CHAPTER 9

Deterring and Mitigating Attack

> The supreme art of war is to subdue the enemy without fighting.
>
> **—Sun Tzu**

INTRODUCTION

The goal of soft target hardening is simple: Deter any would-be attackers through the presence of a secure facility and if they breach your access points or strike from inside, engage with the ability to mitigate the attack and save the lives of your staff and occupants. As discussed in Chapter 2, hardening begins with you: the acceptance the threat exists and your operation and facilities are vulnerable. You likely have taken on some amount of risk by not being able to expend the resources to protect the operation fully, whether due to insufficient resources, lack of support from your leadership, or for business-related reasons. However, there is a spectrum of hardening actions you can take from nothing to everything, from inexpensive to exorbitantly expensive. The key is to understand the desired effect and plan to use your resources in the best possible manner to lower your risk.

DHS's "Soft Targets Awareness Course" (DHS 2008) is a great place to start grasping the overview of the threat and your vulnerabilities. The four-hour curriculum provides facility managers, supervisors, and security and safety personnel with baseline terrorism awareness, prevention, and protection information. The course enhances individual and organizational security awareness and participants gain insight as to why it is important to engage in proactive security measures and define their roles in deterring and detecting terrorist activity, and defending their facilities from it. The class is held all over the country and administered by qualified contractors.

Although your security plan should be an all-hazards approach, meaning that it is suitable no matter the emergency situation, you should focus on preparedness, rather than the specific kinds of weapons or tactics the

bad actor may bring to your facility. With this in mind, you should first assess your vulnerabilities. Prior to creating or improving upon your security plan, complete the FBI's Vulnerability Assessment in Appendix C. Note that this document must be safeguarded because it spells out all of your vulnerabilities. If the total score for the organization exceeds 256, and if local law enforcement has not been involved in the assessment, notify them at once. Hand carry the document, do not email or send through a postal service. After you identify and think through your vulnerabilities, you can create a plan to reduce risk in your operation. Trust me when I say, as the officer who was responsible for the security of Air Force One and the President of the United States while he transited our base at Andrews, you cannot have too much security when faced with an unknown threat and an actor who will engage on the day and in the manner of choosing.

EFFECTS-BASED HARDENING (EBH)

We simply cannot apply all resources toward all threats; a methodology is necessary to ensure actions and resources are directed in the most effective manner to cover your vulnerabilities against the threat and lower your risk. Prior to Operation Desert Storm, the Air Force's aerial campaign strategy was that of attrition—to bomb targets repeatedly and shoot down as many aircraft as possible until the enemy lost either the will or the firepower to fight. However, in order to prosecute the war against Iraq successfully, with restraint to spare civilians and not destroy the infrastructure of Baghdad, Air Force strategic thinkers devised a new approach: effects-based operations (EBO). An EBO approach is one where "operations against enemy systems are planned, executed, and assessed in order to achieve specific effects that contribute directly to desired military and political outcomes" (Carpenter 2004). EBO provides a strategy for the application of resources, phased in a particular way to achieve the desired cumulative effect. For instance, on the first night of the war, F-117A stealth aircraft (my unit) went into Baghdad and selectively destroyed communication towers and antiaircraft batteries. Later in the war, after the battlefield was "softened," targets shifted to military headquarters and enemy airfields.

EBO provides a good theoretical foundation for our efforts to harden soft targets, and for these purposes we call it EBH—effects-based hardening. This proposes a new (or improved) way of thinking and a specific process on both physical and psychological planes. Several axioms must be accepted prior to implementing this approach:

- Actions cause results.
- Inaction also causes results.
- Not seen does not mean not there.

- The goal is to remove the enemy from the fight before it starts.
- Actions are not universally applicable and must be tailored to your situation.
- The plan is fluid; you must constantly assess and adjust based on changes in the environment.
- The "fog of war" means you do not know everything about the threat; there are inescapable unknowables.
- You have no experience with the situation that might occur in your organization; nothing that happened in the past can prepare you.

EBH provides a system for visualizing violent scenarios that might happen to your organization in an unemotional, data-driven way. In order to identify the Achilles heel discussed in Chapter 8 and other vulnerabilities that increase your risk and susceptibility to attack, you have to "go there" and visualize and map out the worst possible scenario in your facility. At the least, consider an enraged outsider, a plotting insider, an active shooter, and a kidnapping and hostage situation.

The good news is that you are fighting this "battle" on your own territory. No one knows the vulnerabilities and strengths of your operation better than you; this puts you in the position of power over bad actors when it comes to deterring or mitigating their attacks. No matter how much preplanning or surveillance takes place, or even if you face an insider threat, you have the upper hand. Accordingly, keep certain details about your plan close, think of your employees' "need to know," and draw a diagram of concentric circles with the critical operations and people at the center and continue outward to the periphery, where you may have building custodial staff and volunteers. They need security and response training, but do not need to understand the security apparatus in place or your plan for protecting the facility and its occupants.

There is an art and science to security. The science part is physical: barricades at certain locations, walk-through metal detectors to keep out weapons, and security personnel stationed at entrance points for presence. The art is using your resources efficiently and effectively to achieve strategic security objectives. EBH can complement (or replace) your current efforts. Any new security processes should be incrementally phased in to shape the behavior of your people (and the enemy), perhaps in a time-phased manner or from most to least critical. However, security is not just a program; it must infiltrate everyday operations and decision making. By baking security into the organization and not just leaving it to the security guard at the front door, you tap the full spectrum of your assets: people, equipment, and building location. You may never know what types of terrorists or violent criminal acts you have thwarted using this methodology, but at the very least you will have a data-driven plan that effectively uses your resources to cover vulnerabilities.

Move forward *unapologetically* with your security plan. Leaders at soft target locations have confided to me their sense of regret about how efforts to tighten security inconvenience their staff and visitors. Those operating a for-profit operation are often concerned with customer satisfaction and whether measures will drive patrons away. I tell them to imagine, for a second, a horrendous attack at their facility. It could be an angry ex-spouse exacting revenge, a fired employee, a disturbed teenager, or a terrorist or group seeking to make the news and further their religious or political cause. As the leader or head of security, you must face the devastated family members and explain how you failed to protect their loved ones. Being a leader means taking responsibility, not only for the good things that happen at your place of work, but also for the bad, and the very, very bad.

EBH, by its very nature, encourages the harmonizing and synchronizing of actions. For example, during an active-shooter event, the front office has a plan: one predesignated person calls 9/11, one makes an announcement on the loudspeaker, and one locks and barricades the door. These types of actions take training and practice. Similar to pilots who are thrown impossible situations to handle in the flight simulator, if you practice for the worst possible scenario, small security issues will be handled effortlessly by the staff, working together as a team. They will also be confident of their ability to handle a large-scale emergency, and this confidence makes them force multipliers to you and your security team.

Matrixing your vulnerabilities, desired effects, the means to lessen your vulnerability, and the capabilities you have and need helps with the decision-making process. Figure 9.1 is an example of an EBH decision matrix for a church or school.

How do you know if your EBH efforts are working? You can test your system by having an outside security company do a red teaming exercise on your property, a tactic addressed later in the chapter. Also, you should ask the people who work in and use your facilities if they feel safe and if not, how you could do better. Not only will you glean valuable information, but the mere process of asking for and then acting on their ideas will strengthen your relationship and open the lines of communication about vulnerabilities.

The rest of the chapter is devoted to best practices and ideas harvested from industry experts—information to guide your EBH efforts.

PHYSICAL SECURITY

(Thank you to Brian Gallagher, former physical security specialist at the US Secret Service and owner of Security at Church (www.securityatchurch.com) for assistance with the following section.)

Prioritized Scenario	Desired Effect	Means	Capabilities and Cost	Implement/Partially Implement/ Table
1. Highly visible location on busy highway draws opportunists	Lower "heat"	Remove external signage facing road	In house, volunteers, free	Implement
2. Too many people with keys to the main door	Restrict building access	Install electronic key lock on main door and obtain keying equipment and cards	Contracted; $3,000	Partially implement; rekey current lock, reissue keys; budget electronic key system for summer 2015
3. Holding meetings after hours for outside groups, attendees wandering in building	Restrict access to the rest of the building	Install locking door between basement and upstairs offices	Contracted; $1,500 with labor	Implement

FIGURE 9.1 Effects-based hardening matrix.

We cannot easily interview terrorists or those who perpetrate violent crimes about deterrents to their activity; however, convicted thieves are accessible and give valuable insight. The chart in Figure 9.2 shows responses from 360 burglars regarding physical security measures that serve as the biggest deterrents to their activities.

Note the presence of people is the number one deterrent, followed by an officer nearby (which may be substituted at night by a preparked patrol car). Alarms are effective, as well as surveillance cameras, dogs, and steel bars on windows. The limited escape route is something to consider as well.

The exterior of your building, the grounds, and the parking lot are all critical to the security of your occupants. As previously discussed, lowering the profile of your building with less signage will deter opportunists from attacking your church or school. Physical hardening of your property could be as simple as installing a security fence or raising the height of current fencing to conceal your building and its occupants (such as children in a schoolyard) and to keep out intruders. Always check the perimeter fence for breaches or the stacking of wood or objects that could allow someone to climb over the fence. Industry experts recommend the following fence standard: seven feet high, with three strands of barbed wire, six inches apart. Shrubbery should be no higher than three feet, and set back one yard from buildings, and tree branches trimmed eight feet above the ground. Outdoor lighting not only illuminating

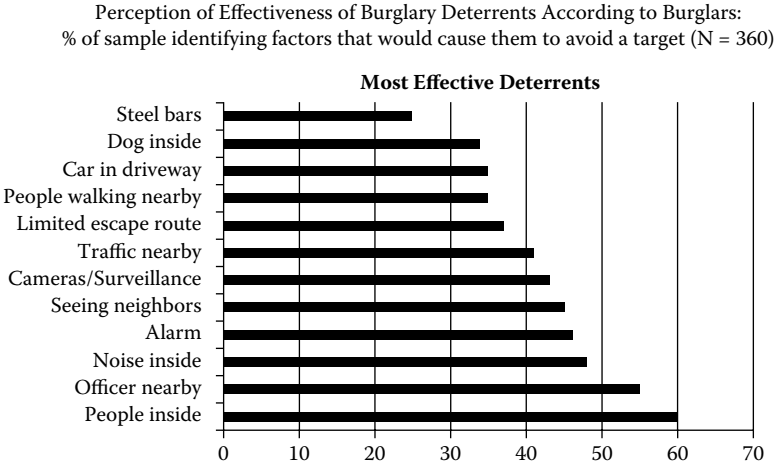

FIGURE 9.2 Most effective deterrents to burglary. (Kuhns, Kristie R., and Blevins, Joseph B. "Understanding Decisions to Burglarize from the Offender's Perspective." The University of North Carolina at Charlotte Department of Criminal Justice & Criminology. 2013. With permission.)

buildings, but also the surrounding property, is important to deter trespassers. Motion lights will keep your electricity bill lower and startle any would-be intruder. There are industry standards for external security lighting; see IESNA, ASNI and OSHA guidelines online.

Parking Lots

As illustrated in previous case studies, several international and domestic terrorists used parking lots to plant the primary bomb, stage a shooting, or place secondary devices aimed at injuring response personnel and evacuees. Therefore, you must secure your parking lot as an extension of your building. The preferable situation is to have the parking lot located inside the fence line, with a greeting area/entry point to control visitors. Churches are especially vulnerable to burglary, with service times posted outside on signage and a lot full of unattended vehicles for an hour or more. A roving parking lot security team provides an extra layer of protection.

Operations with large parking lots such as megachurches, large schools, malls, and sports and recreational venues might consider training for parking attendants called "First Observer" (http://www.parking.org/professional-development/first-observer-program.aspx). The program is jointly operated by the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) to train parking attendants to identify a potential threat. The program also educates the parking attendants with background information on terrorist groups, their tactics, and trends as well as an understanding of weapons. Training of this type turns a parking attendant into a force multiplier for your organization.

Pre-positioned Vehicle

Perhaps you could ask your local police department for a marked police cruiser to be placed at the entrance of your building. You could offer parking to an officer who could leave his or her personal vehicle at your facility and swap out with the cruiser when off duty. The marked vehicle serves as a visual deterrent for those who might be performing surveillance on the facility. If the marked cruiser is not possible, perhaps a member of your church, school, hospital, or organization will give up an old SUV or truck, which you can mark to look like a security vehicle from afar using fluorescent tape and other tools (Figure 9.3).

There are no data to prove the pre-positioning of law enforcement vehicles deters attack; however, anecdotal stories support the theory. For instance, there is reason to suggest that Sandy Hook Elementary School

FIGURE 9.3 SUV repurposed as a mock security vehicle at a compound in the Middle East.

shooter Adam Lanza's initial target was actually Newtown High School. According to a source familiar with the investigation, Lanza's car was identified on the school surveillance footage circling the school parking lot. The official believed Lanza saw two police cars parked in the lot and decided to move on (Lysiak 2013). The absence of such procedures has been used in several "negligent security" lawsuits; for instance, in 2007, a man was killed by a shooter with an AK-47 in a case of mistaken identity in a Waffle House parking lot in Pensacola, Florida, at 3:30 a.m. In the successful lawsuit filed by the family: "The plaintiff alleged that the restaurant was located in a high crime area. The plaintiff's security experts opined that the defendant was negligent in failing to have an armed, uniformed sheriff's officer on the premises with a marked police car which would have deterred the crime" (Rose, Vangura, and Levin 2009).

If your facility is hosting a special guest—one that has been advertised to the public and may be controversial or draw protest, or even a popular celebrity—know that a bull's-eye has just been painted on your facility. You should pre-position an escape vehicle near an emergency exit closest to the place where the person is addressing the crowd. A member of your staff or a trusted volunteer should be positioned at the vehicle as the driver in case of emergency.

Traffic Duty

Soft target facilities have predictable schedules: schools have drop off/pick up, church services start and end at the same time every week, sporting and recreational events have traffic issues at the beginning and end of events, and malls are typically their busiest on Friday and Saturday nights. Choke points outside your facility present a security hazard and you need to keep traffic moving. Mir Aimal Kansi, a Pakistani citizen residing in the United States with phony immigration papers and a forged green card, became enraged while watching CNN news coverage of US operations in Iraq and CIA involvement in Muslim countries. A courier, he often drove by the entrance to CIA headquarters, noting the two lanes of traffic waiting at the light to turn left onto the agency's ground. At 8:00 a.m. on January 25, 1993, Kansi drove his courier vehicle to that very spot, emerged from his vehicle with an AK-47 semiautomatic rifle, and walked up and down the lines of vehicles, firing a total of 10 rounds, killing two CIA employees, and injuring three others. Kansi escaped the country and was arrested by FBI agents in Pakistan in 1997; he was convicted and sentenced to death by lethal injection, which was accomplished in 2002. The military actively tries to avoid chokepoints, such as long traffic lines at gates, where people are vulnerable to attack and are blocking emergency response vehicles, if required.

Many states and counties require some sort of intersection control for larger churches, schools, and sports and recreation events. Although it is tempting simply to use volunteers with reflective vests, it is important to have a uniformed police officer directing traffic along with a marked vehicle with flashing lights, not only to slow vehicles but also to show presence to any opportunist who may decide to strike during the congested, chaotic time. A possible solution is to use a member of your church congregation or the spouse of one of your school, hospital, or sports/recreation venue employees who happens to be a law enforcement officer. However, if you have to hire an officer, go directly through the county or local police departments instead of using a contractor, which is more costly and will likely outsource to the same organization.

SECURITY

We accomplish three goals through robust physical security features: portray to would-be bad actors that the facility is hardened and deter their actions, protect our property and its occupants in the event of penetration or attack, and make them feel safe, improving staff productivity and providing a better experience for users whether learning, worshipping,

or healing. In for-profit organizations, a strong security infrastructure and program will positively affect your bottom line, especially for customers who make decisions about what sporting and recreational venues they will entrust with their lives and those of family members.

Locks

Some facilities have only a few doors and others have many; no matter your situation, know that locks are critical to securing your property. Locks can be very easy to defeat if they are not made or installed properly. For instance, most locks installed on home doors can be defeated in a matter of minutes by someone with basic knowledge, which can be easily gleaned from the Internet. A simple padlock can be cut with a bolt cutter. A file cabinet can be breached by a crowbar. So how do you keep out those with bad intentions?

Although we want the visitor's first impression of the facility to be favorable, always choose security over aesthetics. Exterior doors must have, at the least, a dead bolt and never contain glass or be surrounded by glass window panes. In the Newtown, Connecticut, shooting at Sandy Hook Elementary School, the school's security procedures had just changed, requiring visitors to be admitted individually through a set of security doors after visual and identification review by video monitor. Doors to the school were locked at 9:30 a.m. after morning arrivals. Adam Lanza arrived at the school at 9:35 a.m. and the door was locked. He simply shot through the glass panel next to the door and stepped inside the school (Figure 9.4). According to the official report: "The doors to the school were locked, as they customarily were at this time, the school day having already begun. The shooter proceeded to shoot his way into the school building through the plate glass window to the right of the front lobby doors" (Office of the State's Attorney Judicial District of Danbury 2013).

Once inside the school, Lanza had a distinct advantage because he had attended Sandy Hook and had intimate knowledge of the inside of the building. However, there were infrastructure weaknesses detailed in the Newtown report, disadvantages that allowed Lanza to kill twenty innocent children and six teachers and staff members in just five minutes before turning the gun on himself when the police arrived. For instance, the report discusses the office and classroom doors: "The doors in the hallway all locked from the outside with a key. The interior door handles had no locking mechanism. All of the doors opened outwardly toward the hallway. All doors were solid wood with a circular window in the upper half of the door." Although investigators did not discuss how these doors failed to protect the building occupants, the report is replete

FIGURE 9.4 Front entrance of Sandy Hook Elementary School.

with examples of how Lanza was walking up and down the hallway trying doors and looking through windows. Perhaps, if the doors also locked from the inside, with a double key lock, lives may have been spared. Also, having windows on the doors provides visual advantage to the shooter and another way to get through the door if it is locked from the inside. Photographs taken at the scene show the classroom windows were the type that opened up and inward just a few inches, with not enough space for a child to escape. The classrooms were on the first floor and perhaps people could have fled the scene through the windows if they slid on a track. The Sandyhook tragedy gives much to consider when assessing external and internal building security.

Who has access to your building? How many people have keys to your building? Do they all need a key to the front door? Typically, too many people have keys to a building. Keys should be numbered, issued by signature, and stamped "do not duplicate." The types of locks are also important; for instance, a standard lock has a cylinder inside with a series of pins that move up and down. When you insert a key into the cylinder, it moves the pins up and down vertically; when the pins line up correctly, the cylinder rotates and the lock opens. Locks with more pins are harder to defeat; for instance, a filing cabinet lock may have three pins whereas the lock on your front door may have six or more. The depth of the pins also helps make the lock more secure, to prevent opening by mere jiggling of the cylinder using a pin. Professional locks have pins that are not merely vertical, making them extremely difficult to defeat.

Locks can also have "smart cards" or electronic chips in the key, allowing for remote access and the ability to activate or deactivate a key and to control and track access to a room. For example, using keys and locks with electronic chips allows the facility manager to give access only on certain days (church services or school days). Naturally, we should not assume people with keys to our facility have bad intentions; however, keys are routinely stolen or lost. In government facilities, lost keys often mean locks must be changed and new keys issued. Electronic keying allows for instantaneous changes that immediately prevent access in the case of nefarious intent by a thief or a person finding a lost key. The basic principle is to limit access.

Interior doors should have locks, including supply closets, which are notorious hiding places for a bad actor and/or the stockpiling of supplies for an operation. Business offices must be further hardened to protect not only from the theft of private information, but also the occupants who might be the target of a criminal act or an attack. Keys to these doors must be strictly kept to those who need daily access. Although some large hospitals now have sophisticated systems that automatically lock all doors and stop elevators in the case of a lockdown, consult with law enforcement and fire officials prior to installing such a system, as it could trap people trying to flee.

Alarms

What is the backup plan if your key system is defeated? Some soft target facilities have sophisticated alarm systems and others have none. If you do not have an alarm system, why not? Security companies can install alarm systems at your facility for minimal cost and charge modest monthly monitoring fees. If you do have an alarm system, is it the right one and are all of your bases covered? It may be time for a security assessment and upgrade.

An alarm system obviously protects your building and its occupants, but acts as a powerful deterrent to many would-be intruders. When 422 convicted burglars were surveyed, approximately 83 percent of the offenders said they would attempt to determine if an alarm were present before the burglary and about 73 percent said they would seek an alternative target if so. Among those who discovered the presence of an alarm while attempting a burglary, half reported they would discontinue the attempt, and another 37 percent said they would leave the property. About one-third of the respondents planned their crime; the rest were opportunists, mostly looking for money or drugs (Kuhns and Blevins 2013).

If you have a central alarm system, it can be wired or wireless. It can be monitored by a central location or "bells only" in which you hope the

loud alarm is a deterrent to the penetrator, who then departs the property. Remember that the alarm code is just as valuable as the master key and you should try to limit distribution of this code to staff who come to work early to open the building and stay late to close, or those who need to enter at odd hours. However, all staff should have the silent duress code number they can punch into a panel, alerting the alarm company to call law enforcement, a feature only possible with monitored systems.

If you choose a monitored alarm system, sensors will be placed on doors and windows. You may also add motion sensors to catch movement in the building and glass breakage detectors on sliding doors. When triggered, the alarm signal travels via a telephone or Internet line to a central monitoring location where an employee receives information such as your address and possibly a schematic of your building with the exact location of the breach. The alarm company will have several contacts on file and will first call you before calling law enforcement, to prevent false alarms. Typically, you will have a prearranged, easy to remember telephone password confirming your identity. You must think redundancy when deciding on an alarm system for your facility; if the person is hiding inside the building when you lock up for the day, the motion sensor will detect him or her. If the intruder can breach the external door lock and alarm (pressure pads are easy to defeat, magnetic pads, not so easy)—again, the motion sensor will work. Glass breakage detectors are important on sliding doors, as the actor may try to avoid the sensor on the track by entering through the broken glass.

As previously mentioned, if your system is monitored, an employee can enter a duress code into the panel to alert authorities; in this case, no calls will be made to protect those in the situation and law enforcement will immediately respond to the location. Also, panels typically have hot buttons to push for medical help, fire, and police; these are timesavers during an emergency. An alarm system is a great investment and most insurance companies offer discounts for their use.

You should also have a panic alarm built into the reception area; this is a simple button located under the desk that can be discreetly pushed in the event of an emergency to signal silently for help. The signal can be set up in different ways; it can be wired so the duress call will go straight to the local alarm company, which will immediately send the police. Churches, schools, and hospitals should consider having a duress button in areas where counseling takes place and possibly also in conference rooms. The panic signal button does not have to be programmed to notify the local alarm company or police department; it is possible to have it signal for backup: for a colleague to come to the area and provide backup. The button should be pushed only in a situation where there is the danger of physical violence; the staff could be trained not to enact the duress signal if someone is merely acting demanding or overly

emotional. Banks are served very well by these silent alarms, with police typically arriving while the robbery is being committed or shortly thereafter. Naturally, bank robbers know banks have these alarms and yet are undeterred. Similarly, we need to realize that security features will not keep determined bad actors from engaging.

Visitor Access and Badges

Having a solid visitor management program to control access to your facility is incredibly important. If there are several access points to the building, have clearly marked signage funneling visitors through one set of doors. Have the visitor sign a log with name, time, and cell phone number and produce photo identification for entry, preferably a government-issued card such as a driver's license. You may hold this identification in exchange for a visitor's badge. Many secure government buildings such as the Pentagon require two forms of government-issued photo identification. The best practice is to have the visitor wait in a designated area while you contact the individual he or she came to see; do not let him or her wander aimlessly around the building. Having positive control of the visitor is important. Secure schools do not let parents walk items to classrooms (forgotten lunches, books, musical instruments); they may leave the items in a designated area in the front hallway and the child comes later to collect. Sign-in logs must be kept for a designated period of time, as they will provide evidence if the visitor commits a crime on the property, is in a parental custody battle, and so forth. The rosters also allow other due-diligence activities, such as running the name through the sex offender database. Although these activities may feel uncomfortable or intrusive, remember you are responsible for the protection of hundreds, if not thousands, of innocent people. Inconveniencing a visitor is a small price to pay.

Closed Circuit Television (CCTV)

We have already discussed cameras in terms of violent criminals, who barely see them as a deterrent, hoping they aren't taping or their image is obscured enough to cause doubt of their identity. On the other hand, over forty percent of convicted burglars indicated that the presence of surveillance cameras would deter them from a target. We have discussed how some terrorists often conduct surveillance of their targets while planning, while others simply hit a target of opportunity. A key tenet of this book is that facility owners should not base hardening activities on guesses as to who might attack or how. Therefore, my opinion is that all soft target locations should have CCTV that is preferably monitored, but

at the least, is taping for later reference or evidentiary purposes. Many systems refresh on a cycle; 48 hours is probably a good point to start taping over old data. CCTV acts as a set of eyes when people are not available, and it helps gain convictions and even win court cases for you and your insurance company in the event of a lawsuit or claim.

Admittedly, CCTV does not deter a suicide terrorist who plans to lose his or her life or an enraged violent criminal who is not thinking rationally. However, if the actor believes the cameras are being monitored, they know there will be an immediate law enforcement response, compressing the timetable for the criminal act. Camera systems should be used to watch not only the front door, but also other exterior doors, hallways, classrooms and other multipurpose rooms, and the parking lot. There are state laws against filming in certain areas such as bathrooms, locker rooms, changing areas, or nursing mothers' rooms. New camera systems transmit images over the Internet, so you can watch the feed from your computer or even wireless devices such as a Blackberry or an iPhone. Another great feature of CCTV systems is pan, tilt, and zoom (PTZ) cameras that can be remotely controlled if you need to get a closer look at an individual. For outside cameras, you could also employ infrared (IR) technology to see better in the dark; in fact, many companies are now installing IR cameras indoors to capture criminal activity that may be occurring in dark corners or with flashlights. Many systems may be purchased over the counter and installed by the user; however, security system companies would be happy to bring their experts to your property to discuss CCTV coverage.

Public Address System

I strongly recommend facilities have a public address system for broadcasting emergency information to the entire building. During the Sandy Hook Elementary shooting event, one of the injured staff members unknowingly tripped the loudspeaker system when dialing 911 for help. Her phone conversations were heard throughout the building, as were the gunshots in the front office area. This alerted the teachers and staff to the crisis and they had precious seconds to lock doors and hide students. The librarian called the front office and the staff to see what was happening and the staff member told her there was a shooter; again, this was broadcast to the entire school.

The Winnenden School, located in southwestern Germany, was the scene of a mass shooting when former student Tim Kretschmer entered the school with semiautomatic weapons on the morning of March 11, 2009. Immediately following the start of the attack, the school's headmaster broadcast a coded announcement saying "Mrs. Koma is coming," which is the word "amok" spelled backward. The message was a

safety measure installed to alert the teachers of a school shooting and give them a chance to help students escape or shelter in place; it was established in Germany after a previous school massacre at Erfurt.

Intercom systems are also excellent ways to transmit specific threat and emergency information immediately. Hospitals have elaborate code systems that would be easy to adapt to other situations; for instance:

1. Code blue/code 99: CPR team
2. Code red/red alert/Dr. Firestone: fire alarm, activate department fire protocol (close fire doors, move people past fire zones, evacuate if ordered)
3. Code orange/code purple/code silver: internal incident (psychiatric patient missing, active shooter in building, active bomb threat, etc; activate case-specific disaster plans)
4. Code black/code yellow/code 10: external incident (natural or man-made disaster, mass casualties; activate department disaster plan)
5. Code pink/code Adam/Amber alert: missing infant/child (lock down all exits, be on lookout for suspicious persons)
6. Code green/code 00/all clear: all clear, resume normal duties

In one school district, a "code 303 meeting" was known universally, even among the students, as the code for a bomb threat. "Mr. Falkes" and his parents being in the office meant a bomb threat, "Professor Norris" needing to meet his wife in the teacher's lobby meant weapon/stranger on site, and an "ROTC Club meeting" being canceled meant something very bad was happening that required immediate staff-wide attention (via e-mail or intercom). At an exhibition center in London, loudspeaker calls include, "Will Mr. Goodfellow report to the security suite"—the code for a fire. A report that, "Mr. Goodfellow has left the building" is all-clear code for the fire situation. "Staff call 100" is the code for a bomb threat, and, "Staff call 100 has been canceled," is the code for the bomb threat passing. At one college, instructors use a phone code to alert security that a student they are meeting in private may turn violent. If they want a security guard to come to the office as a precaution, they call the outer office and say "I'll be a little late for our meeting with 'Dr. Barry'"; if they want a guard to come in immediately, they say the appointment needs to be postponed.

The combination of the intercom and a code system can save lives.

Ventilation System

We discussed the threat of weapons of mass destruction (WMDs) in the previous chapter and, for closed buildings and venues, it is important to

understand your central air conditioning and ventilation systems. For example, find out if your building has fresh air intakes or recycled air intakes; newer systems are likely a combination of both. Are the units located on the roof, where they may be harder to reach (ideal) or are they on the ground and easily accessible? If an attacker is using a chemical or biological weapon against the property, he or she will likely introduce it through the intake system for maximum dispersal in the building. Even over-the-counter pepper spray will affect building occupants if introduced this way. If the unit is on the roof, make sure hatches are padlocked. If the unit is on the ground, consider building a fence around the unit with a lock on the gate. If possible, try to monitor these locations with security cameras and, if your organization cannot afford security cameras, then include these locations in a walk-through for your security team or administrative staff.

Dining Halls

For facilities with kitchens, consider whether you have a "clean" environment; for instance, when they are not in use, do you secure items that could be used as weapons such as large knives? Are food items secured in tamper-proof containers or locked refrigerators so a bacterial agent cannot be introduced? In churches, kitchens may only be used once a week, so they may be a good place for an insider or potential attacker to store supplies. Dining halls are particularly vulnerable to a mass shooting or kidnapping/hostage situation because there can be many people in a confined space; several attacks already profiled in this book have occurred in a cafeteria.

EMERGENCY PREPARATIONS

Hardening your facility includes being prepared for any contingency, whether there is an emergency in your town or city and you are receiving scared or hurt people, or whether you have a security incident on your property and need to provide medical care and possibly shelter in place until help can get to you. The first action is to take the applicable free FEMA courses listed in Appendix B, such as IS-360: "Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship" or IS-362.a, "Multi-Hazard Emergency Planning for Schools."

Specifically, you should have a four-pronged approach to cover all bases: a "hold room" to secure your leadership, a command center for

you and your key staff, a strong medical program, and the ability to shelter in place.

Hold Room

A hold room is a place where you and other key staff or important visitors can retreat in the event of an emergency and hold for an undetermined amount of time. The room should be located in an evacuation area or point of the building where law enforcement can most easily get to you and you can get out as needed. The hold room can be as simple as a room with a door and lock or as elaborate as an underground facility. It may be worth the money to purchase a security door for the hold room—whether an "intruder" door that will resist being breached or a ballistic door that protects from forced entry but also repels 30.06 caliber rounds. At the very least, you want to make sure that the door can lock from the inside and it has no windows. Although it seems counterintuitive, it is best to select a room with no exterior windows for additional security. The hold room must have a landline phone in case cellular service is not working, and you may also want to have a charged cell phone in the room in the event the phone lines are not working. Also pre-position a case of water and energy bars in case you need to sustain those in the hold room for more than a few hours. Flashlights are also a good idea in case the electricity goes out, as well as a battery-powered radio so you can get news updates on the unfolding situation. The goal in an emergency is to get out of the facility; however, if that is not possible, the hold room will buy you time until law enforcement arrives. Be sure to add checking the hold room phones, supplies, and door lock mechanism to your facility walk-through checklist.

Emergency Response Team and the Command Center

In the event of a major incident in the surrounding community or at your facility, you may want to stand up an emergency response team and have an area that can serve as your command center. The command center might be the same as the hold room. You will need landlines, flashlights, and a radio with extra batteries, water, and a supply of nonperishable food, such as energy bars. Handheld radios that are charged and ready are a plus if someone needs to leave and communicate with the command center. Pads of paper, pens, and even a whiteboard with dry erase markers would be helpful. This is the central repository for information and checklists.

Next, assess your potential emergency team. You may want to poll your employees to evaluate the additional skills and resources they bring to your operation. For instance, do they have a conceal carry permit and do they regularly carry a weapon? Do they have medical training, private security or a military background, or experience as a volunteer firefighter or paramedic? When formulating the emergency team, think about the skillset and also the mindset: can he or she handle an extremely upsetting, emotional event and be an asset to the team, instead of a liability? Once your emergency team is identified, create an "alert roster" with their names and cell, home, and e-mail contact information. Make sure to check the information regularly to ensure currency.

Who should be around your table? If your staff has directors or heads of specialized sections, they should each be there—security, facilities, communication, human resources, legal, etc. Also, if you have any counselors on staff, one should be designated to sit on the emergency response team. Additionally, have someone on your team in charge of handling the press and social media. If your building has been attacked or there is a mass hostage situation, others will blog, tweet, and Facebook; take control of the "message" and transmit what you want people to know about what is happening inside. Also, information you transmit could save the lives of others; for instance, during the strong earthquake on the Eastern seaboard on August 23, 2011, citizens in New York City saw the Twitter alerts about an earthquake that originated in Virginia 15–20 seconds before seismic waves struck the city. According to Facebook, the word "earthquake" appeared in the status updates of three million users within four minutes of the quake. Twitter said users were sending as many as 5,500 messages ("tweets") per second.

For the purpose of keeping control of the message and transmitting data that could warn others of danger, you may want to have Twitter and Facebook shell accounts established to use as needed. Naturally, do not transmit any information about law enforcement activity in the building—which responders are on site, numbers, and their plan. In many cases, such as the Westgate Mall siege, the terrorists are also using the media to transmit and television and radio to assess the activities of law enforcement outside. Also, never transmit the number of injured or fatalities, or any pictures that could be used as propaganda by the bad actors or disturb family members.

I recommend you have a binder with checklists for each situation that could arise. One thing you *must* have on hand are maps of the building and/or blueprints as these are critical for first responders and law enforcement, especially if there is a hostage or active shooter situation. These floor plans must have cardinal directions and specific distance by feet (and even steps); walk your buildings and grounds and then map it out. Law enforcement will want to know everything about

the ventilation system ducts, whether doors open in or out, and location of light switches. This is why you must know every single inch of your property; you will be the expert they turn to for answers.

Perhaps your binder will include checklists for different contingencies that your facility might face. The best way to ensure your team is prepared and ready to handle an emergency is to practice through exercises. Take the FEMA courses listed in Appendix B, specifically IS-120.a, "An Introduction to Exercises"; IS-130, "Exercise Evaluation and Improvement Planning"; and IS-139, "Exercise Design." In addition to full-scale practices, crisis "table top" exercises where you and the team report to the command center and simply talk through the event are also a must, perhaps quarterly. There are experts who can create scenarios tailored to your organization, or you can simply draft the scenario yourself based on past events such as the Beslan school and Moscow theater sieges, the Boston Marathon attack, Columbine, and so on. Run through it with the team and keep throwing in unexpected problems such as the phones dying, a family member breaching the cordon and entering the building looking for a loved one, or the electricity going out. Remember the "pilots-in-the-simulator" approach; make it very difficult or even impossible for your team to handle and they will rise to any future challenge and succeed. During contingency operations drills in the military, a card may be handed to the leader within the first few minutes of the exercise indicating he or she is out of the fight—either killed in the attack or otherwise incapacitated. This forces the team to consider who would step up and lead and gives the person the opportunity to sit in the "hot seat." Of course, you are not on your property 24/7, and there is a possibility a crisis will strike while you are away. Do not be the single point of failure for your team.

Something to ponder are the trigger points for action. Let us say there is an emergency in the community and it is infringing on your property, threatening your facility and the people within. When should you abandon the facility and how? I was fortunate to attend a conference session in Dubai regarding hotels in the Middle East and their contingency plans. During the 2012 uprisings in Libya, several US hotels were caught in the middle of the crisis in which a US ambassador and his team had already been killed in Benghazi and the embassy burned to the ground. One hotel unexpectedly was the recipient of an influx of people after the embassy made an announcement (without coordinating) that all Americans should go to this particular hotel. The hotel manager looked out the window and saw a line of cars and Americans outside his property's gate, which he had locked down. Naturally, he took all of the Americans in and bedded them down with the rest of the hotel customers and staff. But at some point, he had to make the difficult decision to leave the property, possibly forever because it would likely

be overrun and destroyed by militants. They needed more buses than originally planned, and people could only take one small bag, leaving the rest behind. Travel arrangements had to be made with airlines, and the now-large convoy of Americans to the airport required security. A bad situation quickly degraded to the worst scenario. Fortunately, they all made it out of the country; however, the property still sits vacant.

The manager of the hotel in Libya told us he wished that he had had three plans on the shelf that day, instead of just one. He called them the "alpha, bravo, and zulu plans," Zulu was the worst-case scenario of no rescue possibility and ditching the facility. The account of the hotel manager and others profiled in this book teaches an invaluable lesson: expect the unexpected and plan accordingly.

Bomb Threat

Organizations all over the country receive bomb threats every year by phone, mail, e-mail, or note at the facility. Most of these threats are geared toward one main purpose: to disrupt everyday activities, whether final exams, a church service, or a major event. Although many threats turn out to be benign, attention-getting mechanisms, you should not guess—call law enforcement immediately and they will conduct a thorough sweep of the building, possibly bringing dogs that can detect explosives and other high-tech equipment to ensure the building is clear. The bomb threat sheet provided in Appendix D should be close to all telephones so the call recipient can immediately write down the details from the call. Train those who answer your phones to stay calm and keep the caller on the phone as long as possible to gather information about gender, background noises, etc. The conversation might even allow your staff member to ask when the bomb will go off, to include the time and date, and to query about whether the bomb has already been placed in the building and, if so, where. Practice is key to ensuring your employees respond properly when receiving a phoned-in bomb threat. Appendix E contains the evacuation distance chart that you can use to move people, vehicles, and the like away from the location immediately. Have an evacuation plan, post it, and practice often.

Medical Program

A good medical program is an important part of your security plan. During a medical emergency, unless at a hospital, your staff, building occupants, and visitors may not be able to think clearly and respond while being part of an intensely stressful situation, such as violent

shooting. Therefore, it is important to have medical protocols in place that everyone is familiar with and to train to the worst possible scenario.

There have been cases of people freezing and being unable to dial 911. It was not because they did not know the number "911" but rather because an additional digit was needed to get an outside line, like dialing 9 first. To prevent these kinds of situations, simply place a sign or sticker on every phone that reminds the caller to dial 9 for an outside line and then 911 in the event of an emergency. Recall that part of your hardening efforts will be to ask the staff if they have special skills, including first aid, CPR, or advanced emergency medical care. During an emergency, have a plan to find these people and get them to the scene. Your organization may want to sponsor training days with on-site classes delivered by the American Red Cross, American Heart Association, or the National Safety Council. Check with your staff, church membership, and parents of your students; you may have certified trainers who can teach one of these classes. CPR training for all is a must, and your organization should also consider purchasing automated external defibrillators, known as AEDs, now located in public areas such as airports and shopping malls. These devices are used to shock a person's heart back into a healthy rhythm and are designed for the lay person who has no training, as the unit gives verbal commands to the user on how to use the apparatus. Based on the size of your facility, you may want more than one AED. Make sure you perform routine checks to ensure the battery is charged; add this to your security checklist.

There are many helpful smartphone applications on the market with CPR and tourniquet instructions that you and your staff could preload into your phone or tablet computer. I have compiled a list of emergency-related apps in Appendix F for your consideration.

A first aid station or a central repository for supplies is a good idea. Based on the size of the facility, you may want one on each floor. These range in all types of sizes, shapes, and prices. However, it is important to have at least a rudimentary first aid supply available in the event of an emergency, with many gauze pads and dressings, roller bandages, adhesive bandages including butterflies for deep cuts, tape, scissors, antibiotic and antiseptic salve, "space" blankets, and latex gloves. You may also want to have breathing barriers with one-way valves in case you need to administer CPR to multiple victims. Some kits have the equipment needed to run a peripherally inserted central catheter (PICC) line IV with fluids, as necessary. I recommend keeping these supplies packed in backpacks, as "go kits" for easy transport to the scene of the emergency. Finally, your organization should consider joining the Red Cross Ready Rating Program, which is outstanding and free. The program offers an online 123 point readiness evaluation for businesses, churches, schools, and other organizations to assess

preparedness for an emergency and help to address vulnerabilities (American Red Cross 2014).

Finally, consider purchasing hoods for your employees. A product I used extensively in the Air Force is now available for purchase by individuals and companies. The victim rescue unit (VRU) escape hood is a head and respiratory protective hood that can be donned quickly and is compact, lightweight, and totally enclosed with its own oxygen supply. The VRU will protect the user from smoke, chemicals, biological agents, and radiation. It is available for order online (http://myescapehood.com/). You may want to place hoods in your vehicles, and pre-position enough for your ERT in the command center.

Shelter in Place

During emergencies happening either outside your property or on it, you may choose to direct the staff and building occupants to "shelter in place." This term is widely used by the military and government agencies; the concept originates from procedures taken during a nuclear, chemical, or biological attack. You should prepare for this worst scenario where you need to create a barrier between yourself and potentially contaminated air outside, a process known as "sealing the room" as a matter of survival. This type of sheltering requires prior preparation, planning, and practice.

First, designate a room or rooms with the least numbers of windows, a landline phone, and are stocked with water and nonperishable food supplies such as energy bars. Have a pre-positioned emergency kit with flashlights and a battery-powered radio, and do not forget extra packs of batteries. Gather all building occupants into the room(s), bringing in your first aid backpack "go kits," and then lock the doors and close the windows and all air vents. Turn off fans, air conditioners, and forced-air heating systems. Seal all windows, doors, and air vents with thick plastic sheeting and duct tape. Consider measuring and cutting the sheeting in advance to save time; it must be wider than the opening you are trying to cover. Secure the four corners first with duct tape, pulling the sheeting tightly across the opening. Then tape down all edges to form a seal.

"Shelter in place" is now a term commonly used during active shooter or other violent situations, as a way to keep people inside locked rooms. If sheltering during a violent attack, first lock the door from the inside and cover any windows on the door. Turn off the lights. Move as much heavy furniture as you can in front of the door to prevent it from being kicked in. Move to the back of the room. Tip over long tables and hide behind them in the far corner of the room, lying flat on the ground to lower your profile. Silence all cell phones and pagers and be absolutely quiet.

If you are hit by debris or a stray bullet, do not cry out; remain as quiet as possible and play dead. For more on how to prepare your staff and building occupants for an active shooter situation, I recommend reading DHS's active shooter booklet (DHS 2014) and viewing the Houston Police Department's video "Run, Hide, Fight" (City of Houston 2013).

ELEMENTARY SCHOOLS IN FOCUS

While accomplishing research for this book, I watched video from scenes of church bombings, school stabbings and shootings, the mall massacre in Nairobi, the Moscow Theater siege, and the attack at Beslan. Although each event is disturbing and was horrific in its own way, the three-day Beslan attack was perhaps the most heinous. Schoolchildren are particularly vulnerable due to their size and inability to protect themselves, other than running fast and away from the scene, which several children in the Sandy Hook shooting were able to do. Children have more difficulty than adults discerning between real life and fiction; in the middle of a hostage situation or an active shooter event, they are likely to freeze in a state of suspended reality while trying to decide if it is a staged event or real life. A teenager or adult in today's society is more likely to realize the gravity of the situation and take some type of action to run, hide, or fight.

Therefore, I asked a colleague, Ralph Fisk, who works in the emergency management field and has experience with school preparedness, for advice regarding the challenges and tactics for hardening elementary schools. Please see the checklist in Appendix G.

In terms of school attacks, often the disgruntled actor has ranted on social media about his plight, like UC Santa Barbara shooter Elliot Rodger, who posted a long YouTube video prior to the shootings and had a 145-page manifesto detailing his disgust with his fellow college students. Social media is not only a place to rant, but an outstanding recruiting tool. A disgruntled employee who is vocal about his or her dissatisfaction with your organization makes them a target for bad actors looking for an insider to help plan an attack. Stay vigilant and monitor social media and the Internet through keyword searches to see if anyone is discussing your facility and operation.

Marisa Randazzo is a former chief research psychologist for the US Secret Service who applied a "threat assessment" model to examine the behavior of forty-one school attackers over the previous twenty-six years. She found there was no good "profile" of the type of person who becomes a school shooter. However, there were similar patterns of behavior. School shooters did not just "snap" and begin shooting impulsively; they planned. The attacker was vocal about his or her angst or intentions, trying to procure weapons, writing about the situation in journals

and schoolwork. Randazzo states that "paying attention to changes in kids' behaviors and regularly conferring with one another about smaller threats is key to heading off bigger ones." Of the shooters she profiled in the study, Randazzo found: "These are not kids who were invisible—they actually were on multiple radar screens" (Toppo 2014). In 2014, there were several cases of concerned parents and friends reporting odd and worrisome behavior to school officials and law enforcement, a practice we must encourage, even though the informant likely does not want to get involved.

As a result of the spate of school attacks in the recent year, law enforcement officials have stepped up efforts to hold active shooter drills at schools—sometimes, in a controversial move, using students as role players. On May 19, 2014, at Jefferson Middle School in Tennessee, emergency responders converged on the school after a "report" of shots fired and injuries. The school system fully participated and practiced the evacuation of hundreds of students by bus to a nearby church. Officers and paramedics had to find and subdue the shooters, as well as tend to twenty-two casualties, and school officials had to "lock down" the school and evacuate the students (Marion 2014). This type of realistic exercising is the best possible preparation for the school staff, teachers, students, and local law enforcement in the event of an active shooter situation.

HARDENING THE COLLEGE CAMPUS

Although all of the physical security procedures covered before can be applied, target hardening is not just about barricades and cameras, but also relationships, psychological preparation, and resiliency. Soft target hardening must also harness and apply the soft sciences.

Building Relationships

Several opportunities already exist for schools to partner with law enforcement to address vulnerabilities on campus and harden against threats; however, few engage. This is also a good model for other countries wishing to increase partnering activities between academia and government security organizations. The local FBI office can assist schools with points of contacts for these programs:

1. *The National Security Higher Education Advisory Board (NSEAB).* In response to increased concerns about security on college and university campuses and to open the lines of communication between academe and law enforcement, the

FBI created the NSHEAB in 2005. The NSHEAB consists of nineteen university presidents and chancellors who meet on a regular basis to discuss national security matters that intersect with higher education. Previous panels included discussion on protection of weapons of mass destruction research and laws regarding domestic terrorism investigations on campuses. A new cyber subcommittee is addressing computer vulnerabilities on campuses.

2. *The College and University Security Effort (CAUSE).* FBI special agents in charge meet with the heads of local colleges and universities to discuss national security issues and share information and ideas. CAUSE is a conduit for schools to understand how to harden against the counterintelligence threat.
3. *National Counterintelligence Working Group (NCIWG).* NCIWG was designed to establish strategic interagency partnerships at the senior executive level among the US intelligence community, academia, industry, and defense contractors.
4. *Regional Counterintelligence Working Group (RCIWG).* The RCIWG is a subset of the NCIWG and focuses on special vulnerabilities of local institutions and the threat.

Productive dialogue between education and law enforcement leadership will enhance security efforts. Colleges and universities would be better informed on the threat and mitigation opportunities and can in turn educate government security officials on the rights and protections afforded by the First Amendment in academia and the unique challenges facing our schools. In terms of procedure and policy, college administrators responsible for creating and executing human resources, training, and other programs designed to reduce vulnerability to infiltration and recruitment on campus will benefit. The dialogue will also educate legal personnel in higher education and technology transfer offices at higher education institutions responsible for the execution of sensitive government contracts. The following are suggested questions for colleges and their off-campus law enforcement counterparts:

1. What is the health of this relationship, perceived and real?
2. What is working between the two "tribes"?
3. What are the perspectives regarding which entity is ultimately responsible for protecting the higher education enterprise?
4. How do internal and external factors contribute to the relationship?
5. What policies, procedures, and training would enable a healthy partnership?
6. How can we ensure that faculty and students are part of the solution through increased awareness and decreased vulnerability?
7. How can we open the lines of communication between higher education and the intelligence community?

Students and Staff as Force Multipliers

Often, we fail to share vulnerability information with those who can help us the most: the population we serve. As previously stated in the book, civilians are now the target and therefore have the right to engage in protective activities. Rationale for withholding threat information ranges from not wanting to scare people to not making the organization's weaknesses or vulnerabilities public for business or accreditation reasons. The culture must shift to one in which having a vulnerability and threat dialogue with customers and staff is seen as a sign of strength, not weakness.

As a result of our unwillingness to convey the threat, the "see something/say something" campaigns are largely ineffective and can flood the system with useless data. If citizens do not know the specifics, we will not fully leverage this incredible tool. A better approach would be: If you see (*fill in the "what"*), you say (*fill in what data we want them to collect*) to (*agency they should contact*).

For instance, with respect to meth labs on campus, we may want town pharmacies to be cognizant of repeat pseudoephedrine buyers and give the information to a local drug task force. Agriculture schools have a special resource coveted by bomb makers: fertilizer. Therefore, they must know how to protect the material and report any theft or suspicious activities. Small local airports should be trained to recognize suspicious drug or human trafficking activities. Schools hosting sensitive government research and development (R&D) contracts should ask law enforcement experts to train professors to understand their value to countries of interest and to recognize elicitation attempts by students and report them to the local FBI office. Students participating in sensitive R&D activities, in military ROTC units, and degree programs such as criminal justice and national and homeland security might also receive specialized training to make them force multipliers on campus. The administrative staff that handles the J-1 visa process should know who to contact if a student is a no-show for classes or leaves the university. Clearly, just starting the conversation is a hardening method.

Exercising Due Diligence

If you ask a college president who is responsible for protection from foreign theft, terrorist threats, or a criminal element on campus, he or she may point toward the local police department and FBI office. If you ask law enforcement, they may point to the campus leadership. In the past, schools have very much acted like victims when a national security or major criminal incident occurs, instead of accepting any type of responsibility. When a school reports a violation of government rules

regarding R&D programs, it is typically only "slapped on the hand" and funding is not pulled. In April 2011, the FBI Counterintelligence Unit issued a white paper indicating the escalation of targeting and collection activities, asking universities to please engage to protect their programs (FBI 2011). Who is responsible for the existence of a major spy ring on a research campus, a meth lab in a dorm, or a student whose J-1 visa has expired, yet is still on campus? There is an urgent need for an honest dialogue about responsibility and establishment of punitive action against those who fail to engage properly. This could be the withdrawal of government R&D funds from a campus or a higher level government investigation into failure of local law enforcement to protect the school. As it stands, the lines of ownership are blurred—another vulnerability.

Colleges and universities are soft targets and extremely vulnerable to nefarious activities ranging from misdemeanor crimes to drug trafficking to infiltration by agents of foreign governments. As routine targets become less accessible, domestic and international terrorist groups might also prey on the open campus environment to recruit, spread propaganda, or even stage an attack. In addition to physical hardening, soft targets can be further protected by activities to educate the populace on the threat and build relationships to open lines of communication and ensure unity of effort during a crisis. The successful partnering of academia and law enforcement is essential for both to meet their critical missions. The overarching goal is a balanced and rational approach that preserves our tenets of academic freedom and accessibility yet protects colleges and universities from exploitation.

CHURCHES

All of the preceding hardening tactics certainly apply to churches. For the best example of securing worship services, we might turn to synagogues to gather their ideas and perspectives. Those of the Jewish faith have a history of persecution and Israel is actively targeted by Islamist extremists who have the stated goal of annihilating the country. Naturally, in the face of so many enemies, the Jewish people have unique concerns about securing their facilities. Many synagogues have always employed armed plainclothes security officers, who not only work the perimeter and entrances, but are also seated among the service attendees. Security was tightened with the shooting at a Jewish community center in Los Angeles in 1999, the al-Qaeda attacks of 9/11, and the shootings on July 28, 2006, by Naveed Haq, a self-proclaimed "Muslim American, angry at Israel," at the Jewish Federation office in Seattle. The attack at the Holocaust Museum in Washington, DC, on June 10, 2009, and at the Jewish Community Center in Kansas City, Missouri, on April 15, 2014,

further reinforced the need to protect those of the Jewish faith not only from radical Islamists but also American white supremacists.

The SAFE Washington program (http://www.safewashington.com/) provides an outstanding model of cooperation between religious facilities and federal, state, and local law enforcement. For its eighty Jewish entities, SAFE also "develops best practices for disaster response, community security, community preparedness, and provides low cost or no cost training for community partners through annual training." The website has a password-protected area with secure files only for SAFE members. I would hope there is some intelligence sharing and analysis between law enforcement and SAFE. An outstanding tutorial entitled "Synagogue Security: The Basics" (Moses 2014) gives five pages of security pointed at those leading or securing synagogues. Guidelines for handling visitors, suspicious packages, and security incidents are thorough and tailored to the religious environs.

Following the attack on the Sikh temple in Wisconsin in August 2010, the Sikh community also took actions to better secure their facilities. Using security "sevadars" or volunteers, the temples are protected by trained individuals and the guidelines are to "act without fear, act without anger, act to defend the weak, act to protect the innocent" (Sant Sipahi Advisory Team 2014). As with the Jewish community, much can be gleaned from the activities of those previously targeted to secure their facilities and congregations. There must be a balance between security and the open, welcoming environment that is part of religious doctrine; however, ignoring risks and vulnerabilities is not prudent in today's world.

HOSPITALS

Most hospital planning efforts are centered on response to a natural disaster or mass casualty incident in the local community. Also, there is in-depth planning and training for staff on how to react to common hospital crimes such as violent outbursts in the emergency room, attempts to steal drugs, and domestic situations with spouses and parents. OSHA 3148 requires hospitals and healthcare organizations to do annual workplace violence assessments, and more than thirty-three states also require enhanced protection of hospital and healthcare staff, typically from enraged patients.

However, depending on their operations, hospitals themselves are targets for domestic terrorists such as antiabortion and animal rights activists. Examples presented in Chapter 5 show al-Qaeda and splinter groups are actively targeting first responders at the scene of the incident and then later at the hospital when victims and family members arrive for care. After a few near-misses at its own facilities, the United Kingdom

seems to be leading research on the threat of terrorist attacks against hospitals. Recommended studies include "The Vulnerability of Public Spaces: Challenges for UK Hospitals under the 'New' Terrorist Threat" (Fischbacher-Smith and Fischbacher-Smith 2013), which started the conversation in England regarding the vulnerability of healthcare facilities.

Similar to churches, hospital culture dictates that doors are always open to the masses and restricting entry usually is not possible or desirable. Hospitals not only carry great liability for patient care but also many state patients' bill of rights/state licensing regulations direct patients "receive care in a safe environment." This naturally extends to protection from criminal and terrorist elements and attack. DHS recognizes that nonprofit soft targets such as hospitals need financial assistance to bolster their security and include money in their budget for security enhancements; however, this money is usually apportioned to the states for further dissemination. FEMA has a direct funding program through the Nonprofit Security Grant Program (NSGP). In FY 2014, NSGP was funded to $13 million and plays an important role in the implementation of the national preparedness system by supporting the development and sustainment of core capabilities.

Core capabilities are essential for the execution of each of the five mission areas outlined in the national preparedness goal. The FY 2014 NSGP's allowable costs support efforts to build and sustain core capabilities across the goal's prevention, protection, mitigation, response, and recovery mission areas (FEMA 2014). Several hospitals received NSGP grants in 2014, including John T. Mather Memorial Hospital in New York, which used $75,000 to upgrade its security system, including a new camera system and cards and a card reader for one section of the hospital. Researching how hospitals are using the NSGP grants is a good idea before applying, in order to better tailor the request and posture the hospital for success.

Emergency room entrances are not the only concern; hospital loading docks also present vulnerability. International Association for Healthcare Security and Safety President Lisa Pryse describes loading docks as "volatile" and "often overlooked" and notes there have been two instances where active shooters entered hospitals through unsecured loading dock doors (Canfield 2013). Security cameras should be installed on loading docks as an absolute minimum and a vehicular access control system is also desirable.

MALLS

Naturally, as businesses that are trying to attract customers and make a profit, malls prefer to avoid heavy-handed security measures like metal

detectors, armed guards, and bag screenings. They gravitate toward more passive measures, such as mass crowd surveillance and using human behavior theory to identify would-be troublemakers.

However, the Westgate Mall massacre served as a wake-up call to malls worldwide, which are now upgrading cameras and adding layers of security to protect their businesses and shoppers. Several lessons learned from the strategic response must be addressed in communities hosting malls. First, Kenyan officials did not act to protect their lucrative soft targets despite intelligence reporting on increased capability and threat of active, known, and capable al-Qaeda groups and chatter about their targeting of malls and other civilian venues. Therefore, the mall staff and security officers had no idea the threat was high and likely did not raise the security posture. Second, the police and military had no ability to coordinate and had never practiced communicating or working through thorny first-response issues such as who is the incident commander at a mass shooting event. This lack of coordination resulted in police being fired upon by the military while trying to rescue shoppers. Furthermore, military forces had only exercised a rescue scenario one time and this was their first real-life experience with a mass hostage situation; they were late to the fight and wholly unprepared, lacking even basic equipment such as night-vision goggles. As noted in the case study in Chapter 6, the behavior of security forces at the Westgate Mall lacked professionalism and discipline. Their rampant looting that trumped finding the terrorists prolonged the siege and exposed a degree of corruption that shocked the public and tarnished confidence in the forces' ability (and desire) to keep the population safe. There are many lessons learned from the Nairobi disaster to incorporate into our training and exercises.

In light of the Nairobi attack, several malls in the United States have held large counterterrorism and mass casualty exercises in 2014. Typically led by the FBI, these exercises happen after mall hours.

In Portland, Oregon, joint training between local law enforcement and mall personnel paid off during an active-shooter event at the Clackamas Town Center in December 2012. Responding officers knew the mall layout from the training session and were able quickly to corner and stop the shooter, who had already killed two shoppers and seriously wounded a third in a random act of violence. The training initiative is one of many positive developments driven by the International Council of Shopping Centers (ICSC), which, in conjunction with the Department of Homeland Security, Federal Bureau of Investigation, and police, dramatically improved readiness throughout the mall and shopping center industry. Mall security, formerly ridiculed and scoffed at in pop culture, is now a highly trained, professional force (Bradley 2013). They are faced with a rising number of violent incidences ranging from assault to gang violence and mass shootings and are learning and sharing best practices globally.

A new study examined the infrastructure of the Westgate Mall and how it allowed for a successful asymmetric attack by a small group of men against a large group of first responders and military personnel and apparatus. For instance, the open atrium allowed the shooters to get a high position on top floors and shoot down at fleeing customers and arriving police and military. However, the atrium also provided an advantage for store owners on top floors, some of whom could see the carnage below and were able to lower their security doors and barricade themselves in the store. Enclosed areas, such as the casino and the cinema, were used as holding areas for hostages (Butime 2014). Studying the Westgate Mall attack from the perspective of the element of surprise achieved by the attackers, the vulnerability of shoppers, the physical layout of the mall, and the poorly coordinated response is critical for all who operate, secure, and visit malls.

SPORTS AND RECREATION VENUES

As discussed in Chapter 6, sporting and recreational venues have been targeted by terrorist groups who appreciate the large, dense crowds and televised coverage that will ensure a ripple effect of fear across the populace. Current security procedures include limiting entrance points, limiting the size of bags and thoroughly searching them, and using CCTV and facial recognition technology.

Unfortunately, most venues rely on part-time, low-paid security guards who are both the first line of defense and the weakest link in the sports venue security infrastructure. In 2013, California revoked 154 security guard licenses, often due to criminal convictions discovered after the license was issued, and Florida revokes an average of more than 350 security licenses annually for criminal records. Compounding the problem, there is a "county option" approach to licensing and training of part-time security guards. States vary wildly in their procedures and seven require no security-guard licensing at all. Among those states that do, several, including Massachusetts, do not require training. In Florida and California, perhaps the strictest states, 40 hours of training are required, including a course on terrorism awareness and weapons of mass destruction. Some companies have classified employees as "event staff" in security roles at stadiums to avoid training requirements and to increase profits (Schrotenboer 2013). Also, in the quest to increase profits, sports venues often award security guard contracts to companies that are the lowest bidders. We need to remember part-time staff and volunteers provide a vulnerability in terms of facility access and the ability to stockpile supplies. They can also glean an intuitive understanding of the infrastructure and its vulnerabilities.

According to an Israeli security consultant, there is another inherent problem with security in the United States: Security personnel "don't watch the race, they watch the crowd. That's what they didn't do [at the finish line of the Boston Marathon]" (Schrotenboer 2013). The same consultant explains how, in Israel, unattended packages and backpacks are given about 10 seconds before a security official engages. The next time you attend a sporting event, look at the security guards. Are they looking up into the stadium and scrutinizing people walking by? Or are they watching the game, concert, or event? A quick Internet search yields many pictures from major sporting events such as football and baseball games where professional and volunteer security team members are facing in the wrong direction—the most distressing at the Boston Marathon finish line, seen as the first bomb exploded (Figure 9.5).

In January 2005, the Department of Homeland Security launched the first online vulnerability self-assessment tool (ViSAT) for public venues such as large stadiums. The online tool incorporates industry safety and security best practices for critical infrastructure to assist in establishing a security baseline for each facility. Modules focus on key areas such as information security, physical assets, communication security, and personnel security. As part of the National Infrastructure Protection Plan, DHS also offers site visits and other helpful assistance to partner with owners, operators, and security at commercial venues (DHS 2014). There is a delicate balance between providing security and an enjoyable experience for participants in and spectators of sports and recreation events; with technology, training, and practice, this goal is attainable.

FIGURE 9.5 CCTV capture: first bomb explodes at finish line.

RED TEAMING SOFT TARGETS

As mentioned in Chapter 2, a healthy dose of imagination is needed to protect your facility from threats and to expose your vulnerabilities. According to the 9/11 Commission Report: "It is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination. Doing so requires more than finding an expert who can imagine that aircraft could be used as weapons" (National Commission on Terrorist Attacks upon the United States 2004).

Every security measure has the opportunity to work, but if it fails, it works for the offender. Unfortunately, you, as the facility manager, operator, or security professional, may not see the flaws in your security plan, or be too close to imagine how your techniques could be defeated. In order to have the best plan and make sure your methods work, you truly need to think like the bad guy. Red teaming may be an answer. The term "red team" comes from American military war gaming, where the blue team was traditionally the United States and, during the Cold War, the red team was the Soviet Union. Defined loosely, red teaming is the practice of viewing a problem from an adversary's or competitor's perspective. The goal of most red teams is to enhance decision making, either by specifying the adversary's preferences and strategies or by simply acting as a devil's advocate. Red teaming may be more or less structured, and a wide range of approaches exists. In the past several years, red teaming has been applied increasingly to issues of security, although the practice is potentially much broader.

Superior red teams tend to (Mateski 2014):

- View the problem of interest from a systems perspective.
- Shed the cultural biases of the decision maker and, as appropriate, adopt the cultural perspective of the adversary or competitor.
- Employ a multidisciplinary range of skills, talents, and methods.
- Understand how things work in the real world.
- Avoid absolute and objective explanations of behaviors, preferences, and events.
- Question everything (to include both their clients and themselves).
- Break the "rules."

A red team can undermine a decision maker's preferred strategies or call into question his or her choices, policies, and intentions. As this might be uncomfortable, it is important to put the security of the innocent people who occupy your facility ahead of any ego, sunk cost, or group think about the security of your facilities and organization.

In particular, the Homeland Security Act requires DHS to apply red team analysis to terrorist use of nuclear weapons and biological agents. As terrorists seek to exploit new vulnerabilities, it is imperative that

appropriate tools be applied to meet those threats. Therefore, most red teaming effort currently lies in the WMD spectrum, with professional teams trying to penetrate nuclear facilities, chemical and biological weapons labs, and even military installations that own or operate these sensitive activities. A red team is a group of subject matter experts (SMEs) with various appropriate backgrounds that provides an independent peer review of your processes, acts as a devil's advocate, and knowledgeably role plays the potential enemy. Red teaming can be passive and serve to help you understand the threat and expose your biases and assumptions. Or, activity can be active as the red team attempts to probe and test your security to expose your strengths and flaws. Training is another aspect of red teaming.

Although red teaming for soft targets does not exist today, I believe there can be some cross-application of methodology, currently employed by the US government, to soft targets including schools, churches, and hospitals. Perhaps you could begin with the cross-"inspection" of security procedures by trusted colleagues from other facilities and the cross-pollination of ideas. Or, you may ask them to test your security by sending someone in to test your system. One redteaming exercise recently shared by a colleague included the "perpetrators" wearing a shirt bearing the symbol and name of a famous soft drink company. Holding a clipboard and stating the purpose was to check the soda machines, the redteamer had unlimited access to a school.

For more about the red teaming concept, please see the homepage of *The Red Team Journal,* http://redteamjournal.com/, started in 1997 by my colleague, Dr. Mark Mateski, the industry expert on the topic.

CONCLUSION

Unfortunately, the world has changed drastically since 9/11 and the places we should feel the safest and go for relaxation and recreation are in the terrorist's target book. Fortunately, other sectors such as the military provide a model for soft target hardening activities. Case studies of soft target attacks provide rich examples of successes and failures that enable you to assess your own preparation activities.

You are no longer helpless against this rising threat: you can now confidently move forward and prepare your facility, staff, and users for the unthinkable.

REFERENCES

American Red Cross. "Ready Rating Program" (http://www.readyrating.org/) (2014).

Bradley, Bud. "State of U.S. Mall Security Post 9-11" (December 17, 2013).
Butime, Herman R. "The Lay-out of Westgate Mall and Its Significance in the Westgate Mall Attack in Kenya." *Small Wars Journal* (May 10, 2014).
Canfield, Amy. "Hospital Loading Docks Rival ERs for Security Concerns." *Security Director News* (November 25, 2013).
Carpenter, Mike. "Evolving to Effects Based Operations." http://www.dodccrp.org/events/9th_ICCRTS/CD/presentations/8/092.pdf (March 2004).
City of Houston, Texas. "Run, Hide, Fight." http://www.youtube.com/watch?v=5VcSwejU2D0
DHS (Department of Homeland Security). "Active Shooter: How to Respond" (http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf) (2008).
———. "National Infrastructure Protection Plan: Commercial Facilities Sector" (http://www.dhs.gov/xlibrary/assets/nipp_commerc.pdf) n.d.
———. "Soft Target Awareness Training for Facility Managers, Supervisors, and Security and Safety Personnel: Course Syllabus" (http://www.fbiic.gov/public/2008/nov/STACsylJUL08.pdf) (2008).
FBI (Federal Bureau of Investigation). "Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education" (2011).
FEMA (Federal Emergency Management Agency). "Fy 2014 Urban Areas Security Initiative and Nonprofit Security Grant Program" (http://www.fema.gov/fy-2014-urban-areas-security-initiative-uasi-non-profit-security-grant-program-nsgp) (2014).
Fischbacher-Smith, Denis, and Moira Fischbacher-Smith. "The Vulnerability of Public Spaces: Challenges for UK Hospitals under the 'New' Terrorist Threat." *Public Management Review* 15, no. 3 (March 27, 2013): 330–343.
Kuhns, Kristie R., and Joseph B. Blevins. "Understanding Decisions to Burglarize from the Offender's Perspective." The University of North Carolina at Charlotte Department of Criminal Justice & Criminology (2013).
Lysiak, Matthew. *Newtown: An American Tragedy*. New York: Gallery Books, Simon and Schuster, 2013.
Marion, Steve. "Mock School Attack Tests Readiness." *The Standard Banner* (May 20, 2014).
Mateski, Mark. "Red Team Journal: Understand, Anticipate, Adapt" (http://redteamjournal.com/) (2014).
Moses, Manfred. "Synagogue Security" (2014).
National Commission on Terrorist Attacks upon the United States. (2004): 344.

Office of the State's Attorney Judicial District of Danbury. "Report of the State's Attorney for the Judicial District of Danbury on the Shootings at Sandy Hook Elementary School and 36 Yogananda Street, Newtown, Connecticut." (2013).

Rose, Roger, M., A.Vangura, Jr., and M. Levin. "Wrongful Death, Failure to Deter Crime on the Premises." *Zanin's Jury Verdict Review & Analysis* (http://www.jvra.com/verdict_trak/article.aspx?id=187168) (2009).

Sant Sipahi Advisory Team. "Security and Risk Assessment." (http://www.harisingh.com/SantSipahiAdvisoryTeam.htm)

Schrotenboer, Brent. "Holes in Stadium Security" (May 2, 2013).

Toppo, Greg. "Nerves Fray as Anniversaries of April Attacks Arrive" (April 19, 2014).