raise premiums to cover losses, and customers complained about high rates. The predominance of wooden construction (even wooden chimneys) in dense urban areas made fire insurance unaffordable for many. A serious fire peril persisted.

After the Civil War, loss prevention began to gain momentum as a way to reduce losses and premiums. Fire insurance companies formed the National Board of Fire Underwriters, which, through the use of engineering, investigation, research, and education, was credited with preventing losses. In 1965, the board was merged into the American Insurance Association (AIA). AIA activities have brought about the development of the National Building Code, a model code adopted by many municipalities to reduce fire losses.

Today, executives throughout the insurance industry view loss prevention as essential. Many insurers have loss prevention departments to aid themselves and customers. Furthermore, customers (i.e., the insured), to reduce premiums, have become increasingly concerned about preventing losses. Management in many businesses instituted loss prevention strategies (e.g., fire protection). The security department within businesses repeatedly handle these strategies, which results in an expanded role for security. Expansion of the security function to such fields as fire protection and safety has led to the use of the broader term *loss prevention* rather than *security*.

The Growth of Security Companies

In 1850, **Allan Pinkerton**, a cooper, opened a detective agency in the United States after becoming the Chicago Police Department's first detective. Because public police were limited by geographic jurisdiction, they were handicapped when investigating and apprehending fleeing offenders. This limitation facilitated the growth of private security. Pinkerton (see Figure 1-1) and others became famous as they pursued criminals across state boundaries throughout the country. Today, Pinkerton Service Corporation is a subsidiary of Securitas, based in Stockholm, Sweden.

During the 1800s, because public police were limited by geographic jurisdiction and restrained from chasing fleeing offenders, private security filled this need and became a growth industry.

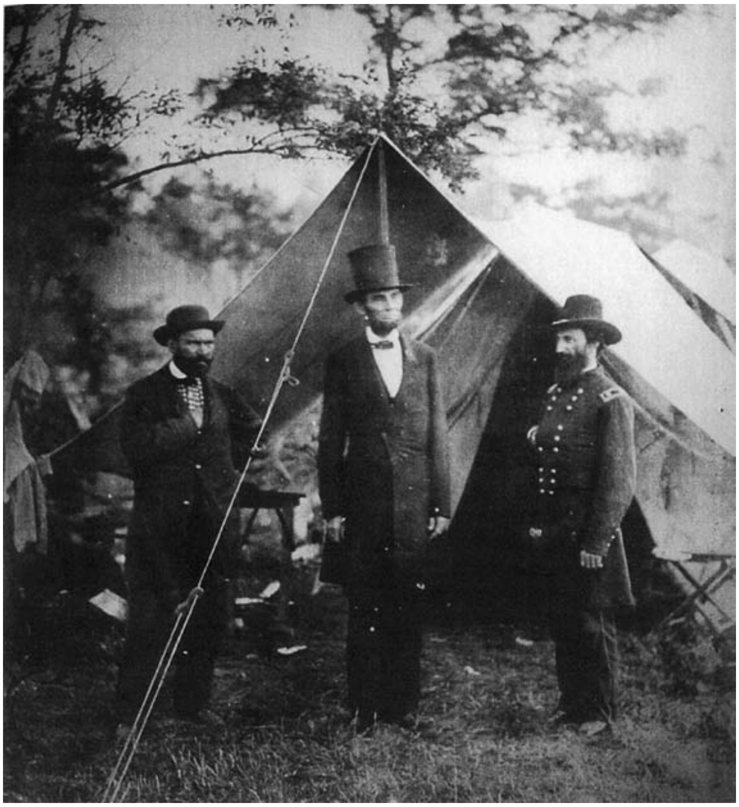

FIGURE 1-1 Major Allan Pinkerton, President Lincoln, and General John A. McClellan, Antietam, MD, October 1862. *Courtesy:* National Archives.

To accompany Americans' expansion westward during the 19th century and to ensure the safe transportation of valuables, **Henry Wells** and **William Fargo** supplied a wide-open market by forming Wells, Fargo & Company in 1852, opening the era of bandits accosting stagecoaches and their shotgun riders. Wells Fargo was acquired by Burns International Services Corporation. The name Wells Fargo is exclusive to Wells Fargo & Company, a large financial services business.

Another security entrepreneur, **William Burns**, first was a Secret Service agent who directed the Bureau of Investigation that preceded the FBI. In 1910, this experienced investigator opened the William J. Burns Detective Agency (see Figure 1-2), which became the investigative arm of the American Bankers Association. Today, Burns International Services Corporation is a subsidiary of Securitas.

Washington Perry Brink, in 1859, also took advantage of the need for the safe transportation of valuables. From freight and package delivery to the transportation of payrolls, his service required increased protection through the years as cargo became more valuable and more vulnerable. Following the killing of two Brink's guards during a robbery, the armored truck was initiated in 1917. Today, the Brink's Company is a leading global security services company. It provides secure transportation services, and it monitors home security systems.

Edwin Holmes is another historical figure in the development of private security in the United States. He pioneered the electronic security alarm business. During 1858, Holmes had a difficult time convincing people that an alarm would sound on the second floor of a home when a door or window was opened on the first floor. His sales strategy was to carry door-to-door a small model of a home containing his electric alarm system. Soon sales soared, and

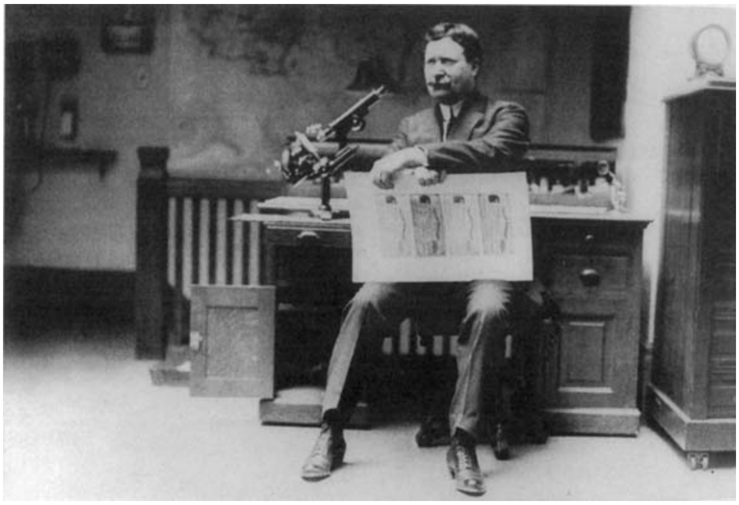

FIGURE 1-2 In 1910, William J. Burns, the foremost American investigator of his day and the first director of the government agency that became the FBI, formed the William J. Burns Detective Agency.

the first central office burglar alarm monitoring operation began. Holmes Protection Group, Inc., was acquired by ADT Security Services, Inc., at the end of the 20th century.

Since 1874, ADT Security Services, Inc., has been a leader in electronic security services. Originally known as American District Telegraph, ADT has acquired numerous security companies since its inception. Today, it is a unit of Tyco Fire and Security Services. ADT is a provider of electronic security services (i.e., intrusion, fire protection, closed-circuit television or CCTV, access control) to millions of commercial, federal, and residential customers.

The Wackenhut Corporation is another leader in the security industry. Founded in 1954 by **George Wackenhut**, a former FBI agent, the corporation extended its services to government agencies, which resulted in numerous contracts since its inception. The Wackenhut Corporation is the U.S.-based division of Group 4 Securicor, located in the United Kingdom.

Railroads and Labor Unions

The history of private security businesses in the United States must include two important events of the 19th century: the growth of railroads and labor unions.

Although railroads were valuable in providing the vital East–West link that enabled the settling of the American frontier, these powerful businesses used their domination of transportation to control several industries, such as coal and kerosene. Farmers were especially hurt in economic terms because they had no alternative but to pay high fees to transport their products via the railroads. The monopolistic practices of railroads created considerable hostility; when Jesse James and other criminals robbed trains, citizens applauded. Railroads could not rely on public police protection because of jurisdictional boundaries. Consequently, numerous states passed laws enabling railroads to organize proprietary security forces with full arrest powers and the authority to apprehend criminals transcending multiple jurisdictions. Railroad police numbered 14,000 by 1914. During World War I, they were deputized by the federal government to ensure protection of this vital transportation network.

The growth of labor unions at the end of the 19th century resulted in increased business for security firms who acted as strikebreakers for large corporations. However, this venture proved costly. A bloody confrontation between Pinkerton men and workers at the Carnegie steel plant in Homestead, Pennsylvania, resulted in eight deaths (three security men and five workers). Pinkerton's security force surrendered. The plant then was occupied by federal troops. Senate hearings followed the Homestead disaster and "anti-Pinkertonism" laws were enacted to restrict private security. However, local and state police forces began to emerge quickly to deal with strikers (Shelden, 2001: 84). Later, the Ford Motor Company and other businesses were involved in bloody confrontations. Henry Ford had a force of about 3,500 security personnel, spies, and "sluggers" (i.e., private detectives), who were augmented by various community groups such as the Knights of Dearborn and the Legionnaires. The negative image brought to the public eye by newspaper coverage tarnished many businesses and security firms. Prior to World War II, pressure from Congress, the Roosevelt Administration, labor unions, and the ACLU caused corporate management to shift its philosophy to a softer "public relations" approach (Shelden, 2001: 92).

The Great Wars

World Wars I and II brought about an increased need for protection in the United States. Sabotage and espionage were serious threats. Key industries and transportation systems required expanded and improved security. The social and political climate in the early 20th century reflected urban problems, labor unrest, and worldwide nationalism. World War I compounded these turbulent times and people's fears. Security became a primary concern. A combination of the "war to end all wars," Prohibition, intense labor unrest, and the Great Depression all overtaxed public police. Private security companies helped fill the void.

By the late 1930s, Europe was at war again, and the Japanese were expanding in the Far East. A surprise Japanese bombing of the Pacific Fleet at Pearl Harbor in 1941 jolted the United States into World War II, and security concerns appeared again. The United States went into full production, and protection of vital industries became crucial, leading the federal government to bring plant security personnel into the army as an auxiliary to military police. By the end of the war, more than 200,000 of these security workers had been sworn in.

The Third Wave

In the decades following World War II, private security expanded even more; during the 1950s, the Korean War and the unrelenting "cold war" created worldwide tension and competition between the democracies and communist regimes. The Department of Defense, in 1952, strengthened the security requirements of defense industries to protect classified information and materials. When the Soviets successfully launched the first earth satellite (Sputnik, in 1957) and first reached the moon with an unmanned rocket (1959), Americans were stunned. The technological race became more intense, and information protection became more important.

The turbulent 1960s created massive social and political upheaval in the United States, and public police forces were overwhelmed by responses to the unpopular Vietnam war; protests over the denial of civil rights to minority groups; the assassinations of President John F. Kennedy, Senator Robert Kennedy, and the Reverend Martin Luther King, Jr.; and rising crime and drug problems. Private security boomed.

Protests, crime, terrorism, and limited public police resources marked the 1970s, 1980s, and 1990s. By this time, the advanced nations of the world had developed into what Alvin Toffler's (1980) *The Third Wave* and John Naisbitt's (1982) *Megatrends* call **third wave societies**: societies based on information and technology. (**First wave societies** had agriculture as a foundation, and these dominated the world for thousands of years, deriving energy from human and animal power. Offenders stole cattle, gold, and other valuables. **Second wave societies** occurred during the Industrial Revolution when production was powered by irreplaceable energy sources such as coal and oil. Criminals focused on money and booming economic conditions.) With the depletion of world resources, the world is becoming more dependent on technology and information; and "third wave" criminals exploit technology to commit their crimes, the extent of which is limited only by technological innovation and the offenders' imaginations.

"Has Cybercrime Surpassed Physical Crime?"

Gips (2006: 24) asked the preceding question in response to an IBM survey of mostly chief information officers. Sixty percent viewed cybercrime as more costly to their business than physical crime. Gips notes that it is difficult to measure and compare cybercrime and physical crime because "studies that attempt to quantify security losses across sectors and types of crime are based on extrapolation and guesswork." He argues that the cost of physical crime in the United States easily outpaces the cost of cybercrime. Gips refers to several sources on annual costs of crime: the FBI estimates that cybercrime costs about $400 billion and counterfeit goods cost about $250 billion; the Association of Certified Fraud Examiners estimates that occupational crime (e.g., altering checks, setting up fictitious accounts) costs about $652 billion; cargo theft costs "tens of billions" of dollars according to the International Cargo Security Council; retailers lose about $40 billion from shrinkage and inventory loss; and physical crime losses often exclude indirect costs, such as defending and paying judgments on lawsuits alleging negligent security. Gips concludes his arguments by noting that "if you think you are at risk for cybercrime, that's likely where you will devote your resources. And if the risk lies elsewhere, that could mean that the company's more costly vulnerabilities will not be adequately addressed."

Convergence of IT and Physical Security

Today, the third wave is continuing with three notable occurrences affecting security. First, terminology is changing. Examples are *cybercrime* and *denial of service*. Second, two distinct security camps have emerged: information technology (IT) security specialists and physical security specialists. Generally, the former possess a background geared to protect against computer-related crime and unauthorized intrusions into IT systems, whereas the latter focus on traditional security duties (e.g., perimeter security, access controls, and contract security forces). Third, both camps often use similar terminology and perform similar duties. Terms common to both groups include *denial of access* and *intrusion detection*. Similar duties can be far reaching and include investigations, information security, loss prevention, and risk management. Jim Spencer (2000: 1-13), writing in *iSecurity*, adds that these two groups have their own suppliers, consultants, publications, associations, and trade shows.

For several years, *cross-training* has been a buzzword for various vocations, such as for investigators and auditors. History repeats itself and we have a need for cross-training for IT and physical security specialists. Each specialist can assist the other with data, technologies, access controls, biometrics, investigations, and business continuity, among other areas. Cooperative planning is essential. Suppose an employee is fired at a company. Security officers and access control systems customarily deny the former employee entrance to the company facility. However, today, protection requires broader applications because of remote access to IT systems. *An offender no longer has to physically trespass to steal and do harm to an organization*. We can only guess at the number of times the traditional security manager has done an excellent job of ensuring that security officers are patrolling, physical security is operational, and the facility is protected, except that a hacker has penetrated the corporate IT system and stolen proprietary information or caused other harm to the business. Physical security specialists and IT specialists must work together for comprehensive protection. As explained earlier, an executive with a title such as Vice President of Security, Vice President of Loss Prevention, or Chief Security Officer can manage all aspects of security (i.e., physical and digital), work to ensure organizational survival, and report to senior executives.

Convergence of IT and physical security means that both specializations and related technologies unite for common objectives. Efforts to secure access to databases, e-mail, and organizational intranets are merging with access controls, fire and burglar alarm systems, and video surveillance. Physical security is increasingly relying on IT systems and related software. Both IT systems and physical security systems have sensors that generate data that is managed. As examples, an IT system will have an antivirus program and a physical security system will have motion detectors.

Bernard (2007: 475) notes that "convergence relating to security is occurring at two levels: technology and management." At the technology level is the convergence of digital information technology with electronic security systems. At the security management level, convergence is the integration of physical security functions, IT security, and security risk management.

There are advantages from the convergence of IT and physical security. These include the opportunity for security personnel to monitor physical security remotely from almost anywhere in the world, less travel time and expenses for monitoring and investigations, and easier software upgrades. Two disadvantages are a virus may affect physical security when sharing a single server; and an organization's bandwidth may reach its limit from the requirements of video surveillance.

Gural (2005: 9) cites a report from Forrester Research that shows increases in organizational spending that brings traditional security functions—CCTV, access controls, and security officer duties—onto the same platform as such functions as IT network access management. In addition, software is increasingly being used for detection and response instead of relying on only personnel. *Security Management* (Tech Talk, 2004: 45) notes that as traditional physical security increasingly relies on IT systems, IT specialists in organizations are playing a larger role in physical security decisions. IT specialists want to ensure that physical security technology is compatible with the network and safe from virus infections and hackers. Physical security purchasing decisions in organizations often consist of a committee of personnel from security or loss prevention, IT, and operations. Generally, the IT department has a larger budget than the security department, and this may increase the clout of IT in purchasing decisions. Furthermore, if IT managers can convince senior management that cybercrime is a greater threat than physical crime, then this also will influence the direction of the security budget (Computer Business Review, 2006).

Another player in corporate management change is the facility manager. This individual, often an engineer, ensures that the company's infrastructure, which houses people and operations, functions at optimum efficiency to support business goals. The traditional security department is likely to feel a "pull" toward IT or the facility manager because its boundaries are dissolving as a result of information and communications technology. The process of management is increasingly dependent on information, who controls it, what is done with it, and its dissemination. The power of IT especially is growing (Freeman, 2000: 10).

There are those who may claim the demise of the traditional security manager, who will be replaced by the IT manager or facility manager. The argument is that if an offender enters a facility and steals a computer, this crime is minor in comparison to, say, the potential harm from a hacker accessing a company's IT system. Such reasoning misses the broad, essential functions performed by the traditional security manager and staff. Examples are preventing crimes against people, responding to crimes, rendering first aid, conducting investigations, working with public police to arrest offenders, life safety, and fire protection. At the same time, traditional security practitioners must be put on notice to become involved in lifelong learning of IT systems, which touch all aspects of their traditional duties.

Convergence of Enterprise Security

Convergence of enterprise security refers to the merging of security functions throughout the entire business enterprise (i.e., business organization). Research conducted by Booz Allen Hamilton (2005) for ASIS International, and others, showed a trend of convergence of all components of security in organizations. The research report titled *Convergence of Enterprise Security Organizations* explains convergence in broad business terminology and emphasizes an enterprisewide view of risk. "Delivering on convergence is not just about organizational integration; rather it is about integrating the security disciplines with the business' mission to deliver shareholder value." "To be effective this converged approach should reach across people, processes, and technology, and enable enterprises to prevent, detect, respond to, and recover from any type of security incident." The research report referred to an incident at the Sumitomo Mitsui Bank in London, England, to illustrate the importance of merging security functions throughout the entire business enterprise. Although the bank had strong IT security measures, hackers took advantage of a lapse in physical security by posing as janitors and installing devices on computer keyboards that permitted them to obtain valuable login information. In 2004, in only three days the MyDoom e-mail virus caused about $22.6 billion in damages as it spread to more than 200 countries. Besides the initial costs of such incidents, long-term harm can damage reputation and brand, and if the incident threatens the public good, regulators may enact stricter regulations of business practices.

Surveys and interviews from the Booz Allen Hamilton research point to several internal and external drivers that are influencing the trend in convergence. They are

- *Rapid expansion of the enterprise ecosystem.* Enterprises are becoming more complex in a global economy of external partners.
- *Value migration from the physical to information-based and intangible assets.* Value is continuing to shift from physical to information-based assets.
- *New protective technologies blurring functional boundaries.* Technology is causing an overlap between physical and IT security.
- *New compliance and regulatory regimes.* Regulations are increasing in response to new threats and business interactions.
- *Continuing pressure to reduce cost.* Enterprises are constantly striving to efficiently reduce risk.

□ □ □

Many companies have two security directors, one for IT and the other for physical security. Do you agree with this approach? Why or why not?

□ □ □

Twenty-First Century/Post-9/11 Security Challenges

The last decade of the 20th century offered warnings of what was to come in the next century. The 1990s brought the first bombing of the World Trade Center, the bombing of the Murrah Federal Building in Oklahoma City, the first war with Iraq, crimes resulting from the Internet, the increased value of proprietary information, and attention to violence in the workplace.

As we know, not long into the 21st century, on September 11, 2001, terrorists attacked the World Trade Center and the Pentagon. Following the attacks, a crisis in confidence in government occurred. Citizens asked: How could the most powerful nation on earth be subject to such a devastating attack? What went wrong? Who is to blame? In response to the crisis, President George Bush declared war on terrorism. He appointed a new Cabinet position, the Office of Homeland Defense, to coordinate counterterrorism. The attacks also led to greater police powers for search and seizure and electronic surveillance, and the age-old question of how to balance police powers and constitutional rights.

These bold, surprise attacks, subsequent bioterrorism (i.e., anthrax attacks through the U.S. Postal System), the war in Afghanistan, and the second war in Iraq show the difficult challenges facing our world in this new century. The United States and its allies are not only faced with conflict in Iraq, Afghanistan, and other regions, but also old and emerging state competitors and the proliferation of weapons of mass destruction.

The 21st century has also recorded huge natural disasters that—along with the problem of terrorism—necessitate a rethinking of emergency management and business continuity. Hurricanes Katrina and Rita, in 2005, devastated Gulf-coast states. Katrina flooded New Orleans. The December 2004 Sumatran Tsunami killed almost 300,000 people and affected 18 countries around the Indian Ocean. The human and financial strain on nations in preparing for and responding to natural and accidental threats is overwhelming. These challenges require global cooperation, a broad base of knowledge, skills from many disciplines, and continued research.

From a business perspective, security and loss prevention practitioners are faced with serious challenges and questions as they assist their employers with surviving in a constantly changing world filled with risks. How can businesses and institutions protect employees, assets, and operations from terrorism and other risks? What does the future hold? Who will pay for protection? Although this book offers some insight into these questions, the answers are still being developed.

A rethinking of strategies will meet these threats. Through improved education, training, research, professionalism, creativity, astute planning, and support from our business and government leaders, security professionals will provide a safer environment.

□ □ □

Search the Web

Access the Web and seek an international perspective by visiting the New Scotland Yard, which includes links to history: http://www.met.police.uk

Use your favorite search engines to check the sites of major security companies. For example: http://www.pinkertons.com/

What did you learn from these sites?

□ □ □

Case Problems

1A. As a security manager you are asked to speak to a local college class on the history and development of the security and loss prevention field. What five significant points in the history of this field do you emphasize?

1B. As a part-time security officer and a full-time college student, you are now working on an assignment to think critically about the history of security and loss prevention and prepare a typed report. The assignment requires you to focus on some aspect of the history of security and loss prevention that you believe is biased or inaccurate, and to explain your interpretation of historical events.

1C. As Director of Security for a corporation, you are responsible for security officer operations, investigations, and physical security. You presently report to the Senior Vice President. A pending reorganization may place you, your department, and its budget under the supervision of either the Director of IT or the Director of Facilities. You may become an Assistant Director. Time is now available for possible negotiation. Changes will be finalized in three months. Soon you will be meeting with the Senior Vice President. Are you in favor of the pending changes? What suggestions do you offer? If you would like to maintain the present position of security, what justification and value do you offer your supervisor and the corporation? What justification and value do you think your supervisor will present to you to support change?

References

ASIS International. (2004). *Chief Security Officer Guideline*. www.asisonline.org, retrieved May 1, 2006.

Astor, S. (1978). *Loss Prevention: Controls and Concepts*. Stoneham, MA: Butterworth.

Bernard, R. (2007). "Convergence of Physical Security and IT." In J. Fay (Ed.), *Encyclopedia of Security Management,* 2nd ed. Burlington, MA: Elsevier Butterworth-Heinemann Pub.

Booz Allen Hamilton. (2005). *Convergence of Enterprise Security Organizations*. (November 8). www.securitymanagement.com, retrieved January 27, 2006.

Brinton, C., et al. (1973). *Civilization in the West*. Englewood Cliffs, NJ: Prentice-Hall.

Bugbee, P. (1978). *Principles of Fire Protection*. Boston: National Fire Protection Association.

CSO. (2004). "What Is a Chief Security Officer?" *CSO* (September 13). http://www.csoonline.com/research/leadership/cso_role.html, retrieved May 1, 2006.

Computer Business Review. (2006). "Survey Says Cyber Crime Overtakes Physical Crime." *Computer Business Review Online*. www.cbronline.com, retrieved March 24, 2006.

Ellis, D. (1991). *Becoming a Master Student*, 6th ed. Rapid City, SD: College Survival, Inc.

Feuerwerker, A. (1989). "Great Wall of China." *World Book Encyclopedia*. Chicago, IL.

Freeman, J. (2000). "Security Director as Politician." *Security Technology & Design* (August).

Germann, A., Day, F., and Gallati, R. (1974). *Introduction to Law Enforcement and Criminal Justice*. Springfield, IL: Thomas Pub.

Gips, M. (2006). "Has Cybercrime Surpassed Physical Crime?" *Security Management*, 50 (July).

Gural, A. (2005). "Convergence Proves More Than Fad." *Security Director News*, 2 (February).

Holden, R. (1986). *Modern Police Management*. Englewood Cliffs, NJ: Prentice-Hall.

Naisbitt, J. (1982). *Megatrends*. New York: Warren Books.

Post, R., and Kingsbury, A. (1977). *Security Administration: An Introduction*, 3rd ed. Springfield, IL: Charles C. Thomas.

Safi, A., and Burrell, D. (2007). "Developing Critical Thinking Leadership Skills in Homeland Security Professionals, Law Enforcement Agents and Intelligence Analysts." *Homeland Defense Journal*, 5 (June).

Shelden, R. (2001). *Controlling the Dangerous Classes*. Boston, MA: Allyn & Bacon.

Spencer, J. (2000). "Of a Single Mind." *iSecurity* (November).

Stead, P. (1983). *The Police of France*. New York: Macmillan.

Tech Talk. (2004). "IT Gains Clout in Making Security Decisions." *Security Management*, 48 (June).

Toffler, A. (1980). *The Third Wave*. New York: Morrow.

Ursic, H., and Pagano, L. (1974). *Security Management Systems*. Springfield, IL: Charles C. Thomas.

Weisheit, R., Baker, L., and Falcone, D. (1995). *Crime and Policing in Rural and Small Town America: An Overview of the Issues*. Washington, DC: National Institute of Justice.