CHAPTER 9

A Sampling of Settings

After reviewing the basics in Part I and then taking a look at the multiple layers of security that can be applied to any target environment outlined in Part II, readers will begin to see how ideas about security and the process for identifying security objectives begins to take shape. Chapter 3 provided a series of snapshot scenarios to use to consider how some of the basic threat and risk related security concepts from Part I could be discussed in various settings.

Those new to the security industry may have difficulty in their initial efforts to apply these concepts in different environments. This is an acquired skill and takes some practice. So practice. This chapter provides an opportunity to play with the ideas presented in the text so far, and will allow you to play with these ideas more fully by offering the chance to consider these ideas in four fairly comprehensive, yet totally fabricated, target environments. In class we call this "target practice."

The target environments include a bank, an airport, a school, a hospital, and a convenience store. Think about the security issues you are likely to encounter and then plan a security response for each of these settings. Consider an abbreviated list of the topics discussed in the book so far: threat identification, assessment of risk levels, physical security, asset protection, information security, computer security, personnel issues, and security management. Your goal is to take this information and develop a clear set of security objectives. Maybe you even want to provide an integrated system. Maybe you want to identify the threats to the environment. How would your evaluation differ if you do it by yourself, or if you do it with two other students? How much research can you do to help you make decisions about the threat list and possible countermeasure responses?

Certainly, there is no way to provide information about any environment in such a short scenario. Consider the information provided in this chapter to be only general background information. Get to know the setting by looking at the relevant sample floor plan, and then begin the process of identifying and exploring information about securing that particular environment. Even with the floor plans provided, you will have to make some assumptions about the settings. If you get stuck, make a note about the information you think you need in order to move forward with a decision and then move on to other things. These exercises are appropriate for individuals, groups, or for the entire class,

ISBN: 0-536-91271-8

if you have one. They are always fascinating, loads of fun, and, without exception, informative.

USING THE STRUCTURE OF THE TEXT AS A GUIDE

One approach to using this chapter might be to do a security evaluation for each setting, based on the information presented in the previous chapters. For each setting, review the basics from Part I, including environmental conditions, threats, risk levels, and countermeasures, and then expand on those to include the internal security issues presented in Part II. Again, these are physical security and asset protection, information and computer security, and personnel and security management. Think about how these distinct elements of the security response could be integrated and connected into an overarching security plan. No two readers will develop exactly the same plan, and that is fine.

The objective here is to take time to think through the layers of security and spend time considering the breadth and depth of their importance in a specific target environment. Security must be seen as being bigger than just buying cameras and contracting with an alarm company. Attention must be given to the concepts, the essential pieces of the larger security system. I teach my students that specific information may not always be useful, but if you understand the concepts and general principles behind the specifics you can take that information anywhere and make it work for you.

Consider using the plan in Exhibit 9–1 as a guide to the chapter. Note that public law enforcement, legal liability, and disaster responses (including accidents and emergencies) are involved in an overall security management strategy, but they are discussed in Part III as external connections. After spending time with Chapters 10, 11, and 12, revisit these scenarios with an eye toward linking your existing security objectives with these external connections.

The Selected Settings

Each case study begins with a sample floor plan that I made up. Information collected from recent journal articles and trade publications about that type of target environment follows. This information is not exhaustive. Just as in real-life target environments, security professionals get to know what else they need to know by going beyond the information provided. Readers may choose to look beyond this information and bring in additional resources. It is not the job of the people working within the environment to provide a security professional with everything he or she needs to know about security in that setting. Security professionals must research both their environment and environments with similar security-related concerns, in an effort to better serve the needs of the target setting. Such is the task you now have before you.

ISBN: 0-536-91271-8

Exhibit 9–1 Proposed Plan for Reading about Each Setting

1. Draft a list of individual security objectives for areas within the target environment.
2. Draft a statement detailing the overall security objectives for the target environment.
3. Identify a list of likely threats and assign related risk levels.
4. Consider the physical security concerns.
   - Using the "layer of defense" process or the "interior/exterior" threat identification process, discuss physical security options.
   - Identify technologies that would be useful in the setting to ensure physical security.
5. Consider asset protection.
   - What areas in the environment include assets important to the company?
   - What actions should be taken to enhance security for these targeted areas?
   - What assets are going to be particularly troublesome to protect?
   - What specific conditions may make providing adequate security difficult?
   - What technologies would be useful in the setting to protect the assets?
6. Consider the information and computer security needs.
   - What information in the target environment needs securing?
   - What would a policy and procedure manual for that environment contain?
   - What computer system (networks, etc.) are at work in the environment?
   - What vulnerabilities are likely to exist in the computer systems?
7. Consider the personnel issues.
   - Is it better to use contract or proprietary security personnel in the environment?
   - How should hiring and employee selection be handled in the environment?
   - What groups of people will spend time in the environment?
   - What responsibilities will nonsecurity personnel within the environment have for security?
8. Consider the security management concerns.
   - What role do different divisions of the company plan in security?
   - What is the structure of the group of security professionals within the target environment?
   - What authority do the security professionals have?
   - What coordinating efforts are necessary for addressing a threat?
9. Consider the goal of integrating security objectives.
   - How do agencies and divisions within the target environment relay information to each other?
   - How do agencies and divisions relate to each other?
   - How do agencies and divisions relate to the overall security objective?
10. Think about the generalizations you have been forced to make during this exercise. Which of your responses might change as a result of adding additional information about the site-specific conditions in a given target environment?

Another thing readers may want to keep in mind is the fact that many large environments (e.g., hospitals, airports) will have different people in charge of different aspects of their security and/or management operation. Most security professionals do rely on other security professionals. For purposes of this chapter, however, readers should imagine that they are the security manager charged with directing the development of the overall security plan in each setting.

ISBN: 0-536-91271-8

TARGET ENVIRONMENT: HOSPITAL

Hospitals (Figure 9–1) must be prepared for everything. If there is an accident involving multiple victims, the hospital must be prepared to address the needs of a large number of people—sometimes without much notice. Most hospitals have many different parts, including maternity wards, operating rooms, recovery rooms, intensive care areas, emergency rooms, patient waiting areas, pharmacies, gift shops, and food service areas. There are different security concerns for each division.

Specific threats in the hospital will differ, depending on the area of the hospital. Risk levels associated with those threats may also differ. Consider the following issues as they relate to the security needs of a hospital:

- Most hospitals are shifting paper medical records to computer databases that contain electronic medical records.[1] Hospitals, like other organizations in other industries, are moving toward an organized information system, with a chief information officer coordinating this effort.[2] How can patient information be protected yet still readily available to medical personnel?
- Between 1983 and 1998, 103 babies under six months of age were abducted from health care facilities by nonfamily members.[3] Newborns were taken from the mother's hospital room, the nursery, the pediatrics

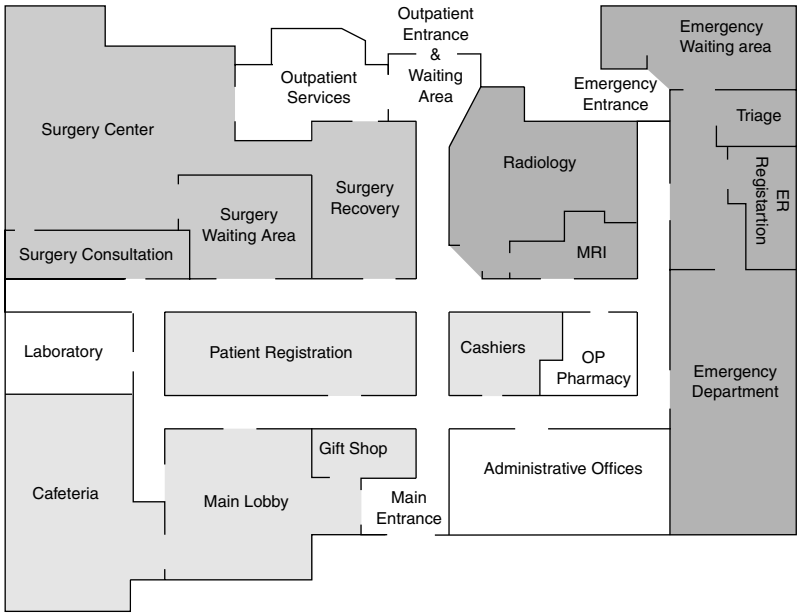

FIGURE 9–1 Sample Target Environment: Hospital

ISBN: 0-536-91271-8

unit, or elsewhere on the facility property. Most of the babies have been recovered; six remain missing.[4]

- Hospitals with psychiatric wards face additional threats and risks.[5,6]
- Various steps must be taken by hospital personnel to prevent the transmission of disease. One of the most prominent occupational risks to health care workers is exposure to blood-borne viruses. While disease transmission to workers can take place in various ways, much research has been done on the process of taking blood from the patient.[7]
- Hospital emergency departments experience many security problems. People who are under stress, either as a patient or as the family member of a patient in a life-threatening situation, can be extremely demanding—so much so that hospital staff may require security resources to get their job done. Often understaffed due to budget cuts and overflowing with patients who use the emergency department as a "walk-in clinic," emergency departments must deal with people who yell and get irate because they are not being attended to as quickly as they think they should be.[8]
- With cuts in social assistance, more people are coming in with more social problems. "You get a lot of street people, a lot of psychiatric patients and drunks."[9]
- The implementation of managed care systems (including health maintenance organizations) has health care professionals frustrated with the frantic pace they must keep, which they blame on the change toward managed care coverage.[10] Jobs are being cut, and people are nervous about losing their jobs.
- Hospitals are introducing computer-controlled drug vending machines, like the Pyxis Med Station System 2000. One hospital reported that the new system jammed two times in one hectic weekend, making the drug supply unavailable.[11]
- Hospitals that provide acute care and operate at bed occupancy levels of 90 percent or more face regular bed crises, which place patients at risk.[12]
- It is recommended that medical equipment or utility system components that are deemed "critical to patient safety" have emergency procedures including backup systems in the event of malfunction or failure. "Critical to patient safety" means that the equipment or component includes life-supporting, life-sustaining, or other critical equipment whose malfunction would result in an "adverse patient outcome."[13]
- Hospitals are deciding how to best provide quick access to data and furnish referring physicians with relevant data while also maintaining patient privacy. Some hospitals use a computer program that provides access to information electronically from any Web browser on the hospital's computer network.[14]

ISBN: 0-536-91271-8

- Certain types of protective clothing are more effective at filtering infectious agents and, therefore, can help health care workers reduce exposure to several pathogens that are borne in blood and body fluids.[15]
- A California-based health care association estimates that 1500 of the 2700 hospital buildings in the state could collapse during a serious earthquake.[16]

TARGET ENVIRONMENT: AIRPORT

Airport (Figure 9–2) security is increasingly a feature of national and international news. As the airline industry expands, as people increasingly travel for business and pleasure to all parts of the globe, the industry is forced to confront some new challenges. Aviation disasters create disturbances for the industry and the traveling public. Within the next decade, the number of annual U.S. aircraft passengers is expected to be 1 billion.[17] Threats of terrorism result in increased security efforts, which can lead to flight delays and unhappy passengers. The causes of some aviation disasters may never be determined. After four years of investigation and recovery of more than 95 percent of the wreckage, the cause of the crash of TWA flight 800 is not known.[18] The federal government's response to this tragic crash included the implementation of heightened security measures at all airports and the creation of a White House

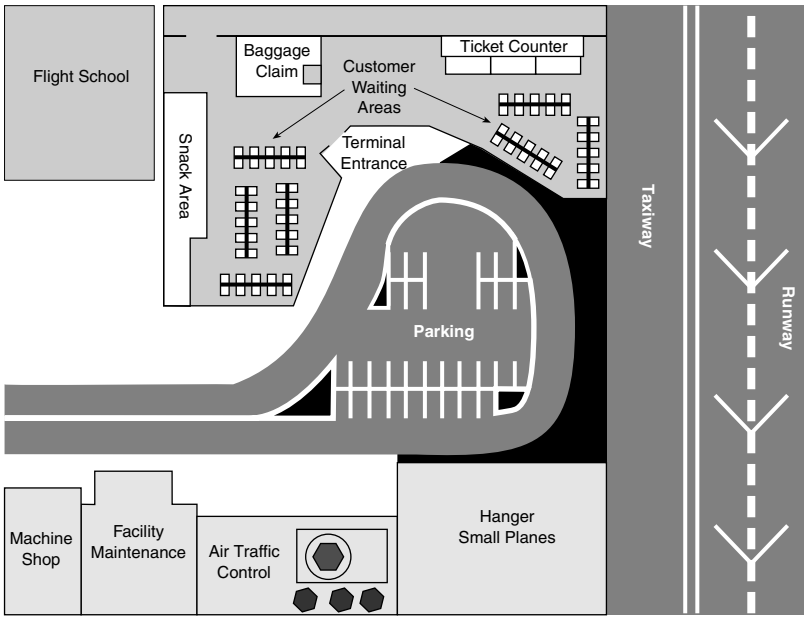

FIGURE 9–2 Sample Target Environment: Airport

ISBN: 0-536-91271-8

Commission on Aviation Safety and Security. Reducing unknown risks in air travel comes with direct tradeoffs. "Each measure to improve safety and security can have an impact on the direct costs to travelers, delays, convenience, civil liberties, fatalities, and taxpayer costs."[19] Consider the following issues being discussed in the aviation industry:

Considerations Identified Prior to 9/11

- In 1998, the National Transportation Safety Board received 2210 reports of commuter and private aircraft accidents within the United States, and these accidents resulted in 641 fatalities.[20]
- Thieves in airports are targeting laptop computer owners. By employing distraction techniques, the thieves are making away with the computers.[21]
- Enhanced security precautions allowing only ticketed passengers into gate areas do not permit entry for persons traveling with the new electronic ticket, or e-ticket.
- An airport in southwest Florida has been using a dog to scare away birds; collisions between birds and jets last year cost the U.S. civil aviation industry an estimated $300 million in damages.[22]
- In August 1999, a sting operation at Miami International Airport highlighted security concerns about airport employees. The relaxed nature of checks on prospective employees has been a real problem.[23]
- Strikes or sickouts by air traffic controllers, flight attendants, and pilots have disrupted airline services to passengers.
- Airport security managers can implement a new technology, called threat image projection, to test the alertness of the security screeners. The technology projects a simulated threat into an actual bag, for example.[24] The system projects simulated objects, such as a handgun, into a bag as it moves through the X-ray machine to see if guards make the observation.
- The Coalition for Airport and Airplane Passenger Safety (a group of labor unions representing firefighters, airline pilots, flight attendants, and workers in a number of airline trades) prepared a report titled "Surviving the Crash: The Need to Improve Lifesaving Measures at Our Nation's Airports."[25] The report suggests that passengers and workers at U.S. airports are not adequately protected from a variety of life-threatening conditions.[26] (The Federal Aviation Administration [FAA] disagrees with the findings presented in this report.)
- Outdated FAA regulations are to blame for firefighter and rescue units not being properly staffed, equipped, or trained to respond to crashes and other emergencies. In addition to being unprepared for aviation disasters, airports are woefully unprepared to address terrorism threats, accidents involving hazardous materials, medical emergencies, and problems that

ISBN: 0-536-91271-8

might result from such a heavy concentration of passengers in the airline terminals.[27] (The FAA disagrees with the findings in this report.)

- Traveler fatigue and frustration are becoming increasingly evident, with high-profile incidents resulting in the need for security intervention.[28]
- There is concern about the state of explosive detection technologies, their lack of reliability, the frequency of false alarms, and the delays in processing passenger baggage. The FAA has certified only one explosives detection machine (the CTX 5000) for checked baggage screening. The certified machine has an actual "throughput rate" that is much less than the designed rate of 500 bags per hour; thus, two units are necessary to meet the FAA's throughput requirement. Even with two machines, there is significant potential for operator error. It seems likely, for example, that in the press of rush hour, operators will start ignoring "positives" to reduce the ire of busy travelers. Estimates are that it would cost $2.2 billion to put these detection machines in the 75 busiest airports in the United States.[29]
- Proposed programs to match passengers with bags by checking claim tickets, for example, could add an estimated $2 billion annually, compounded by the need to find additional personnel and additional time to implement the programs.[30]
- The Computer-Assisted Passenger Screening program, developed by Northwest Airlines, is being used in over 240 cities to screen passengers in an effort to prevent terrorism. Customer information is matched against undisclosed criteria to determine whether the passenger's luggage should be subjected to additional screenings. The passengers are not informed that the additional screening is taking place.[31]
- Surface capacity at airports is increasing, and existing ground control efforts are argued to be insufficient to prevent collisions on the ground.[32]
- In bad weather, both pilots and air traffic controllers require critical information on airport conditions and relevant traffic.[33]
- Personal identification and verification of airport personnel is essential.
- Most airports deal with cargo and freight transport as well as passenger transport, although this usually happens in a different section of the airport.
- Investigators from the FAA conducted a battery of 170 tests at eight U.S. airports. They gained access to restricted areas in 117 cases. Of particular interest is the fact that once they had entered secure areas, they were able to board aircraft operated by 35 different aircraft carriers. Violations that allowed access to restricted areas included an absence of personnel assigned to the task or lack of awareness and willingness to enforce the existing procedures.[34]

ISBN: 0-536-91271-8

- Questions have been raised about the role of vendors and other airport tenants (fast food vendors, newsstands, mall shops, etc.) in meeting security objectives.[35]

Considerations After 9/11

- There are additional security checks of carry-on luggage.
- Vehicle check points are in place at many large airports.
- Increased numbers of Federal Air Marshals are on board commercial aircraft.
- There is strong support for pilots to carry guns in the cockpits on a voluntary basis.
- Armed National Guard officers are posted throughout airports to increase security.
- Some security experts say that an invisible wall of security, like that set up in casinos, could help alleviate anxiety and inconvenience. This would mean relying heavily on surveillance cameras and undercover security officers. The possibility of profiling is expected to increase.
- The Transportation Security Administration (TSA), which oversees airport security, recently conducted tests and found that privately contracted screeners missed fake weapons smuggled by undercover agents in a quarter of the trials.
- The TSA has deployed federal screeners to 82 airports.
- The TSA has announced 145 Federal Security Directors, who are responsible for 380 airports.
- The TSA is accepting applications for positions in 420 airports and has received over 1.1 million applications to fill some 52,000–54,000 federal passenger and baggage screener positions.
- The Aviation and Transportation Security Act mandates that a sampling of all checked luggage must be scanned for explosives after December 31, 2002.

SCHOOL SECURITY

Incidents of school violence (Figure 9–3) have been prominent in the media in the last 5 to 10 years. Technological devices for enhancing security are becoming fixtures in schools across the country. The most likely products used by school security professionals include emergency communications devices, badging systems, access control and alarm systems, closed-captioned television (CCTV) systems, and metal detection or X-ray screening.[36–38] Judging by the incidents reported in the last decade, students could be facing various threats that might require expanded emergency response plans. If evacuation is or-

ISBN: 0-536-91271-8

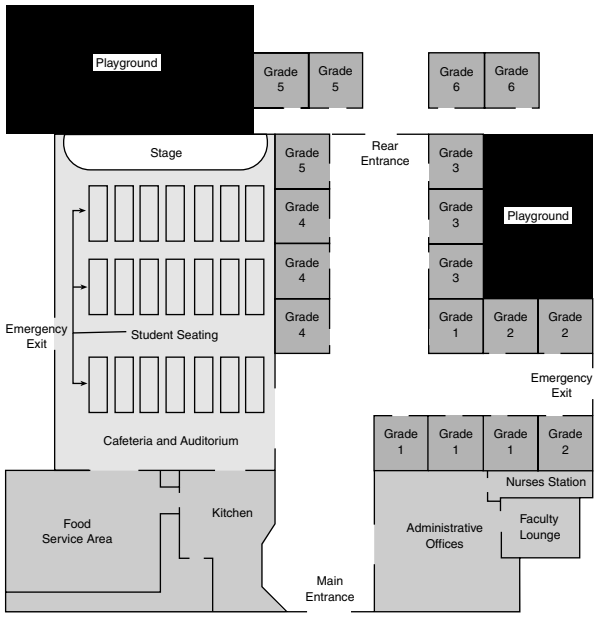

FIGURE 9–3 Sample Target Environment: School

dered, it is possible that students could be sent into the line of fire if snipers wait outside the school. On the other hand, if a classroom lockdown is ordered in an attempt to isolate students from attackers but the attackers used explosive devices, students, faculty, and other staff may become victims. School security professionals (such as Curtis Lavarello, executive director of the National Association of School Resource Officers) argue that much of the concern about security in schools is directly linked to access to guns. While many people are concerned about what they identify as an increase in violent crime in schools, experts are constantly reminding people that "schools are still among the safest places for children."[39,40] Some school officials argue that what is done in schools to provide a safe learning environment will not ever be the same after the Columbine High School shootings in Littleton, Colorado.[41] Consider the following information about school crimes and crime prevention efforts:

- Safe School Crime Stoppers set up an anonymous hotline for parents and students to call and report suspicious or unlawful behavior.[42]
- Most of the alleged killers in recent school shootings actually told other people about their plans before they acted.[43]
- Violence occurs at greater levels in schools where minor infractions of school policy are ignored.[44]

ISBN: 0-536-91271-8

- School resource officers are used for security but go beyond the traditional role of security guard to developing relationships with students as a proactive measure to prevent crimes.[45]
- Schools can enhance physical safety by taking the following steps:
  1. supervising access to buildings and grounds
  2. reducing class size and school size
  3. adjusting scheduling to minimize students' time in hallways or in potentially dangerous locations
  4. conducting a building safety audit
  5. arranging supervision at critical times
  6. having adults visibly present throughout the school facility
  7. staggering dismissal times and lunch periods
  8. monitoring the school grounds
  9. coordinating with local police to ensure that there are safe routes for students going to and from school[46]
- Creating a positive school environment by increasing positive encounters in the classroom and school community is proving to be one of the most effective ways to address potentially violent or disruptive behavior. Clear expectations, consistent treatment, and just actions can go a long way in addressing classroom fears.[47]
- Although windows are also vulnerable, doors are the usual access point for intruders in schools. Choosing the right locks for entryways can be critical.[48]
- Each year, on average, 9 children die in school bus crashes; another 26 die when hit by either the bus or a passing car.[49]
- "Peer mediation" is being added to school programs to help students resolve conflict.[50,51]
- Some school programs are rejecting metal detectors and bomb-sniffing dogs in favor of programs focused on prevention and early detection. One example is the Principal's Student Leadership Group, in which kids who are selected to help monitor incidents.[52]
- Signs that a student is troubled include excessive feelings of rejection, expression of violence in writings and drawings, and overt threats.[53] Other warning signs are a history of drug abuse, talk about suicide, a lack of coping skills, a precipitating event, and no apparent emotional support system.[54] Schools must have a plan in place to help these students when warning signs are displayed.
- One of the most troubling trends in schools is the increasing incidence of bomb threats.[55]
- Arson, theft, and vandalism can be recurring problems for any school.
- A "war on drugs" is being waged in the nation's public schools.[56]

ISBN: 0-536-91271-8

- Requiring students to wear uniforms is argued to reduce "acting out" behaviors.[57]

BANK SECURITY

Clearly, banks (Figure 9–4) are one of the most notorious targets for theft. These days, however, in addition to their traditional banking services, banks have added automated teller machines (ATMs) and are expanding to include banking services online. Banks are increasingly layering access control throughout their facilities rather than just having perimeter security.[58] Furthermore, various techniques are argued to be excellent weapons against counterfeit checks. These techniques include transaction reports, fingerprint signatures, a training and award program for bank personnel, and the issuance of security alerts. Consider the information in the following lists.

Banks in General

- The greatest financial losses to banks result from external check fraud and internal embezzlement.[59]
- The prime time for bank robberies is from 10 A.M. to 3 P.M. with Friday being the day of choice.[60]
- One type of secure entry that is being explored in various banks is a series of double-locking, bullet-resistant doors. A customer comes in

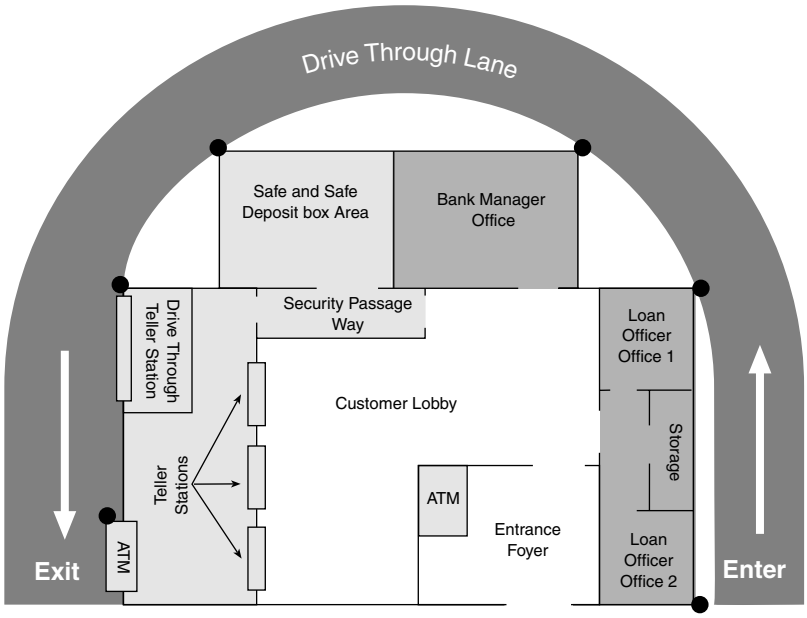

FIGURE 9–4 Sample Target Environment: Bank

ISBN: 0-536-91271-8

through one door and must go through selected security devices (e.g., CCTV, metal detector) before proceeding through a second entry door. As the exterior (or first) door locks, the interior (or second) door unlocks so the person may proceed through. The system resets itself when the interior door is shut.[61] These systems are more common in European and South American banks and, at $40,000–$50,000, are quite expensive.[62,63]

- Today, sophisticated computer programs allow criminals to create corporate payroll checks that are nearly indistinguishable from the real thing.[64]
- One type of fraud that appears in banking institutions is the use of a legitimate customer's information by an illegitimate user. The legitimate customer's full name, address, Social Security number, and account information is used by the perpetrator, who then acquires a fake ID and comes to the bank claiming to be that customer. In one bank, this happened three times in a year, to the tune of just over $50,000 in losses for the bank.[65]
- Although the number of bank robberies is down, according to the Federal Bureau of Investigation (FBI), the number of incidents involving a weapon and the number of cases that involve violence are up.[66]
- Some of the best information about robbery prevention comes from analysis of the robberies that have happened across a chain of banks over time. This allows the banking institution to zero in on vulnerabilities.[67]
- Title 12 of the U.S. Code, also known as the Bank Protection Act of 1968, outlines minimum standards for the installation, operation, and maintenance of security devices and procedures at financial institutions.[68] It requires all federally insured banks, savings and loan institutions, and credit unions to designate a security officer, cooperate with and seek advice from the FBI and other law enforcement agencies, develop comprehensive security programs and implement protective measures to meet (or exceed) federal standards, keep "bait money" (or money for which numbers have been recorded), periodically remove excess cash from the tellers' windows and bank premises, and finally, develop stringent opening and closing procedures.[69]
- Security cameras installed at a six-foot height can easily be covered over with spray paint or disabled during a robbery.
- Computerized signature and photo records are a much more effective means by which to verify signatures than the signature cards that have traditionally been used.[70]
- Poor-quality security cameras can result in a picture whose resolution is so bad that the picture taken is useless.
- The open design of banks often leaves tellers accessible and overexposed.[71]

ISBN: 0-536-91271-8

- Client information is as important as the money clients deposit. If clients do not believe the bank will keep their information confidential, they might take their money somewhere else.[72]
- The theft of data (e.g., customer accounts, customer profiles, credit records, loan records) has compelled many banks to invest in access control systems.[73]
- Banks are reported to be interested in security systems that are convenient, able to be networked throughout their entire system of bank branches, sophisticated, and integrated.[74]
- Financial institutions want access control databases that can automatically communicate with all other databases so that information can be exchanged almost instantaneously.[75]
- Bank management wants access control features that are integrated with other features (like CCTV and ID badging systems) to provide, for example, visual confirmation in addition to the access record kept by the access control system.[76]
- Online services are said to "save you hours of standing in lines, punching a calculator, and juggling paperwork." An increasing number of banks now offer custom Web sites that let people pay bills and download bank and credit card statements. Even better, the sites help people research mortgage refinancing, find the best credit cards, and analyze their investments.[77]
- In 1998, approximately 1200 banks contracted for Web-based banking designs. In 1999, over 7200 were estimated, with more projected to come in the following years.[78]

ATMs

- In 1992, there were 70 ATM burglaries and attempted burglaries. By 1997, there were an estimated 200.[79]
- With the growing need for convenient access to cash, ATMs are more common and less fortified. In 1985, there were approximately 44,000 ATMs; in 1997, that number had increased to approximately 165,000.[80]
- ATMs hold anywhere from $15,000 to $250,000 depending on the size of the machine.[81]
- Satellite tracking systems are being used in ATMs as a means of retrieving the equipment if it is taken.[82]
- Various ATMs in the United States and abroad are testing the use of iris scan technology. A photo of the iris is taken and then converted into a computer pattern. The pattern is compared to data on file. The process takes about two seconds.[83]
- Fraudulent use of ATM cards costs banks up to $150 million a year.[84]

ISBN: 0-536-91271-8

- Bank cards with magnetic tape are being replaced by "smart cards" that store cardholder data. Smart cards are said to be infinitely more durable and secure.[85] From the moment smart cards appeared on the marketplace, hackers have been trying to crack the code.[86,87]
- Lighting is seen as an integral security feature for ATMs, but there are no national guidelines about this lighting. In some places (e.g., New York City) a city ordinance dictates the lighting standards required for ATMs.[88]

CONVENIENCE STORE SECURITY

When looking at information about the incidence of robbery at convenience stores (Figure 9–5), readers must be discerning. For example, a 1991 report put out by the National Association of Convenience Stores (NACS) said that during the 10-year period from 1976 to 1986 the number of convenience stores doubled while the number of convenience store robberies remained relatively constant, suggesting that the robbery rate per store was cut in half over that 10-year period, due in large part to the implementation of several deterrence measures.[89] These measures include (1) cash control techniques, (2) clear sight lines in the stores, (3) prominent position of the cash register, (4) lack of

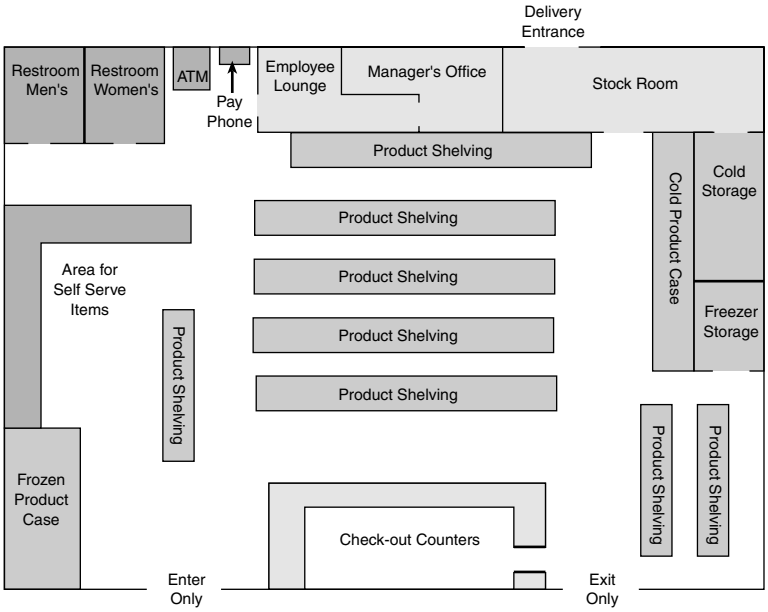

FIGURE 9–5 Sample Target Environment: Convenience Store

ISBN: 0-536-91271-8

escape routes, (5) balanced exterior and interior lighting on the premises, and (6) employee training programs. Furthermore, the industry study took issue with FBI data reported in 1990.[90] It may not be surprising that the industry projected numbers that were lower than the FBI's. In 1989, the NACS study projected 23,311 convenience store robberies compared with the FBI report of 36,435.[91] For 1990, the NACS findings suggest 22,935 compared to the FBI-reported 38,435 convenience store robberies.[92]

In 1992, Ron Hunter and C. Ray Jeffery outlined in their research that the preventive measures endorsed by the greatest number of studies include (1) having two or more clerks on duty, especially at night (a form of employee surveillance); (2) cash handling techniques; (3) access control features; and (4) natural surveillance.[93] Hunter and Jeffery highlight elements of the Sessions report (the FBI data) suggesting that between 1985 and 1989 robbery in convenience stores increased 28 percent, representing the most rapid growth within all categories of robbery during that period.[94] While the NACS study suggests crime rates were "cut in half," the Hunter and Jeffery article suggests the "dramatic increase in convenience store robberies is of major concern to public officials and the convenience store industry."[95]

The industry also disagrees with the FBI regarding the dollars lost at these robberies. According to the NACS survey, register robbery in 1989 averaged $173, compared to the FBI's average of $364. As mentioned briefly in Chapter 8, the losses from theft are minimal when compared to the loss of business from customers, who are afraid to shop in the stores; the loss of qualified employees, who are afraid to work there; and successful litigation by individuals who have been harmed because of convenience store robberies.[96]

In one of the earliest studies of convenience store robberies (1975), Crow and Bull found that the "results support the concept that robbers select their targets and that physical and behavioral changes at the site can significantly reduce robberies."[97] Consider some of the following points of interest:

- The peak robbery period for convenience stores is between 9:00 P.M. and 11:00 P.M. That same study found that nearly 35 percent of robberies in Florida occurred between 11 P.M. and 6 A.M.[98]
- Approximately 94 percent of all convenience store robberies had only one victim. The robbery success rate does not increase as the number of victims increases.[99]
- Crime prevention strategies supported by the NACS include the use of signs indicating that the clerks have access to only limited funds, good cash handling procedures, enhanced visibility inside and outside the stores, alteration of escape routes, use of security devices, encouraging activity in or near the store, employee alertness, and store cleanliness.[100] NACS argues that if these recommended practices are followed, it will be

ISBN: 0-536-91271-8

unnecessary to have multiple clerks on duty, use security enclosures, and limit store hours (close stores at midnight).[101]

- Florida has some of the most stringent mandated prevention strategies in the nation. The prevention techniques recommended by the Florida Department of Legal Affairs include silent robbery alarms, security cameras capable of identifying robbery suspects, drop safes or other cash management devices, well-lighted parking areas, posted signs indicating that there is less than $50 cash on hand, clear and unobstructed windows, height markers at entrances, no concealed access or escape areas, cash handling policies to limit available cash at any given time, employees trained in robbery deterrence and safety, and two clerks on night shifts.[102]
- Handguns were used in 71 percent of the reported homicide cases in convenience stores.[103] Sixty-five percent of the homicides involved no resistance or provocation from the clerk and were therefore labeled as "random/senseless" violence.[104]
- Two-thirds of the reported rapes in convenience stores were unrelated to a robbery.[105] Eighty-nine percent of the rapes reported occurred at night.[106]
- No conclusive findings could be reached about the effectiveness of bullet-resistant barriers in convenience stores.[107]
- Gasoline driveoffs accounted for 48 percent of all police calls from convenience stores.[108]

REFERENCES

1. M. Hagland, "Confidence and Confidentiality," *Health Management Technology 18,* no. 12 (1997): 20–25.
2. S. Pelton, "Authentication Captures Security of Hardware, Convenience of Software," *Health Management Technology 20,* no. 10 (1999): 50.
3. T. Eskreis Nelson, "Safeguarding Newborns: Managing the Risk," *RN 62,* no. 3 (1999): 67–70.
4. Eskreis Nelson, "Safeguarding Newborns."
5. C. Leliopoulou, H. Waterman, and S. Chakrabarty, "Nurses' Failure To Appreciate the Risks of Infection Due to Needle Stick Accidents: A Hospital-Based Survey," *Journal of Hospital Infection,* May 1999, vol. 42, no. 1, 53–59.
6. R. L. Calvin, "Evaluation of the Protective Value of Hospital Gowns against Blood Strikethrough and Methicillin-Resistant Staphylococcus Aureus Penetration," *Association of Operating Room Nurses Journal 69,* no. 6 (1999): 1264.

ISBN: 0-536-91271-8

7. C. Leliopoulou et al., "Nurses' Failure."
8. M. McDonald, "Overstretched in Emergency: On Both Sides of the Border, Hospital ERs Feel the Pinch," *Maclean's 109,* no. 49 (1996): 74(4).
9. McDonald, "Overstretched in Emergency."
10. McDonald, "Overstretched in Emergency."
11. McDonald, "Overstretched in Emergency."
12. A. Bagust, "Dynamics of Bed Use in Accommodating Emergency Admissions: Stochastic Simulation Model," *British Medical Journal 319,* no. 7203 (1996): 155.
13. G. Mills, "Issues in Health Care Construction," *Heating, Piping, Air Conditioning 70,* no. 7 (1998): 28(4).
14. Pelton, "Authentication Captures Security of Hardware, Convenience of Software," 50.
15. Calvin, "Evaluation of the Protective Value of Hospital Gowns," 1264.
16. C. Vanchieri, "Badly Braced for the Big One," *Hospitals and Health Networks 72,* no. 20 (1999): 42.
17. M. Lease and T. Burke, "Law Enforcement's Response to Small Aircraft Accidents," *FBI Law Enforcement Bulletin,* February 2000, 14.
18. R. W. Hahn, "The Cost of Airport Security Measures," *Consumer's Research Magazine 80,* no. 7 (1997): 15(5).
19. Hahn, "The Cost of Airport Security Measures."
20. National Transportation Safety Board, "1998 Aviation Accidents," *http://www.ntsb.gov/aviation/9801.htm*, accessed February 2000.
21. "Laptop Theft: A Variation on an Old Trick," *Maclean's 109,* no. 20 (1996): 17.
22. "Feather Buster: A Florida Airport Unleashes a Weapon in Its Battle against Birds: Border Collie Jet," *People Weekly 52,* no. 7 (1999): 85.
23. J. Dettmer, "FBI Has Grounded Airport Security," *Insight on the News 15,* no. 35 (1999): 48.
24. M. Lavitt, "New Technology Tests Alertness of Airport Security Screeners," *Aviation Week and Space Technology 150,* no. 13 (1999): 88(2).
25. M. Bradford, "U.S. Airport Safety Criticized," *Business Insurance* 3 (1999): 1.
26. Bradford, "U.S. Airport Safety Criticized," 1.
27. Bradford, "U.S. Airport Safety Criticized," 1.
28. "Diana Ross Released and Given Warning," *Jet,* vol. 96, no. 19, p. 54.
29. Hahn, "The Cost of Airport Security Measures."
30. Hahn, "The Cost of Airport Security Measures."
31. P. G. Chronis, "Airlines Have New Security 'Screen': Secret System Raises Discrimination Questions," *Denver Post,* 1 January 1998, B-01.
32. S. Young et al., "Safely Improving Airport Surface Capacity," *Aerospace America 36,* no. 5 (1999): 22.

ISBN: 0-536-91271-8

33. Young et al., "Safely Improving Airport Surface Capacity," 22.
34. T. Anderson, "Airport Security Fails Tests," *Security Management,* February 2000, 73–74.
35. Anderson, "Airport Security Fails Tests," 74.
36. M. Fickes, "The AVS's of Security Technology," *American School & University 71,* no. 11 (1999): SS21 (4).
37. M. Kennedy, "The Changing Face of School Violence," *American School & University 71,* no. 11 (1999): *ss*6(3).
38. Kennedy, "The Changing Face of School Violence."
39. J. Agron, "Lessons Learned," *American School & University 71,* no. 11.
40. Kennedy, "The Changing Face of School Violence."
41. Agron, "Lessons Learned."
42. Agron, "Lessons Learned."
43. M. Simpson, "Taking Threats Seriously," *NEA Today 17,* no. 1 (1998): 27.
44. M. Dunn, "Critical Elements in School Security," *American School & University 71,* no. 11 (1999).
45. C. Mulqueen, "School Resource Officers More Than Security Guards," *American School & University 71,* no. 11 (1999): p. 17(1).
46. Dunn, "Critical Elements in School Security."
47. J. N. Lederhouse, "You Will Be Safe Here: Realizing a Positive School Climate," *Educational Leadership 56,* no. 1 (1998): 51(4).
48. J. D. King, "Locking in on Safety," *American School & University 70,* no. 2 (1997): 36.
49. A. Spake, "Tussling over Buses," *U.S. News & World Report 127,* no. 13 (1999): 62.
50. P. Welsh, "The Price of Protection," *U.S. News & World Report 126,* no. 17 (1999): 28.
51. "NEA Affiliates at Work for Safety," *NEA Today 18,* no. 1 (1999): 14.
52. D. Goodgame, "7:10am School Security: Always on the Lookout for Signs of Trouble," *Time 154,* no. 17 (1999): 74+.
53. D. Marcus, "Metal Detectors Alone Can't Guarantee Safety," *U.S. News & World Report 126,* no. 17 (1999): 26.
54. S. Band, "School Violence: Lessons Learned." *FBI Law Enforcement Bulletin 68,* no. 9 (1999): 9.
55. J. Agron, "Safe Havens: Preventing Violence and Crime in Schools," *American School & University 71,* no. 6, (1999): 18(5).
56. B. Dority, "Big Brother Goes to High School," *Humanist 57,* no. 2 (1997): 37(2).
57. M. Gips, "Securing the Schoolyard," *Security Management,* March 1996, 47–53.
58. J. Kirch, "Investing in Better Controls," *Security Management,* May 1999, 83.

ISBN: 0-536-91271-8

59. R. E. Anderson, "Bank Security," in *Handbook of Loss Prevention and Crime Prevention,* ed. L. Fennely (Woburn, MA: Butterworth-Heinemann, 1982).
60. P. Carroll, "The Chicago Bank Robbery Initiative," *FBI Law Enforcement Bulletin 66,* no. 4 (1997): 9–15.
61. J. Konicek and K. Little, *Security, ID Systems and Locks: The Book on Electronic Access Control* (Newton, MA: Butterworth-Heinemann, 1997), 76.
62. Konicek and Little, *Security, ID Systems and Locks,* 76.
63. T. Mann, "Policies That Pay Off: Although Robberies Are Down, They Are Becoming More Costly and Violent," *Security Management,* February 2000, 42–46.
64. K. Null, "One Bank's Fraud Fight: Security Doesn't Have To Sit by Helplessly in the Fight against Financial Services Fraud," *Security Management,* February 2000, 37–41.
65. K. Null, "One Bank's Fraud Fight," 38.
66. T. Mann, "Policies That Pay Off," 45.
67. Mann, "Policies That Pay Off," 45.
68. Anderson, "Bank Security," 740.
69. K. Hess and H. Wrobleski. *Introduction to Private Security* (Minneapolis, MN: West Publishing Company, 1996), 526.
70. R. Bordes, "Security Measures That Earn Interest," *Security Management,* June 1994, 71–72.
71. Bordes, "Security Measures," 71–72.
72. J. Kirch, "Investing in Better Controls," *Security Management,* May 1999, 82–88.
73. Kirch, "Investing in Better Controls," 84.
74. Kirch, "Investing in Better Controls," 85.
75. Kirch, "Investing in Better Controls," 84.
76. Kirch, "Investing in Better Controls," 84.
77. M. Hogan, "Easy Money Meets the Web," *PC/Computing 10,* no. 10 (1997): 129.
78. B. Orr, "A Service Bureau for Next Generation E-banking," *ABA Banking Journal 91,* no. 4 (1999): 68.
79. Gannett News Service, "ATMs Proving Convenient to Robbers as Well as Users," *St. Cloud Times,* 6c.
80. Gannett News Service, "ATMs Proving Convenient," 6c.
81. Gannett News Service, "ATMs Proving Convenient," 6c.
82. Gannett News Service, "ATMs Proving Convenient," 6c.
83. P. Davidson, "ATMs That ID Consumers by Eye To Get Test." *USA Today,* March 18, 1998, p. A1.

ISBN: 0-536-91271-8

84. Davidson, "ATMs That ID Consumers," A1.
85. J. Kutler, "Even Abundant Security Features Don't Spur Smart Card Buy-In," *American Banker 163,* no. 221 (1988): 1–3.
86. Kutler, "Even Abundant Security Features," 1–3.
87. P. Wayner, "Code Breaker Cracks Smart Cards' Digital Safe," *New York Times,* 22 June, 1998, D1.
88. R. Goetzke, "Shedding New Light on ATM Security," *Security Management,* September 1994, 57–60.
89. National Association of Convenience Stores, *Convenience Store Security: Report and Recommendations* (Alexandria, VA: 1991), 4.
90. W. B. Sessions, *Crime in the United States: 1989 Annual Report* (Washington, DC: Federal Bureau of Investigation), 1990.
91. National Association of Convenience Stores, *Convenience Store Security,* 13.
92. National Association of Convenience Stores, *Convenience Store Security,* 13.
93. R. Clarke, ed., *Situational Crime Prevention: Successful Case Studies* (New York: Harrow and Heston, 1992), 195.
94. W. B. Sessions, *Crime in the United States: 1989 Annual Report* (Washington, DC: Federal Bureau of Investigation, 1990), 21.
95. Hunter and Jeffrey, "Preventing Convenience Store Robbery Through Environmental Design," in *Situational Crime Prevention: Successful Case Studies,* ed. R. Clarke. (Albany, NY: Harrow and Heston, 1992).
96. Clarke, *Situational Crime Prevention,* 195.
97. Crow and Bull, *Robbery Deterence: An Applied Behavioral Science Demonstration—Final Report* (La Jolla, CA: Western Behavioral Sciences Institute, 1975), ii.
98. R. Degner et al., *Food Store Robberies in Florida: Detailed Crime Statistics* (Gainesville, FL: Florida Agricultural Market Research Center, 1983), 26, 27.
99. Degner et al., *Food Store Robberies in Florida,* 18–19.
100. Clarke, *Situational Crime Prevention,* 204.
101. Clarke, *Situational Crime Prevention,* 204.
102. R. Butterworth, *Study of Safety and Security Requirements for "At-Risk Businesses"* (Tallahassee, FL: Florida Department of Legal Affairs, 1991).
103. National Association of Convenience Stores, *Convenience Store Security,* 17.
104. National Association of Convenience Stores, *Convenience Store Security,* 17.
105. National Association of Convenience Stores, *Convenience Store Security,* 17.

ISBN: 0-536-91271-8

106. National Association of Convenience Stores, *Convenience Store Security,* 17.
107. National Association of Convenience Stores, *Convenience Store Security,* 22.
108. N. LaVigne, "Gasoline Drive-Offs: Designing a Less Convenient Environment," in *Crime Prevention Studies,* Vol. II, ed. R. Clarke (Monsey, NY: Criminal Justice Press, 1994), 91–114.

ISBN: 0-536-91271-8