2

Security Plan

> I have six locks on my door all in a row. When I go out, I lock every other one. I figure no matter how long somebody stands there picking the locks, they are always locking three.
>
> **Elayne Boosler, Comedian**

In an ideal security world, we would take our Risk Assessment and come up with a perfect plan to mitigate every risk. In reality, the plan you create and implement will be influenced by your style, education, and experience and that of your manager and maybe your lawyer. That is why I do not presume to tell you how to run your department. Instead, I offer some proven methods, best practices, and even some unusual ideas that I have seen or tried myself. It will be up to you to apply the ones you think will work for you and your property.

The security plan is a document that explains what security measures will be taken to mitigate risks (prevent crime and accidents) on and around the property. This process is a bit subjective for hotels and entertainment venues because there are generally no standards or codes that address them. In an airport or nuclear facility, there are government regulations that standardize access control and other physical security aspects. Hotels, amusement parks, nightclubs, and similar facilities are not so regulated. There are certainly fire and building codes, OSHA guidelines, and other applicable regulations, but in general, cameras, lighting, security staffing, and other security measures are not included. The hospitality industry has not yet standardized physical security either. However, there are some best practices and corporate policies applied by larger hotel chains. These will be used throughout this reference and should be used whenever possible in the security plan.

Remember, as with risk assessment, the main purpose of the security plan is to defend the security posture of the property in court. Since there are no standards, a plaintiff lawyer is sure to compare the security at the defendant's property with one that has better security. So, for the purposes of this plan, the best practice will be recommended every time. Your goal is to provide the best defense (security plan) that you can within your budget.

SECURITY IN COURT

When an unfortunate event happens on hotel property, the victim of the act often names the hotel in a lawsuit. The victim sues the hotel—not because the hotel caused the act, but because the hotel did not take adequate measures to prevent the crime or incident from occurring. It is for this reason that the risk assessment and the security plan are so important. The plaintiff's lawyer will try to find where the security was weak or below standards. Since there are no standards, the only way to prove substandard security is by comparing to other properties. The risk assessment will show where the other properties were examined and the security plan will show that the security was equal to or the same as other properties.

The first defense is a good offense. The risk assessment sheds light upon the potential for events, such as a robbery in a parking garage. The security plan will deal with those initial security defenses. If a robbery does occur, it does not mean that the security defenses were weak, but they were obviously weak enough to allow the event to happen. The Security Director then has two choices: (1) leave security as it is and hope for the best or (2) fortify security in the garage and prevent it from happening again.

Option 1: Leave security as is. This option is riskier, but less expensive. Many businesses manage risk in this manner, hoping, gambling, and calculating that another incident will not occur. This is usually a measured risk, weighing the option of spending money on security or spending money on litigation later. This option usually does not appeal to the Security Director, but it is a product of the business world. There is a strong likelihood that the property management makes these types of decisions for the Security Director (more on this topic in Chapter 12).

Option 2: Fortify security. This option may be considered safer, and even morally correct, but is obviously more expensive. There will be costs associated with purchasing and installing equipment and paying wages for increased labor. This option also may be viewed as better for the business's image: It takes safety seriously and does what it takes to provide it to its guests.

SECURITY PLAN

We cannot create a Security Plan until a Risk Assessment has been completed (Chapter 1). The plan includes security staffing amounts, cameras, lighting, access control, CPTED (crime prevention through environmental design), and many other physical aspects. It may also include policies and procedures. Many organizations create and follow very detailed and lengthy plans that explain and outline all of these pieces of their security posture. Other, maybe smaller, properties do not make a written plan. Most security directors are either operating under a plan written by a predecessor or do not have a written plan at all. They rely on their mental notes and personal philosophy to create policies and organize their protective measures.

Like the Risk Assessment, the Security Plan is not very valuable unless it is written. Those who do not have a written plan simply have not had to justify their security to their boss for the purposes of obtaining funds for staffing and hardware. They also have not been deposed on their justification for why they had a certain level of staffing, certain video or alarm systems, or policies that did not address certain aspects of security. The formal Security Plan is not that difficult to write and may save time and money later.

What does the plan look like? In the Risk Assessment example in Chapter 1, guest rooms were evaluated. Guest rooms will be one portion of the plan. The plan will take the risks identified in the assessment and outline how to mitigate them. For example, if robberies were a documented risk, security patrol, cameras, controlled access, and peepholes might be recommended in the Security Plan. By the time each area's security plans are compiled and added to other components like policies and procedures, it becomes apparent that the Security Plan is a comprehensive and lengthy document.

OUTLINING THE PLAN

Part of the Security Plan will be a Policy Manual. To make the plan-writing process easier, the plan presented here will be designed like the manual. This will save time and allow for some solid consistency between the Plan and its key component. The outline of the Security Plan will look something like this:

Department Mission
Organization
Policies and Procedures
Overall Property
Specific Areas

Each of these components of the Security Plan is explained in more detail.

Department Mission

The mission is the overall strategy of Security for the property or organization. This is vital to the plan so that the reader knows what the intent of the Security Department is. While most hotels might presume to have the same mission, they actually do vary. As we see in every type of business that we frequent, there are many missions with many different goals. In a multiuse facility, the focus may have to be explained. Is the mission guest safety, protection of company assets, or life safety, or all of the above? Other departments or contractors may be responsible for one or more of these components, so we will leave those missions to them.

Most hotels are basically the same. The mission might be "to protect the assets of the hotel and its guests and employees while maintaining a safe and comfortable environment for everyone." That is a good mission statement, but the plan will need some more detail. A high-end hotel or a brand-reliant property may incorporate "brand protection" or "luxury" into its mission statement. A budget property or family-oriented facility might not want to include these elements in their plan. Security is a general element of every mission statement, but other elements specific to the type of property also can be included because they will affect decisions on security applications in the plan.

EXAMPLES OF MISSION STATEMENTS

"The Mission of Southwest Airlines is dedicated to the highest quality of Customer Service delivered with a sense of warmth, friendliness, individual pride, and Company Spirit."

"The Ritz-Carlton Hotel is a place where the genuine care and comfort of our guests is our highest mission. We pledge to provide the finest personal service and facilities for our guests who will always enjoy a warm, relaxed, yet refined ambience. The Ritz-Carlton experience enlivens the senses, instills well-being, and fulfills even the unexpressed wishes and needs of our guests."

Remember, we are working on a Security Department mission statement. It is not the mission statement for the entire organization. They are separate and different. It may make sense to follow the corporate mission statement in security, but the corporate statement does not address security decisions. Reading the mission statement of the Ritz-Carlton in the adjacent textbox, you would have to assume that the mission of their Security Department is consistent with the hotel's mission of "finest service" and "unexpressed wishes." It is likely that security's mission is something along the lines of discretion, comfort, and service that supports the objectives of the hotel. As for Southwest Airlines, their Security Department probably focuses on the keywords in the corporate statement like warmth, service, and friendliness.

Your Security mission statement should be consistent with your corporate mission, so consider looking at other departments to see what they have. You also may talk to those who wrote the corporate mission statement and get ideas from them. Finally, as I mention throughout this book, ask your own employees to help develop your mission. Your mission statement is not just something to hang on the wall; it will be used to make important decisions on the type of security used throughout the property. Refer to it each time you make a decision or create a policy. This will help you remain consistent.

Organization

Organization of the Security Department includes the chain of command—or hierarchy—from executive down to front line. The purpose of this section is to make clear who reports to whom and who has which responsibilities. Names are not important—just positions. Why is this important in the plan? One reason is that those who read this plan (lawyers, your boss, and your successors) need to know how decisions are made and at what level. Do frontline employees operate on their own, with minimal supervision, relying on management from other departments to make important decisions or is the organization large enough where there is a shift manager to whom officers report? This may be a vital component of the plan when, in court, your company is trying to defend a poorly made decision.

Starting at the top, who has the highest, or ultimate, responsibility for security matters? This depends on the corporate structure, the size of the organization, and the corporate philosophy. Many companies have an executive security position reporting to the CEO or property manager. This is most preferred and explained in more detail in Chapter 12. Some companies have the security leader (director, manager, etc.) reporting to Legal, Human Resources, or Facilities. There are good reasons for each reporting structure, but that reasoning is probably out of your control. So, for the purpose of the Security Plan, we are simply documenting it, whatever it is.

This organization chart is going to look somewhat like a pyramid and the previous paragraph describes the point at the top. Next is the second line of management. Large organizations use an operations manager in this senior middle position. It also may be divided between operations and investigations or administration. Instead of having two managers in this position, the Ops manager can take the Personnel/Operations side and the director can take the Administrative or Investigative side. The director is still the highest authority, but it saves a position. (It is advisable not to have two persons in charge of the entire operation.)

The above level can be skipped entirely if the organization is small-to-medium in size. The third (or second) tier is middle management. This position could be called supervisors or shift managers, depending on the number of frontline staff. The ideal proportion of supervisor to officer is 1:5. So, if there are 10 officers on a shift or team, there should be 2 supervisors. This is not to say that if the property has decided to use a “shift manager” format, that two managers are needed per shift. It means that each five persons need a supervisor, so this can be accomplished through different levels of supervision.

The next level might include supervisors (if managers are used above) or senior (lead) officers. If a property has 15 officers on a shift, there could be a manager and two or three supervisors, or a supervisor and three senior officers.

Keep in mind that a small property may not have many levels of supervision in Security. If there is one officer on duty at night, he or she may report to a hotel manager or similar position. However, your ideal ratio depends on the size of your property, the skill

V.A. Graicunas developed the term *Span of Control* in 1933 when he researched the effectiveness of varying management ratios. He determined that there were several factors, such as the physical location of the employees (whether they work together or separately), personalities, types of work performed, and the capabilities of the employees. That ratio was found to be acceptable at 4 employees to 1 supervisor all the way to 22:1 depending on those factors. Police departments operate at about 4:1 and fire departments operate at about 3:1.

In the 1980s, a new factor was found to influence the effectiveness of this ratio: technology. Computers and other automation systems took away some of the duties of supervisors and managers and many corporations “flattened” their chain of command. Middle management positions were eliminated as duties were given up to technology. We still look today to eliminate middle management as one way to save money, so if your ratio is higher than those described in this chapter, don’t worry.

level of your employees, and other factors. This needs to be drawn out in the organizational chart as well.

The final level—the base of the pyramid—is the officer. This is the front line and the most important because they do the most work.

The organizational pyramid likely includes other units of responsibility besides Operations. Investigations, Training, Administration, and Safety are common units to include in your chain of command and organizational chart. Others included in some hotels are Lifeguards, Lost and Found, Shuttle Drivers, Parking Attendants, etc. Whatever legs of your pyramid you might have, each has to have an "upline" and a "downline" of who reports to whom from the director on down.

Job Description

Each of the positions described previously and each position held in your department requires a job description. The purpose of a job description is to outline the job functions of that position. This description may be needed in litigation, for progressive discipline, coaching, training, promotion processes, and light-duty determinations.

A job description is relatively simple to create and your Human Resources Department may have already done this for you. Following is an outline of a generic job description.

Position title
Department
Pay range
Reports to
Subordinate positions
Minimum qualifications
Physical requirements
Hours or schedule (if applicable)
Job functions
Revised date

It is important to be as specific as possible, but to leave that last and famous line "and other duties as assigned." That line avoids the insubordinate retort: "That's not in my job description." When all the job descriptions are complete, all of the duties under your authority should be documented. If anything is missing, that will explain where you lack accountability.

Policies and Procedures

This is not going to be the complete security policy manual (that will come later in Chapter 4). For the Security Plan, there will need to be some basic policies that dictate how security will function in each area so that it can be applied later in the plan. This may involve other stakeholders. The Risk Manager (legal counsel), the General Manager, and affected department heads may have a say in how security operates and performs certain functions.

In this section of the plan, it is decided how Security patrols, prevents crime, and reacts or responds to certain events. The Security Director needs to decide in advance of the Security Plan if security is contracted or staff positions, if they will be armed, if they will handle violent, medical, or life-saving situations, and if they will perform other skilled functions, such as profiling and gang intervention.

> In November 2008, 2,000 shoppers lined up outside a major retail store seeking to take advantage of Black Friday specials. Just before the doors were about to open, the crowd broke the doors, and trampled an employee, killing her. Arguably, this incident was not foreseeable and was considered a horrible tragedy. In fact, the major retailer avoided criminal prosecution and any civil penalties by reaching a modest settlement that included changes to procedures that would prevent the situation from occurring in the future. In the years following that event, every store in the chain implemented procedures that prevented the stampede for bargains and the chain had no further incidents. In November 2010, another large retailer had an incident very similar to the one in 2008. In this scenario, the crowd rushed the doors—also seeking bargains—and trampled a fellow shopper. Nobody was killed. What if the injured shopper was killed? Was there foreseeability? Could it be argued that the retailer was negligent? Would you like to be the lawyer or the Security Director for that store?

Overall Property

The security posture of the property also needs to be decided in advance of the deployment of the plan. The director and executive team has to decide if the property will have uniformed security, and if they want to be visible and highly aggressive or discreet and reactive. Generally, the hospitality industry tries to be open and inviting, so bollards, guard posts, cameras, fences, and restrictive signage go against that philosophy. This is not to say that those measures will not be deployed, if necessary, but they need to be justified. CPTED is one way the property and its management can decide to mitigate risk while maintaining that hospitable feeling for its guests.

One of the first things learned in law enforcement or the military is the concept of layered security. If you think you are not familiar with it, don’t be so sure. Anything that is protected is protected in layers. Your home, for instance, likely has several layers of security. Obviously, there is a door with a lock. There probably is also lighting, a peephole, neighbors watching, a standoff area (lawn), white picket fence, a barking dog, and maybe an alarm. These are all layers of security. Our hotel uses layers as well, and we will be documenting these layers in the Security Plan.

Layers of security in the hospitality environment are, primarily, physical, technological, and human. Layers can be considered as concentric rings around the asset, such as fences and walls around a prison. Layers do not have to be physically concentric. Just as in the previous example of your own home, the dog and the alarm are not actually concentric to the house. They are simply another level of security.

A layer is anything that detects, delays, deters, or denies entry to the asset. Examples of layers used in the Security Plan are thus explained.

Physical Layer

A common example of a physical barrier is a wall. Shrubs, trees, bollards, rivers (moats), rocks, and fences also can be physical layers. Potentates and presidents use people as physical layers. Traditionally walls and fences were less attractive, uninviting layers of denial. Advances in architecture and landscape have applied design to this science in the last few decades so the hospitality industry can protect its assets and maintain the beauty and convenience of the property. Each of these types of layers is discussed specifically throughout the book.

Technological Layer

Cameras, alarm sensors, radar, and lighting are examples of technological layers. Cameras provide detection—if they are being monitored—and provide deterrence if they are visible to would-be offenders. Alarm sensors, such as motion detectors, can be an active or a passive form of detection. Radar, not generally used in hospitality applications, is an active form of detection. Lighting is one of the most common layers of security. It is regularly misused or under-used as a decoration or a practical visual aid. When used correctly, lighting allows cameras to work better, deters crime by eliminating hiding places, provides an appearance of activity, and detects criminals in otherwise dark places. Technology also allows us to use tools, such as biometrics and video analytics, as another layer of security.

Human Layer

There are several ways to use staff as a protective layer. Fixed guard posts, walking, driving, and bicycle patrols are common and effective measures used outdoors. Behavioral recognition, undercover officers, and intelligence gathering are some of the more advanced methods of human intelligence used by all types of properties and assets. Personnel are the most effective type of security because they provide detection, deterrence, delay, and denial while providing subjective, intelligent decision making and the ability to interact with guests and provide guest services and other duties. Humans are also the most expensive layer so tend to be used as little as possible.

About 80 school children on a field trip to a water park in Concord, CA, in 1997, caused a major accident. Trying to break a record for the most kids on a slide, the kids overloaded the slide against the orders of the lone ride attendant. The slide, which was designed for single riders, was overcome by the weight and collapsed, killing one and injuring dozens.

Personal responsibility for reasonable behavior does not apply in the hospitality/recreation industry—especially when children are involved. The property needs to take reasonable steps to prevent foreseeable incidents.

Several hotel cases in a few different states are currently shaping the concept of foreseeability. They are considering the presence of other factors such as due care by the hotel, and prior, similar incidents. Even the word "similar" is not a term agreed upon by most litigants. These discussions are too complex and lengthy for this forum, so we will leave that to our legal experts.

The bottom line for any security director to remember is that if an incident occurs, it will be used against you later. How you document that incident and how you react – to the point of making substantial changes to your Security – will be scrutinized. Incident documentation is presented later in this book, but the Security Plan is where we document the changes after an incident.

Specific Areas

While there will be a general security posture for the property as explained previously, there may be some exceptions. Areas behind the scenes or "back-of-the-house" may have less attractive barriers to protect valuables than those in view of guests. A motel in a high-crime neighborhood may use a walk-up window at night for check-in. Many newer luxury hotels have eliminated the check-in counter altogether. Guests at these resorts approach a kiosk for check-in and are helped face-to-face by a customer service representative who can provide a more physically engaging experience. You can imagine that this technique does not work for all hotels in all markets.

Deployment

Deployment includes where officers are needed, how many, and what their purpose is. Some hotels use the "shotgun" approach to staffing and deployment: Hire as many officers as the budget will allow and spread them around the property to provide as much visibility and coverage as possible. This approach is obviously lacking in efficiency or logic. Even if money is no object, the idea of providing security based on geography, rather than risk, may leave the property wasteful in one area and negligent in another.

For example, the retail area of a hotel property would need more of a physical presence during business hours than it does during times when the shops are closed. That is because the risks associated with a retail area change as the chance of robberies, shoplifting, violent crimes, and even accidents are reduced when customers are not present.

Similarly, the retail area may require less of a physical security presence than a nightclub when both are open for business. A nightclub generally has higher risk factors, such as intoxicated people, fights, and larger crowds. (The documented Risk Assessment for each area would exemplify and justify these variances in security posture.)

Waste would occur where officers are placed in these lower risk areas, especially where locked doors and gates or cameras might suffice. Negligence might apply when something happens in the nightclub and an officer is assigned to patrol other areas instead of the nightclub.

Using risk factors to determine staff deployment in the Security Plan is much more efficient, and easier to justify to management and lawyers. Other factors besides risk need to be considered in placing bodies around the property. Image, guest service, and other duties of the officers are explained next.

In a hotel/casino, security officers do most of the moving of money. This is generally not because of the risk associated with theft, but because most casino regulations require a department independent of the casino to be the third party in a transaction to avoid collusion. This goes against the popular belief that the casino places all its security officers around the cage and the pits for protection. The casino actually has much more to lose from a guest being robbed in its parking garage than it does with a theft from a blackjack table.

Upscale hotels do not earn their reputations lightly. These hotels, known for their high ratings, high-profile guests, and high prices might want smartly dressed officers in the lobby and porte-cochère as a visual comfort to their guests even though there is not necessarily any higher risk in these areas. This type of property is not only reducing physical risk and protecting its assets. It is also protecting the reputation and image in which it has invested so much.

Conversely, a smaller hotel with few staff members might have no visible security because they are not concerned as much with their aesthetic image. The security budgets are understandably smaller and it might assign its security to drive the company airport shuttle. Security does this function because they have a driver's license, can handle most off-property guest situations, and probably because they are the only employees not assigned to other duties. This is not an ideal use of Security, but sometimes it is a reality in the hospitality business.

These variables will have to be calculated into the Security Plan depending on the situation of the property and after the other risk factors have been addressed. To mitigate the risk factors into the Security Plan, take each area that was evaluated and decide if it needs an officer to mitigate it. The Risk Assessment in the preceding section was made either by area or by type of incident. Either way, the Security Plan is better segmented by area of the property. As each area is reviewed, determine if it needs a fixed post, if it is part of some type of patrol route, or if other tactics can be used to mitigate the risk.

Work Force

There is no widely accepted formula to calculate work force in a hotel. Various groups and individuals have tried to assign ratios, such as one officer per number of square feet, or per quantity of hotel rooms, or per amount of floors. This might work in a warehouse, factory, or office building, but not in a hotel. The variable is "people." It completely depends on the quantity and demographic of the guests, the neighborhood, and the region. A hotel attached to a theme park or a casino has entirely different staffing needs than a business hotel in a downtown city or in a rural agricultural community. It may be easier to determine staffing if you had a magic formula, but it would be more difficult to justify it later. This is why we did the Risk Assessment. The reality of a Security Plan is that you can justify and document all day long, but if your company does not allow that level of staffing, you will have to make due.

If you are having trouble justifying your staffing level, or you want to justify more, here are three suggestions for your overall staffing.

1. Hire as many as your budget will allow. If you already have an established staffing level and budget, you are unlikely to justify more. If you are starting with a new operation, check the properties around you or in your brand line and take the highest number.
2. Use your Security Plan. Add up your total posts and patrol areas figured into your security plan and hire enough to fill those positions. Do not forget breaks and supervisors. Also, consider how many you need to handle a major emergency like an evacuation. A large hotel needs several officers to clear all the rooms. Select the higher of this number and the number of posts.
3. Find an established precedent. Any hotel that has been sued for having inadequate security has had to justify their staffing numbers. This is not only a very accurate estimate, but is already proved in court to be adequate. If you have been through this, consider it the silver lining of all those deposition hours. If you have not been through it, find a similar property that has and compare those numbers.

It will be extremely difficult to decrease security staffing once you set your number. This is perceived as taking away protection from guests. This leaves your guests more vulnerable and you more liable. If you have to reduce staffing, take the staff away from noncritical areas such as supervision, administrative duties, or merchandise protection.

In 2005, a man walked into a shopping mall wearing a trench coat with a rifle and pistol underneath. He called 911 and told the operator he was about to commence shooting. He shot seven people and took four as hostages before being taken into police custody. One of the victim's families sued the mall for inadequate security. The plaintiff argued that the mall did not take even the most basic steps to protect its patrons—armed security or off-duty police, tracking of past crimes, public address system, and coordination with police to prevent attacks. The mall owners argued that the incident was not foreseeable and, therefore, not preventable. The court sided with the plaintiff that the incident was foreseeable and the mall should have implemented procedures such as those argued above.

Combining Layers

Other ways to secure an area or reduce risk involve the use of hardware or some type of equipment, such as cameras or locks. In some ways, hardware—or technology—offers a better and cheaper option for a layer of security. Locks, doors, and fences are generally infallible and cannot be distracted or overwhelmed. They also do not offer any subjectivity, which makes humans the better choice in some instances. However, humans cost more and have to have days off, lunch breaks, and insurance benefits.

Fixed posts, regular patrol, and security systems are most often combined to provide the most secure environment. It is the security director's responsibility to determine the best combination and application to reduce risk in each area. The director's experience, education, and training come into play here, but here are some basics that anyone can follow in securing an area in the most efficient and effective way possible.

Begin with the easiest and cheapest method of security possible. Then add layers until the risk has been mitigated. As you evaluate each risk, decide which security measure will most effectively and inexpensively prevent it. That may include a combination of measures or multiple layers such as a lock and an alarm, or prickly shrubs and a camera. This requires knowledge of those measures and layers and the experience of knowing what works and what does not. Do not hesitate to consult with an expert if you are not sure about whether it will work. You will find some good suggestions of what works throughout this book.

Using the standard hotel room as an example, the first layer of security is the lock on the door. In the old days, this was the Security Plan and you would be finished. As we figured out that keys could be lost, stolen, or duplicated, another layer was added. The key lock was replaced with a magnetic key lock and most of those issues were alleviated. Dead bolts and secondary door locks were added so guests would feel safe from the intruding housekeeper or technologically advanced burglar. For most hotels, the Security Plan is finished with the door locks. If the Risk Assessment includes the chance of robbery or room invasion, the next cheapest security method is the peephole. There is still the risk of door pushers, stalking crimes, and other violent acts, so it may be necessary to add cameras in the hallways or elevators. The final layer to add is physical patrol. Adding layers to physical patrol is achieved by increasing the frequency all the way up to a standing post.

Summary

The Security Plan is a justification for your policies, deployment, staffing, and all the neat gadgets you have acquired. You may never need to justify these to anyone, but you need to be prepared to explain why you spent this much money protecting this and that much money protecting that. The Security Plan keeps this process objective. For example, 20 years ago cameras were installed in elevators. That was seven directors ago and now your new hotel manager wants to know why we are spying on people in elevators. A Security Plan would explain to you and your new boss that a sexual assault in an elevator cost the hotel $750,000 to settle.

You also may find yourself on the witness stand trying to explain why the previous security director did not put a lock on the fitness center when it was built last year and a hotel guest was robbed. This is why you want to update your Risk Assessment and your Security Plan often and especially when you take over the responsibility for each. Each time you make a change to your plan—adding cameras, reducing workers, remodeling the nightclub—consider how it will affect your liability. Ask yourself if you will be able to justify this change to your boss, to a jury, or to your successor if something goes wrong.

The format of the plan is not as important as the content. If you are not sure of your format, use the previously mentioned outline or the one for the Security manual in this book. As long as you can read it and use it to provide your justification, you will be fine.

You need to keep current on new technology, current events, industry standards, and market practices. This knowledge is needed to keep your Security Plan current. (See Chapter 12 on career improvement.) At the very least, subscribe to magazines and newsletters that provide this information to you. Track cases and case law on matters of security and hospitality. Attend as many local and national seminars and organizations as you can. As I mention many times in this book, you need to be the subject matter expert on hospitality security to adequately protect your business.

SPECIALIZED PATROL

There is an entire chapter (Chapter 8) devoted to patrol techniques and types, but the programs that follow are important enough to change your entire Security Plan, so they are included here.

Armed Security

Most advocates for armed security will tell you that an unarmed security guard is about as effective as a doorstop against an armed assailant. Opponents of "guards with guns" will argue that the cost and liability of carrying guns is just too great. Although I am one of the advocates, I agree that guns have their limitations. I think I can present this program to you in a way in which you might agree.

Management Buy-In

The decision to arm security officers is usually way above the director's pay grade. If you want to issue guns, you will need buy-in from the executives (the general manager [GM] or owner) and their legal counsel. As soon as you mention it, images of Barney Fife—the incompetent TV deputy played by Don Knotts on *The Andy Griffith Show* who was not trusted with bullets for his duty weapon—and little old ladies with bullet holes lying in your hotel lobby will come to mind. This is not a good starting place, so instead of starting at the bottom, let's come in from the top.

Your Risk Assessment should have identified the need for armed security. You may be located in an urban area that experiences armed robberies, gang shootings, homicides, and other violent crimes. You may have even had some incidents on your property with guns, knives, or other dangerous weapons. Your hotel may have been identified as a piece of critical infrastructure and is therefore a target for terrorism. Finally, the prevalence of active shooter incidents from disgruntled workers or domestic violence in the workplace has likely come very close to your property.

These incidents, including any others, such as police chases through your property, law enforcement warrant service, or felony traffic stops in and around your hotel should be documented. Just as you did for the Risk Assessment, keep a running tally of these occurrences and be prepared to use them to justify guns both before and after the program is in place. Next, compile some lawsuit data.

Many security law publications do this for you. Alternatively, you can do a Web search for accidental shootings by security officers, negligent training security, security shot bystander, security shot suspect, etc. Find every lawsuit you can for the past 10 years that shows guns, good or bad, in the hands of Security. One more thing to research: employees (guards) who have sued their employer for not providing the proper equipment to save their own life. I can think of a couple of world famous headlines where Security was sued for not taking action because they lacked the proper tools. Then there is the guest who could probably prove that a gunman in your hotel was foreseeable and that your security was inadequate because you had no armed personnel to mitigate the threat.

All of this data and anecdotes make a great presentation, but the GM still has that vision of Barney Fife. You need to dispel this image by presenting a quality training and firearms program. It cannot hurt to show some examples of successful (no bad shots fired) armed security programs in your area or at least in hotels similar to yours. Your objective, like any other proposal, will be to show how the positives outweigh the negatives. So, before you make that presentation, let's work through the cons and turn them into pros.

Policy

Usually, when I am asked for advice on starting an armed security program, the questions are about training and bullet strength. Unfortunately, it is not that simple. Way before we get to that, we have to develop a firearms policy. Your policy will protect you, your employees, and your company from those bad things in your lawyer's head. The policy covers the rules involved with purchasing, storing, maintaining, loading, carrying, pointing, shooting, and reporting (the use of) a firearm. You cannot establish your training program until you work out the parameters involved in those aspects of the program. This book is not going to cover everything you need to know, but here are some things to consider.

Hiring—As you hire new officers, you should assume that they will be armed at some point. This may change the questions you ask, the experience you seek, and the background check that you perform. It is more difficult to switch from unarmed to armed officers because you were not considering this when hiring your current staff.

Armed officers—There are many arguments on whether to arm officers indoors. Many properties choose to arm only those officers who patrol outdoors or supervisors and managers. A firearm in a crowded nightclub may actually do more harm than good—unless you are faced with somebody shooting at you. Arming officers who only work outside may be a good way to get management comfortable with the idea.

Open carry—The decision to carry weapons openly on a uniform or to conceal them under a blazer is entirely dependent on your Security Posture (discussed earlier in this chapter). One is a deterrent and reactive and the other is only reactive. There also will be considerations of permits and governmental regulations for carrying.

Use of force—You should already have a use of force policy that specifically justifies what level of force to use depending on the force presented by a suspect. This policy is used to justify your actions and protect you and your officers, but also to enforce the policy. Those officers who abuse their ability to carry a deadly weapon are dealt with swiftly and severely.

Use of force continuum—This is discussed in more detail in Chapter 6, but an important consideration is "use of force options." If you provide firearms and nothing else, you may be negligent in not providing some less-than-lethal force option as an intermediary to avoid unnecessary use of deadly force.

Pay differential—You may want to pay armed officers a bit more than their unarmed counterparts. This not only recognizes their additional training and experience level, but also shows them, and possibly a court, that you take this program seriously. Whereas some "guard" companies just throw a gun on their hip and go out, hoping for the best, your company provides quality training of quality officers who receive a reasonable pay.

Equipment—You have probably seen security companies that allow officers to bring their own weapons, holster, and leather gear, with any type of ammunition and style and caliber of gun. It creates a bad image to have a bunch of "cowboys" or "hired guns" protecting your assets. Take time to research and invest in quality equipment that is consistent, maintained by the company, issued in a proper fashion, and carried like a professional.

Training

Training is absolutely the most important part of this program. It is difficult to decide how to start. I have two suggestions. One is to certify an in-house instructor (or two) with the National Rifle Association (NRA) or other qualified firearms trainer. These schools, usually a week long, teach everything from tactics to policy to instructional methods. Do not just pick the employee who grew up with hunting rifles or used to be a police officer. A qualified trainer, combined with firearms aptitude and devotion to the company, is best.

The second suggestion is to connect with local law enforcement trainers. They are definitely qualified, but you may have to remind them that your rules of engagement are different from a police officer's rules. Where the police may draw their weapons on any felony suspect, our policy is likely something like "only in the defense of our life." (This is only an example—policies vary.)

Once you have the policies and the trainer in place, you will need a training program. Look to other companies and your local police departments for guidance on what your program will look like. Even though you may think you don't have the time and budget to copy a police program, you may be surprised how little time they spend on firearms training. Devoting the same time and money to your program as the local police or a local "competitor" looks very good for you. Remember that if you are sued for a shooting, the amount of training and the quality of your program will be scrutinized.

Make sure your training program includes the following components: relevant laws associated with firearms, use of force policy, operation and basic functions of all types of firearms, firearm malfunctions, loading and unloading, near and distant shooting, tactics, stance, intuitive decision-making skills, tactical loading, range safety, and much more.

Discipline/Enforcement

How you enforce the policies for firearms is very important to the integrity of the program. Allowing officers to use poor judgment in drawing their weapons will diminish the perception of your level of competency. Those who violate these policies need to be held strictly accountable. A review and reporting process for any firearms or use of force related incident is vital. Once you allow someone to blur the boundaries or make a mistake, your firearms program is threatened.

The reality is regardless of what preconceived notions your lawyer and GM may have, Security Departments that deploy armed officers do not engage in random, accidental, or reckless use of firearms. If they did, they would not stay armed and you would not even consider it. Accidental or unlawful shootings by trained security officers are so rare that there is no trend or pattern that could lead anyone to prove otherwise. It is much easier to show where armed officers have saved lives, prevented crime, and kept many properties safe.

Nonlethal Weapons

In 2003, security officers used pepper spray to subdue a fight at a Chicago nightclub. The aerosol spray spread throughout the club causing minor irritations and vomiting for some customers. A panic stampede resulted from most of the 1,500 guests not knowing what the odor was; many assumed it was a poison terror attack. The only exit used was the front doors, which opened inward, then led to a steep flight of stairs down. Twenty-one people died and the club owners received prison sentences for code violations.

Doors opening inward and stairs leading directly to a door are fire code violations and an unsafe practice. Pepper spray in its aerosol form is not advisable indoors and, in this case, turned a nonlethal weapon into a deadly one.

I mentioned nonlethal weapons in the “Armed Security” section and they are justified in Chapter 6. If you do decide to deploy an intermediate weapon to avoid deadly force, there are options.

Taser®

The Taser is a revolutionary device that emits projectiles that apply a high-voltage electric charge to a suspect. The charge contracts muscles and usually incapacitates an aggressor. This weapon is very controversial and is under enormous legal scrutiny. In my personal opinion, the problem with the Taser is not its function, but in its application. Many police departments have failed to properly place this device on their use of force continuum and even when they do so, they fail to enforce its correct usage. We have all seen this device used as a *first* resort or in an inappropriate situation. Most police departments have a limit on how much they have to pay in a lawsuit, but private corporations do not.

If you have a hard time selling firearms to your executive team, it will be impossible to sell the Taser. Just to be clear, I think this is a great device and very effective when used correctly, but until the tendency for every “victim” of its use to sue goes away, it will not be in your financial interest to use it.

Baton/Impact Weapons

Like the Taser, batons have taken a beating in the courts due to their misuse. Baton training was always of a defensive nature, but Rodney King-type situations have left the legal perception that it is offensive. If you use a baton, and there is a death due to a blow to the head or vital organ, your defense will be expensive.

Other impact weapons include asps, saps, straight sticks, kubutons, and any other device used to strike or apply pressure to a combatant. When used correctly, these can be amazing instruments with very effective techniques. Unfortunately, a serious injury from a stick will just produce dollar signs for most plaintiff lawyers.

Pepper Spray/OC

Oleoresin capsicum (OC) is an oil-based organic substance derived from hot peppers. It is designed to burn and distract the combatant to the point that he or she cannot focus on the offense. Several years ago, it replaced tear gas and MACE as the preferred chemical irritant for most police and security departments. Most police officers will use the aerosol form of OC because it quickly affects the lungs and eyes of assailants, incapacitating them faster. Unfortunately, aerosol also affects others nearby including the officer. See the accompanying textbox on previous page.

Pepper Stream was developed to avoid the problems associated with aerosol, but it also splatters and does not affect the assailant as severely. Pepper Foam is relatively new. It hardly splatters and remains on the skin longer, but does not affect the lungs and eyes as much. However, in my experience, it is quite effective. The downfall of OC is that it does not affect everyone the same and some not at all. The positive is that there has never been a death directly associated with its use and the effects wear off.

Like everything else we talk about in this book, we have to look at weapons not just for their effectiveness, but also from a liability standpoint. The best device to protect our guests and ourselves may not be the best to protect our assets. Choose your not-so-lethal weapons wisely.

Dispatch

To some properties, Dispatch is a function of communication, to others it is a room where systems are monitored, and to the rest of us it may be a method of gathering and documenting activities. Call it a Dispatch Office, a Command or Control Center, an Operations Center, or whatever. The function should be all of the above.

Communication

Dispatch, in this sense, is just like a police department or a taxi service. Calls are received, prioritized, and dispatched to your officers. In smaller facilities, your hotel phone operators or front desk personnel may do this. A large property may have several persons devoted to the dispatch function. This becomes a highly specialized function, requiring advanced training and above-average intelligence. Many hotels and tourist venues provide training similar to 911 centers to do telephonic medical triage, phone etiquette, radio procedures and language, hostility de-escalation, and more. On top of all this, we often ask them to handle housekeeping or engineering calls as well as the functions listed next. Training and experience are highly encouraged for this position, as it is an expectation of service from your responding agencies as well as your guests.

System Monitoring

Because Dispatch is usually a constantly staffed, isolated room, it is the perfect place to monitor video systems, fire alarms, panic and intrusion alarms, access control systems, and even facility monitoring (HVAC, boilers, etc.). Some of these functions are explained in more detail in Chapter 9.

Documentation

What better position to log all of our activities than the dispatcher? While you are answering routine and emergency phone calls, dispatching a dozen officers, watching 20 television screens, and answering alarms, why not write all of this stuff down for us? There are computer-aided dispatch systems that make this job a bit easier, but it is still a huge task, although a vital one for your department.

VIP Protection

As a proprietary Security Department, protecting celebrities, politicians, and executives hardly falls into the mission of protecting the company's assets. However, we all know that these individuals show up, sometimes announced, sometimes not, sometimes prepared with Security, sometimes not. Whichever way they present themselves to you, their presence will definitely disrupt your business and create a threat in one way or another. So, on occasion it may become your duty to protect these people from themselves and from others.

In most cases, your department will be one layer of security (such as with the president). On the other hand, you may be the proprietary source of information to the personal team that needs to get around the property easily. With some would-be celebrities or newsmakers, they may not bring their own staff, which puts you on the spot. Finally, some security staff or bodyguards may be your biggest threat.

Planning for this event is straightforward—if you are the one doing it. If you were planning it, you would first conduct a Risk Assessment. List the possible threats and their likelihood. Then create a Security Plan. Document how each threat is mitigated. This is also called an Incident Action Plan. Then you have to arrange these plans, such as crowd control for celebrities, personal protection for a rich executive (and his or her family), and so forth. It is helpful to have a small group of officers or managers go through some sort of executive protection training to provide expertise in these situations. You also can contract this service to professionals.

As with the president or a very famous person, he or she will have his or her own security and only need you to assist with access and travel through the property. In this case, assign a liaison from your staff to theirs to help this process run smoothly. Remember for whom you work. Your mission is to protect your company. The best way to do that is to collaborate with these people, as a negative incident on your property is not good for business.

Special Events

Just about any event that is not normal for your property, or that disrupts your regular business, is a special event. These also require an Incident Action Plan (Chapter 4) and some special policies and procedures. Crowd control, access control, evacuation routes, and other procedures not normal to your operation need to be addressed in the plan.

How many officers you will require, what they do for certain emergencies, will you search attendees, and many other issues need to be addressed in the Plan.

MEDICAL PROGRAM

Defibrillators

It was said at the turn of this century that you were safer in a Las Vegas casino than anywhere else if you were going to have a heart attack. Automatic external defibrillators (AED) used to be reserved for larger properties with highly trained security departments. Any property that has them has probably seen them not only used, but also used successfully to save lives. Ironically, most properties use AEDs more than they use fire extinguishers. Like most technology, they are now cheaper, easier to use, and more prevalent. This does not negate the need for a robust policy and training program for their use.

Defibrillators are a portable, battery-operated diagnostic heart monitor that measures heart rhythm and automatically delivers a shock if it detects the need for one. The user needs only to turn it on and connect it properly. AEDs also include audio recording, voice prompts, and other features. Just because technology has made them easier to use does not mean that you can just buy a couple and stand by to save lives. Just as you would not buy guns and pass them around to your officers without training and a strict use policy, you cannot do this with AEDs. A program is absolutely required before, during, and after being equipped with these units.

Justification

If you do not have AEDs, get them tomorrow. There is no acceptable reason not to have them these days. Serious brain injury occurs after four minutes of a stopped heart. Moreover, even if you live across the street from a hospital, the only way to get a shock to the heart in four minutes is to have an AED within two minutes of every person in your facility. When you are sued for not having AEDs, and you will be, what excuse will you give for not having them? Cost? Convenience? Time? There is no excuse.

Medical Sponsor

Many large hotel chains contract with a heart physician to oversee their AED program. This doctor, who must practice and maintain his or her education in cardiac and emergency medicine, advises on policy and training and reviews each incident where the AED was connected to a person. For a stand-alone hotel, you may be able to do this on a per diem basis with a local physician. The local ambulance company, fire department, and even the health department in your area may provide this service as well.

Training

To protect your liability, training should be done with a certified AED/CPR (cardiopulmonary resuscitation) trainer from a reputable organization. There are nonprofit associations that provide this training and can train trainers to lessen costs. Most training sessions for first responders are approximately eight hours and include CPR, basic emergency aid, and AED use. If you have read any part of this book, you know I am going to recommend every security officer have this training. The last thing you want is to have your one or two trained officers busy when the call comes out for a cardiac arrest. Try explaining that to a jury.

If you have a small security department, you may want to train other employees on your property that are mobile and easily deployed in the event of a medical emergency. This would include any department with radios.

Policy

This policy saves lives, but can also cost lives if not implemented and followed properly. Training is most important. Next is a policy requiring when the AED unit is dispatched to a medical call. You need to decide if you will bring it to calls of a sleeper, no-answer-to-knock calls, check-the-welfare calls, etc. Since we are not doctors, or even paramedics (in most cases), who are we to decide if the AED is needed at each particular medical call? As soon as a person is suspected of being unresponsive, or worse, the AED should be automatically sent. This is usually by the second officer (if there are two or more) or by the first if there is only one. This allows the closest officer to get on scene, perform a quick assessment, and start CPR if necessary. It would be an unfortunate mistake if the security officer assumed someone was just sleeping, fainted, faking, or otherwise and it turned out to be a fatal incident. Better to bring it each time and not use it.

A hotel in Nevada wisely deployed defibrillators and trained each officer on their proper use. This program was quite successful and saved several lives. However, in one incident, caught entirely on video, a man was found unconscious in the lobby. The first officer responded in seconds, but did not bring the defibrillator (AED) as trained. The second and third officers also responded very quickly and did not bring the defibrillator. The supervisor arrived, also with no AED. The officers could detect no heartbeat but heard gurgling so they assumed the man was breathing. An ambulance was called and paramedics were on scene eight minutes after the man went down. They immediately deployed their defibrillator, which malfunctioned.

The supervisor called for the hotel's AED and the man was revived after being shocked by the AED. The man survived but his family sued, as he did not fully recover from the brain damage. In court, the family subpoenaed video and reports from seven other incidents where the first officer to the scene brought the AED. They also showed the hotel's training program, which mandated the AED be brought to every medical call. The hotel claimed that they thought the man was just drunk and unresponsive because they heard him gurgling. As you guessed, the hotel took a serious hit because the training was not consistently applied.

In this case, the hotel had AEDs, had a policy to bring them, and violated their own policy. It was easy for the plaintiff to prove that they contributed to the man's ill health.

You should also have very strict policies on inspection and testing of the units and their associated equipment, changing of the batteries, storage area access, security, etc.

Storage and Access

You have seen AEDs in shopping centers and airports mounted very conspicuously for everyone to see and use. Other places, such as casinos, keep them behind the scenes. The difference is usually the size of the security force. A smaller staff will rely on other employees or even guests to retrieve the AED and use it or to get it for the single security officer that may show up. Casinos and other large businesses use more expensive and advanced units and prefer to keep them safely stowed away, but in convenient locations. However you decide to do it, make sure they are accessible regardless of the crowd you have and that they are placed conveniently for an officer to grab quickly.

It is not necessary to have them spread throughout a hotel tower. If you are going to have the second responder obtain the AED, then he or she is most likely coming from someplace other than the tower. The lobby, bell desk, or adjacent area is a wiser choice.

If you have a smaller security staff, you may need to train employees from other departments on how to use the AED.

Follow-Up

After an AED incident, it is advisable to have a review by your medical sponsor. Using the recording and data stored in the unit, he or she can evaluate the performance of the officers and provide constructive feedback as to where they can improve and what they did well. Regular training drills and this type of feedback will make this process much less stressful and more successful. There is nothing more rewarding than saving someone's life in this manner.

Medical Calls

Accidents and illnesses are certainly the most common types of calls in a tourist-based business. The policy for medical calls is property-wide and requires training, or at least an awareness, of all employees. Every employee needs to know that Security is the first responder so all calls that are related to a medical problem are routed to security. Perhaps the hotel operator will call local paramedics if there is no full-time Security Department. On the other hand, the front desk personnel could do this.

The hotel operators will receive most calls from guests for medical assistance. They need to have the most basic training: location and type of problem. Security is on the way. Then they transfer the call to Security, staying on the line to ensure the call goes through. There are three stages in this process for when Security should call an ambulance (or whoever provides your emergency medical services [EMS]).

1. If the guest asks for an ambulance, do not question it. Call the ambulance. It is okay to obtain information, but do not delay or deny EMS.

2. After the dispatcher takes basic information, he or she will have to make a decision to call paramedics and send Security.
3. Send officers to the scene to make a decision.

Determining when to call paramedics is very easy. If they are conscious, ask them. Would you like an ambulance? No? How may we help you? If they are unconscious, call the paramedics—every time. Varying from this policy will open your company to great liability.

Medical Personnel

In the old days, fancy hotels had a "house doctor" on staff that would help sick guests. We have come a long way from that luxury, partly due to economics and malpractice insurance, and mainly due to advances in emergency medicine and "911." In fact, in the 1990s many large hotels hired and trained Emergency Medical Technicians (EMTs) or registered nurses to provide an increased level of service for guests. The theory was that this would be an added layer of safety for guests. What happened was EMTs and nurses were expected to diagnose medical problems and save a trip to the hospital. You can imagine an EMT telling a guest with a bad headache that they need to take aspirin and rest, and then the guest turns out to have a stroke or a tumor. That only needs to happen once for a hotel to think twice about those EMTs. In an effort to save the EMTs, we ended up sending them *and* the outside agency to every call. It was soon declared redundant and a waste of money, so most hotels discontinued their medical programs.

Almost every city in the world has some sort of emergency response network that sends specially trained personnel with special equipment to deal with almost every situation. What that means to a modern hotel facility is that we have become the intermediary between the guest and this public service. Our service, therefore, is one of stabilizing and relaying information to the authorities. The expectation of service has even risen above that which we would receive in our own homes if we had a heart attack.

Whether or not you agree with it, we have to meet these expectations by providing at least that level of service for which we can reasonably train security officers. AEDs, for example (discussed in the next section), allow a superficially trained person to shock a heart back to life. As these advances become more prevalent, such as an automatic baby deliverer or brain surgeon, perhaps we will be expected to provide those services as well. Until then, we will provide that which is expected and keep our eye on the next technology and adjust accordingly.

In 2010, we have evolved (backward) to providing basic first aid care. We can respond quickly, assess the situation, and relay that information to the responding agency. Our training is limited to CPR, AED, and stabilizing shock. Let me be clear on this: You still need to designate a 24-hour team (Security) to respond to medical calls. They still need to have at least basic first aid training and CPR. This training may have to be more advanced if you are located in a rural area where paramedic response is farther away.

As with every policy introduced in this book, place yourself on a witness stand trying to explain why you did not train your officers to do CPR. There is no right answer.

Medical Equipment

Equipment is needed corresponding to the level of training. If you are training in CPR and AED, you will need oxygen and associated canulas, breather masks, and regulators. First aid supplies may include bandages, eyewash, thermal blankets, etc. This equipment needs to be stored in a central location depending on the layout of the property. A suitable bag or case should be issued to transport the items to the scene. You should also consider one or more wheelchairs to move sick persons to a taxi, intoxicated individuals back to their rooms, etc.

Inspections and stocking of the above items is just as important as having them. When one item is used, it must be replaced. I suggest keeping a stock of all items in a closet somewhere and inspecting the medical bag every shift or daily to make sure items were replaced.

ANTITERRORISM

Hotels have been soft targets for terrorism for years before 9/11. 9/11 brought the idea home to us here in the United States that it could actually happen here. Hotels are considered "soft" because they are not hardened to intrusion. By their nature, they are open to the public and have very little access control. They are "targets" because they offer the opportunity to provide mass casualties, visually dramatic destruction, economic impact, and iconic news coverage.

The good news is that 9/11 raised awareness and concern (and spending) on counterterrorism. Unfortunately, we are taking too long (over 10 years now) to get to the level of protection we need to reach. The federal government—and by grants, local and state governments—is spending huge amounts of money on developing plans and buying equipment that is not following any specific strategy or purpose. For example, following 9/11, we knew that radio communications between agencies was nonexistent. In 10 years, very few agencies have resolved this issue. This is not meant to be critical of the government, because they have thwarted and prevented many major attacks on the United States and should be recognized for such. It is to say that as private entities, we have some, if not most, of the burden of making our properties hardened to this threat.

We are not the government, and do not get much of the funding described previously, so we have to do what is best for our guests and us. We have to balance our risks—all of them—with our budget and practicality. We have to be smarter rather than harder. Therefore, I will not be recommending any of those cool automatic bollards or x-ray cameras. I will review some effective and simple countermeasures we can use to prevent terrorism. The best way to do that is to understand first what terrorism is, and then how we can prevent it.

The FBI defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives." You can argue with that definition that gang activity is terrorism. For the sake of this section, we will focus on al-Qaeda and others who have designs to attack targets in the West and any that may suit their designs. For the sake of prevention and behavioral recognition, these terrorists do not choose their target based on personal reasons or monetary gain. We know from previous incidents that they choose a target based on high media value (popular place), symbolism (e.g., World Trade Center), or high body count (which would include hotels).

Just like criminal networks, terrorists operate in organized or solo ways. The "lone wolf" is a radicalized individual who is moved to militancy because of extreme ideology or political views. Timothy McVeigh and Charles Manson were lone wolves. (Manson was a lone wolf who successfully created his own terror network.) Groups of terrorists are called "cells," which operate within either highly structured or loose organizations. There are active cells, fringe cells, and sleeper cells. Because Muslim terrorist groups think of their Jihad as a long-term war, there may be sleeper or fringe cells anywhere that can activate at any time. Authorities have been successful routing out some of these groups, but there is no way of knowing how many there are or where they are hiding, which is likely in plain sight.

According to the U.S. Department of Homeland Security (DHS), al-Qaeda leaders have called for Westerners to conduct simple, small-scale attacks against familiar targets that do not require extensive funding, support, or training. In recent years, we have seen numerous attempts foiled by the FBI and there is no reason to think that terrorists will not continue to learn and alter their strategy based on these arrests. Terrorist groups are very structured in their ability to compartmentalize plans and missions while using technology like the Internet to communicate and train.

Attacks in other countries and attempted attacks on U.S. soil usually include bombs (improvised explosive devices—IEDs), but some—like in Mumbai, India—combined bombs with small arms fire. Our government authorities and oversees hotel colleagues have learned a great deal from these attacks and we have the good fortune of being able to learn and plan based on this intelligence. Here are some recent incidents involving hotels.

In January 2008, several men lobbed grenades at security guards at the access gates of a luxury hotel in Kabul, Afghanistan. Once they made entry to the fortified hotel, one man activated a suicide bomb. Six were killed, mostly security and staff. The terrorists were disguised as local police to get close to the gates and guards.

A truck filled with explosives approached the front gate of a Western luxury hotel in Islamabad, Pakistan, in September 2008. The driver exchanged gunfire with gate guards and then detonated the explosives. The explosion and ensuing natural gas leak and fire destroyed most of the hotel, killing 60 people, and injuring 250. It was believed that the lone terrorist was targeting a group of U.S. marines who were staying in the hotel.

In November 2008, 10 heavily armed men, operating simultaneously in teams of two, attacked several targets in Mumbai, India. They entered the rear of the hotel—with help from employees—while detonating IEDs at the entrances of the two hotels to prevent first responders from entering. IEDs also were detonated in taxis around the city to distract and deter police. The gunmen took hostages in the hotels and engaged first responders with guns and IEDs, which set the building on fire. The incident lasted 3 days and at least 173 died.

A car filled with gunmen exchanged small arms fire with gate guards at another luxury hotel in Peshawar, Pakistan, in June 2009. They forced their way through a gate and detonated a car bomb near the hotel, which killed 7 and wounded approximately 40.

In July 2009, bombs ripped through two iconic hotels in Jakarta, Indonesia. They were detonated five minutes apart, killing 7 and wounding approximately 50. After an unexploded bomb was found in a hotel room, it was determined that it was intended to activate first, causing guests to flee toward the lobby where that blast would have caused more fatalities. This is referred to as a "secondary explosion" and is intended to exploit panic resulting from a primary explosion.

Four Baghdad, Iraq, hotels were targeted in simultaneous attacks in June 2010. Each of the attacks involved explosives that killed 36 people and caused extensive damage to each hotel. Witnesses reported one of the vehicles containing a bomb was disguised to look like an emergency vehicle with flashing red lights.

In Mogadishu, four men disguised as government security forces shot their way through security in August 2010. Most members of the Somali parliament who were at the hotel for a conference were shot and killed.

On June 28, 2011, nine assailants armed with automatic weapons, rocket-propelled grenades, and explosives attacked the Intercontinental Hotel in Kabul, Afghanistan at 10:30 p.m. The attack began with a suicide bombing at a side entrance, which allowed other assailants to avoid heavier security at the main entrance. Once inside, the assailants killed as many guests and employees as possible. As NATO-led forces arrived, the attackers fled to the roof where some detonated their suicide vests and military personnel in helicopters killed others. The siege ended at 3 a.m., but one terrorist hid in the building until 8 a.m. when he detonated his vest, killing two police officers and a civilian. In all, 20 people were killed and approximately 18 were injured. The Taliban claimed responsibility for this attack and has vowed to carry out similar attacks in the West.

These attacks were carried out overseas and we have no reason to believe these types of attacks could occur on U.S. soil. Or do we? We had the same outlook before the World Trade Center Bombing (and soon after it). Let's take advantage of the information we have and take the simple steps to harden and prevent *before* something happens instead of afterward.

Note that the bombings and shootings mentioned previously all occurred in the past few years, post-9/11, and each of the properties had hardened themselves to prevent those types of incidents. That hardening had varying levels of success depending on the intelligence done by the terrorists, their financial and physical capabilities, and the personnel resources available to them. Some were military or government-backed and many used "inside" personnel. Most hotel security directors overseas will tell you that hiring is their biggest problem. Determining and relying on the loyalty of security officers hired locally when faced with a fellow citizen with a gun or bomb is a risky proposition.

In the United States, we are fortunate that we do not have this problem to the same extent, but we still need to make sure our background and hiring processes are consistently strong. Once hired, it is important to have an employee awareness program. Many corporations and hotels in our industry have adopted the federal government's "See Something, Say Something" program. This is a very simple program because it quite succinctly reminds the employee to report suspicious activity to a supervisor or security. DHS has videos available to show your employees in each department what they should be looking for. These are free or you can buy them from various companies. Following is a list of indicators that may indicate suspicious behavior. This list should be incorporated in training for security and other employees.

- Front desk
  - Using false ID or no ID at check-in
  - Requests for anonymity on registration
  - Paying for room with cash
  - Using someone else's credit card
  - Third-party registration
  - Extending stay one day at a time
  - Requests for specific room, floor, or view
- Housekeeping
  - Refusal of service for long periods
  - Little or no luggage in room
  - Renting room, but not using it
  - Leaving all belongings in room upon check-out
  - Multiple visitors or deliveries to room
- Security
  - Attempt to access employee areas
  - Unusual interest in hotel security, access, cameras, stairwells, etc.
  - Use of alternate entrance and exits to avoid being seen
  - Not following hotel policies
  - Unusual interest in staff shift change, operating procedures, etc.

Other target-hardening measures will depend on your risk assessment and your location. I would not expect a hotel in the Midwest to be as heavily hardened as a hotel in New York City. You will have to decide, based on cost and feasibility, which, if any, of these procedures and equipment you want to acquire.

Standoff

Standoff distances for hotels vary between extremes. At a minimum, there should be some sort of bollards blocking runaway vehicles from entering doors and windows. Valet concourses built before 9/11 were designed for door-to-door convenience, but new construction since then has blocked or removed the traffic lane that is closest to the building.

Generally, hotels will back off traffic as far from the building as possible without making it too inconvenient for guests. Bollards in a hotel setting need to be decorative, so a popular choice is a big flowerpot. These likely will only stop a slow-moving car. Rather than purchase the expensive, in-ground bollards, I suggest using a wedge-shaped pot or planter. When these are tipped over, they create a wedge that brings any size vehicle up off its front wheels.

Metal Detectors

Metal detectors are contrary to the hotel business and I would not use them unless there was a specific threat. Bag searches may be a more friendly option if you find searches necessary.

X-Ray Luggage

After 9/11, many hotels started using x-ray machines for luggage that went through the main entrance. These machines are very expensive to maintain, they break down a lot, and they are not foolproof as TSA (Transportation Security Administration) has reminded us.

Bomb Dogs

Several hotels throughout the United States have sniffer dogs. This is a large expense and is not practical for 24-hour operation. Hotels that have them use them for random patrol, for investigating suspicious packages, and for a visible presence.

Countersurveillance

Part of the countersurveillance process includes behavioral recognition (discussed in Chapter 8). The other component involves assigning an investigator to inspect the property on a regular basis to identify those who may be gathering information on the property. Their other function is to identify vulnerabilities from the terrorist's point of view. If you send someone out to try to "break" your defenses, he or she will find vulnerabilities for which modifications can be recommended.

Video Surveillance

Your digital video system should have analytics that can be used for counterterrorism. Your system should be able to "see" packages or bags left unattended, persons in unauthorized areas, license plate recognition, facial recognition, and many other bells and whistles.

Many other counterterrorism procedures and agencies can help with this process. DHS offers free site inspections and can make recommendations on your vulnerabilities and mitigation suggestions.

DOMESTIC TERRORISM

The previous section was mostly geared toward traditional Islamic terrorism. We must not forget that the United States and other Western countries have their own domestic terrorists. Their goals are generally the same: death and destruction to bring attention to their cause. There are known cases of environmentalist, animal rights, antiabortion, and White supremacist groups that have bombed buildings, assassinated executives, and set fire to structures to raise awareness for their "cause." For our purposes, most of the measures in the last section still apply, but generally, these groups have specific targets. Intelligence and research are the keys to prevent being a target of these groups. For a hospitality venue, we need to watch what groups rent our meeting space, what executives or dignitaries visit our guest rooms, and what vendors with which we do business.

Keep an eye on your Sales and Convention departments and make sure they inform you of every group coming on property. A simple Internet search can answer most of your questions, or at least cause you to make the appropriate alarm. You are not looking out for just the initiators of violence, but also the potential victims of it. For example, a hunting group may be targeted by an animal rights organization, or an obstetrician symposium may be attacked by an antiabortion group. Besides violence and property destruction, the last thing you want is a protest on your sidewalk by one of these groups.

DATA SECURITY

This book is primarily about physical security, but we cannot ignore the convergence with data security. Those of you who deal with this collaboration might not describe it as such. These days, trying to run physical security without IT (information technology) support is like trying to be captain of a ship without an engine room. Some companies have figured this out and they put that captain in charge of his or her own engine room. Others have IT and Physical Security report to the same person. Still others are trying to work together, but with entirely different operations and agendas.

I suspect most hotels operate like the latter because they have not quite accepted that IT flows through every department and all aspects of the operation. In Security, that flow is through alarms, access control, video, reports and admin functions, and even patrol systems. Physical Security is using more "bandwidth" and more "systems" than ever before. Convergence has been the term used in most security circles to describe the new relationship between these two entities. If you have ever had any drug recognition training, you know that convergence means two eyes working together to focus on one target. If that is true, then we don't have to look at IT as a threat or an intruder in our world, but one with whom we can collaborate to achieve a common goal. After all, one eye without the other cannot perceive depth.

Several years ago, I was embarking on a project to switch from analog to Internet Protocol (IP) cameras. My logical assumption was that I would be working with IT to transmit my data from the camera to the recording source, but also throughout the property to several end users. I called a meeting of Security, Engineering, and, of course, IT. As we gathered around waiting for the meeting to start, we all discussed with some excitement the new technology that was about to open many doors for us. The IT Director walked in quietly, went to the whiteboard, and wrote "NO" in large letters. We looked at each other and then him, and asked what he meant. He said, "No, you cannot use *my* network for video." A long argument ensued about whose network it was, whose side he was on, and so on. Then he walked out.

That IT guy does not work there anymore, but that decision came too late as I had to build an entire network for video from scratch. I would have saved money, time, and probably improved the company intranet if he had been more cooperative. I hope you can learn two things from this story: One is that you need buy-in when you tromp into someone's field as I did, and two, don't act as he did when you need to work together on a project. The fact is there are hardly any projects or any equipment you will acquire where you won't need the expertise of the IT department.

You need IT probably a bit more than they need you (which may lead to some of that animosity), so build that relationship with them before you really need it. IT doesn't really need me to get into their office, but I rely on IT to make sure my network is up, that I have Internet and email, that my password works, and that all my systems are operating properly. I hope that you have a good person who understands we are all here to protect the assets and the guest. This is one of the first relationships you need to build if you have not done so already.

Besides convergence, there is another side to data security that has nothing to do with physical security. While you may have bad guys that occasionally come into your property to do bad things, your data are under attack constantly. There are people in other countries who do nothing all day but exploit vulnerabilities in your network or data chain. If you have email, Internet, or any other link to the outside world—and you do—your data are at risk. Your data may be the most valuable asset your business has. Credit card info, personal identities, client lists, payroll, and employee lists are all on your servers and your servers all connect in some way to China, Nigeria, and who knows where else.

This is not a full-time job; worse, it is a job for an entire department of experts. For every inebriated guest or shoplifter you physically deal with, there are another thousand attacks on your network. I am not a professional in data security, so I say leave it to the experts and support them 100 percent. One of the biggest risks to data security comes through employees. Either inadvertently, or intentionally, employees are responsible for the vast majority of data leaks, breaches, thefts, and viruses. Your IT department should already have policies in place that address these vulnerabilities, but they are often enforced by Security—as are most thefts. Some policies regarding data security are as follows:

Confidentiality—Most employees do not leak information on purpose. It is often through a clever scam or accidentally opening a bad link. Still, everyone must sign and adhere to a confidentiality policy and be held accountable if they break it. Training sessions on scams and Internet dangers should supplement these policies whenever possible.

Unauthorized hardware—This is often an unintentional breach as well. Employees bring in their music device or that free flash drive they received from the trade show. That device was probably made in China and its origins or intent are dubious. Companies should exclude all external drives and USB plug-ins for this reason. Besides, that sales manager who found a better job down the street just might like to supplement his income with the convention client list from your hotel. There is technology now that detects these devices being inserted into a desktop computer.

Personal electronic devices—Besides the USB devices just mentioned, cell phones and other data devices are problematic for several reasons. Cell phone cameras, Wi-Fi, Bluetooth, and hardwire connections are great ways to accomplish data theft. Some of the more advanced data companies can detect these devices being used, but no one has been able to detect a photo being taken of a computer screen. Cameras have some other ramifications. There have been sexual harassment and privacy cases against companies that allowed employees to have cameras on them at work.

Passwords—Password sharing is still the biggest problem for data security. Usually among co-workers, password sharing leads to some policy violations and access control issues, but when shared accidentally with outsiders, it can lead to real problems. A policy against password sharing should be enforced.

Internet/email filtering—Many companies have Web filters; presumably to keep workers from being distracted by nonwork-related Web sites. A more important reason is to avoid malicious sites. Just entering an unverified site can download a virus or cause other technical problems. Those filters usually are experienced-based, meaning that they are not put on the exclusion list until someone finds out about it. This means an email can have a link to a malicious site that has not been vetted and can inadvertently download something bad.

One thing you do not want at work is your employees abusing the Internet. Besides being a distraction of their real work, and the possibility of downloading viruses (mentioned previously), there are some other issues. Viewing and downloading pornography, for example, could result in sexual harassment issues. What if it is child pornography or exploitation? Keeping these filters current and strict keeps everyone out of trouble.

A few years ago, and probably still today, we were being bombarded with the Nigerian 419 scams. These people would send out millions of emails hoping to get just a few suckers and they did. One that affected businesses was the charming guy that convinced the lonely secretary to rescue him from his life of poverty with a promise of riches to be unlocked by the two of them later. This scam coaxed many an employee to use their business contacts and accounts to make airline reservations, long distance phone calls, and wire transfers, with the understanding that it would just be a "loan" to be paid back when their newfound wealth arrived.

DATA INVESTIGATIONS

Another point of convergence for IT and Security comes in the form of investigations. Data evidence is critical in many investigations now and both departments need to work together. For example, it is common to use archived emails as evidence in a sexual harassment case. There are many systems within a hotel that house or process information that you will need from time to time. You need to set up that relationship in advance so you can get to the data quickly and cleanly when needed. A good IT department can go one step farther and alert you when problems occur. Web filters can monitor attempts to enter pornography sites, emails with key words, unusual login times and frequency, access level violations, etc. These triggers can be set in advance with a consistent response from Security and Human Resources (HR).