1

Risk Assessment

Despite the scoring, the results are absolutely in accord with our risk assessment.

—Marc Short
U.S. Homeland Security spokesman, defending a grant program

Whether your property is in design phase, recently completed, or an established destination facility, a Risk Assessment needs to be completed. A properly researched and considered Risk Assessment will not only help management plan protective measures, but also it will provide a legal defense for those measures.

Many hotels have been in operation for years and have never completed a formal Risk Assessment. Informal Risk Assessments are performed constantly by security professionals, engineers, and risk managers. Formal or informal, the process is largely the same. Your first decision is whether you should do this process yourself or hire a professional.

EXTERNAL RISK ASSESSMENT

An outside consultant can add some integrity to your Risk Assessment. The professional has the experience and the resources to do a thorough job and the résumé to add credibility to the finished product. The only reason not to have this contracted out is the cost. However, as we learn later in this book, costs can be justified by savings in other areas.

INTERNAL RISK ASSESSMENT

Besides saving money on hiring this process out, the education you will gain and the knowledge of your own property will be priceless for you.

A Risk Assessment is quite simply a calculation of severity and probability. Don't let the math scare you. Security professionals perform these assessments on a regular basis—and they do so in their head. Each time a security officer approaches someone in the hotel, a mental Risk Assessment is being performed. The immediate results of that mental calculation are used to determine the officer's stance, demeanor, reaction, and level of readiness. For example, a petite, elderly, intoxicated woman trying to get her room key to work

generally would not pose the same threat or prompt the same response as a tall, muscular, younger man. That is a simple Risk Assessment. In his head, he calculated the probability of that person being a threat (attacking him) and he counted the severity of that threat (big guy versus little old lady) and made an instant decision to prepare himself.

The Risk Assessment process takes this simple calculation, expands it for a variety of threats, and formalizes it so that a security plan can be developed and documented for use later in justification. So, why do we need to go through all of this if we can do it in our heads? To protect our assets in court. I will explain toward the end of this chapter, but first, the assessment. This process can be divided into five steps. First, we will divide the property into sections. Then we will list all the possible threats and hazards for each area. Next, we will compile some historical data to determine probability. After that, severity will be figured into the process. Finally, we will work with the resulting values to determine risk.

Step 1—Divide the Property

Step 1 is to categorize the property into areas. Each area is like its own business with its own particular threats and risks, so it will be simpler to work with them separately. Do this by physical location, department, or revenue center—whatever makes sense to you. We will do a separate Risk Assessment for each of these areas, such as front desk, nightclub, guest rooms, and retail store. Some threats and hazards are to the entire property—such as floods and hurricanes—although the likelihood and severity will depend on your location. These are addressed in Chapter 10. We will use "Guest Rooms" as an example of one of our sections for the remaining steps (see Table 1.1).

Step 2—List Threats

Step 2 is to list the threats for each area. Consider every threat, no matter how remote its possibility. For our purposes, threats are crimes, natural hazards, and accidents. In

Table 1.1 Risk Assessment Example (Guest Rooms)

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**

Table 1.2 Listing Possible Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**
Robbery			
Domestic violence			
Property theft			
Assault on employee			
Noise complaint			
Fire			

Table 1.2, some examples of threats are robbery, domestic violence, property theft, assault on employee, noise complaint, and fire.

Step 3—Severity

Severity is completely subjective. We are going to fabricate these numbers based on our own common sense or opinions. Different persons may evaluate severity a bit differently, but even that will not matter for this exercise. Even though opinions vary, most people will rate incidents relatively the same. Death is more serious to everyone than vandalism, so the values are not as important as their ranking with the other threats.

For the purpose of this Risk Assessment, Severity is a rating of 1 to 10 on how bad the event would damage the assets or persons. Death would be a 10 and excessive noise in a hotel room is likely a 2. In Table 1.3, I have assigned values to each of the threats

Table 1.3 Determining the Severity of Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**
Robbery	8		
Domestic violence	2		
Property theft	5		
Assault on employee	8		
Noise complaint	2		
Fire	9		

based on my opinion of a sample hotel. I made "Fire" the most serious with a rating of 9 because it can do the most damage and disrupt business most severely. I rated "Domestic Violence" and "Noise Complaint" as least severe with 2 each. Both of these types of incidents cause a minor disruption to a few other guests and it is unlikely the hotel would suffer any loss from either. Your ratings may be different and that is fine as long as you can justify them.

Step 4—Probability

In order to determine probability, we need to do some research. Although our severity numbers in the table were subjective, the probability numbers better have some backing or you will look ignorant in a deposition. Backing comes in the form of historical crime data.

GATHERING LOCAL CRIME DATA

Before risk can be assessed, some data need to be gathered. First is historical "neighborhood" criminal activity. Criminal activity would include just about every type of activity that could happen at the hotel. Few crimes that occur at businesses, residences, or on the street are not a potential threat to a hotel, so just about every type of crime is pertinent.

There are several possible sources for local crime data, the most likely of which is the local police department. Many police departments provide regional crime data and calls for service through public source Web sites. Others provide it by less technically advanced means like paper reports available from the police station or city hall. Most large cities like Los Angeles, Las Vegas, and Chicago have easy-to-navigate Web sites that provide crime data that can be filtered and sorted. Many smaller cities provide this service as well. The easy way to find out is to do a Web search for your city name and "crime data."

There are other privately owned, but free, Web sites that provide this service for most cities using public information. Try searching "crime data by city" or "crime data by zip code." Of course, a few crime analysis companies provide this data for a fee. The price may include the Risk Analysis that is being explained here and other valuable information from other sources combined into one professional presentation. Consider these services to save time.

If the local law enforcement agency does not provide this data in an electronic form, it may be necessary to query them personally. This is public information, but there may be a fee associated with compiling the information or copying files.

Other sources for historical crime data are the Business Improvement District, Business Owners' Association, or Chamber of Commerce. The hotel may already belong to such a group, which generally has this information compiled or can easily access it through its law enforcement liaisons.

Many security departments will task someone with keeping this neighborhood crime activity documented and categorized (see Chapter 11). There are other investigative reasons for doing this, but for the Risk Assessment, it fulfills the data-gathering requirement. This is

an easy process to set up and the events can be taken from a police blotter in the newspaper, personal contacts at the police department, or regular phone calls to the report desk.

When gathering crime data, it is important to establish the radius or area from which the data are derived. This depends entirely on the location of the property. If the property is in a downtown urban setting, the entire downtown region should be used. If it is more of a suburban area with a couple of other hotels around, those few square acres might be enough. This may seem subjective and it is. Two requirements apply here. First is that the area surveyed is the same every time the data are collected. Second is that the area is large enough to find reported crimes and a good cross section of types of crimes.

It is also important to establish a time frame for the criminal activity. This may be limited by the source. Las Vegas, for example, only provides 60 days' worth of stats. It would be advisable to go back a year to cover all seasons and weather periods as well as tourist and economic cycles.

COMPILING LOCAL CRIME DATA

Once the information is gathered, there may be a murder, a couple of robberies, a few auto burglaries, and so forth. This is only the start. For the Risk Assessment, it will be necessary to know time of day, type of business, violent or property crime, etc. It also will be helpful to note the type of security in place at those places for comparison later. (See Table 1.4 for an example of local crime data.)

From our fictional crime data (Table 1.4), we can draw several conclusions with just a cursory look. There has not been a history of hotel homicides, which is why we did not include them in our Risk Assessment earlier in this chapter. Assaults also are not an issue, and judging by the stats, are probably mostly domestic. Robberies, however, are a problem. Of the robberies in this area, 20% were in hotels. Auto thefts were also a sizable percentage of the total, likely because of the nice selection in most hotel parking lots.

Table 1.4 An Example of a Crime Data Table

Local Crime Data—Downtown Any City					
Crime	**Daytime**	**Nighttime**	**Hotel**	**Other Business**	**Residential**
Homicide	1	2	0	0	3
Sexual assault	3	5	2	1	5
Robbery	10	15	5	15	5
Assault	25	26	4	11	36
Burglary	30	24	6	16	32
Theft	49	54	10	76	17
Auto theft	17	18	5	14	16

GATHERING PROPRIETARY INCIDENT DATA

Besides knowing what is going on around the property, it is necessary to know what is happening on the property as well. Proprietary data should be the easiest to get. Depending on what types of records are kept, the form they are in, and how long they are held, they can be the most useful. Ideally, the hotel has some reporting system in which data can be mined, sorted, and filtered into what is necessary.

If you are coming into a new property and do not have the historical records that you might expect, then you may need some help. Just as you did previously, consult the local police for their records. This will not have everything (only those incidents reported to the police), but it will provide something with which to work. You might even do this if you do have your own reports because some victims report crimes to the police and not to the hotel. Another dataset to ask for is "Calls for Service" by address. This will give you a great idea of incidents like domestic violence that do not always have an associated police report. The data, when compiled, will look like the police data already compiled (Table 1.4). Rather than create another table, just add the new data to the existing data.

GATHERING MARKET INCIDENT DATA

The third type of data needed is market data. This will be the same crime activity gathered previously, but it will be from like properties in the same market. A hotel located by itself may not have neighbors with which to compare, so it has to be assumed that similar hotels in the same region are going to have similar crime activity, threats, and risks. For this research, location of the other property or properties is less important than their type. If the property for which the Risk Assessment is being performed is a multistory, medium-priced resort, then it should not be compared to a budget motel. It is better to find a similar property in another city.

This information can be retrieved online or from the police as explained previously, but is best when taken from the source. Security directors who share the same market and have similar crime victims should already be communicating. They certainly should not have any problems sharing anonymous crime data. Unlike colleagues in the sales department, security operations should not compete. Competition when it comes to guest safety does not help anyone and ultimately results in a bad reputation for your region or tourist market. Relationships with peers are discussed in more detail in Chapter 12. Add this third data set to the existing data. The result should be a table showing what crimes are more likely to occur at our hotel based on neighborhood crime data, our own proprietary reports, and industry averages.

DETERMINING LIKELIHOOD

We will use all of the data compiled previously to determine trends and probability. The future cannot be predicted, but history provides a very good view of what is likely to happen. Applying this data in a simple list makes some things very clear. In the example

Table 1.5 Determining the Probability of Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**
Robbery	8	4	
Domestic violence	2	6	
Property theft	5	4	
Assault on employee	8	3	
Noise complaint	2	8	
Fire	9	1	

in Table 1.5, the Risk Assessment is performed on guest rooms. Not all of the crimes are relevant to guest rooms. Auto theft data, of course, will be used for our assessment of the parking areas, but robbery, assaults, and other thefts may be important to assess risk in guest rooms. These data are objective as they are derived from actual events and require little guesswork or assumptions. The Risk Assessment is almost complete.

In Step 4, probability—or likelihood—is determined. For each event, what is the likelihood (on a scale of 1 to 10) that it will happen? As before, the actual number does not matter as much as the order of events. The most likely should be high on the scale, and the least likely should be at the bottom (near 1). Confusion often arises in this step. Are we to determine the probability of the occurrence without security measures taken, or with mitigation? For example, the likelihood of theft with no lock on the door is higher than if there is a working lock. This will be discussed in more detail later, but for this assessment tool, it is better to determine the likelihood using existing or normal preventive measures. Therefore, when figuring the values in this column, assume that working locks are in place, proper lighting exists, and so on.

In Table 1.5, I assigned a rating of 1 to "Fire" because in my sample hotel there is a no-smoking policy, bed linens meet modern fire retardant standards, and we have never had a fire in our hotel. "Robbery" and "Property Theft" each earned a 4 because we have had both occur with almost equal regularity and other hotels in our area have had them as well. "Noise Complaint" was rated highest because we are a value-oriented hotel and we get noisy guests all the time. Once again, your values may be different based on your history, type of hotel, and your surroundings.

DETERMINING RISK

The final step of the Risk Assessment is the easiest, and for those visual learners, the most revealing. Multiply the severity value by the probability for each threat to determine risk. In some exercises, you may add these numbers instead of multiplying them. Using the

Table 1.6 Determining the Risk of Threats

Threat/Hazard	Severity	Probability	Risk
	10 = Most Serious 1 = Least Serious	**10 = Most Likely 1 = Least Likely**	**Severity × Probability**
Robbery	8	4	32
Domestic violence	2	6	12
Property theft	5	4	20
Assault on employee	8	3	24
Noise complaint	2	8	16
Fire	9	1	9

likelihood as our multiplier will give us a broader range of values when we are finished, making it easier to distinguish one risk from another.

In our example in Table 1.6, we had some expected results and maybe a surprise or two. Robbery was high, as expected. Domestic violence and Fire came out low as risks. We probably will not devote as many resources to prevent these in our Security Plan. (Remember, Fire is already addressed in building construction and existing detectors and alarms as per fire code.) "Assault on Employee" was higher than expected. This is a risk that is not always sufficiently addressed in Security Plans, but there are plenty of high-profile examples where housekeepers have been attacked, raped, and even killed by hotel guests. We will address this in our Security Plan in Chapter 2.

Insurance companies use this same formula to calculate your insurance premiums. They just use many more variables for severity and probability. Probability factors for car insurance, for example, are driving record, geographical location, age, gender, etc. Severity factors are cost of vehicle, income level, deductible, etc. These factors and others are entered into complicated algorithms to determine what type of risk you are. You can get just as complicated with your property Risk Assessment if you want to take the time. In fact, your business insurance company has likely done something similar to this already.

FORESEEABILITY

Foreseeability is the trump card to the Risk Assessment. Foreseeability means that if an event has occurred on the property before, then it is possible that it will happen again. As mentioned before, history is a good indicator of potential hazards, so if the environment allowed an incident to occur, and the security environment does not change to meet that threat, then it can happen again. This becomes a liability issue. If it does happen again, it will be considered as having been foreseeable by the courts. The event happened because

of the inadequate security, nothing changed to prevent it from happening again, it did happen again, and now it is management's fault.

In 2008, an employee sued an Oklahoma hospital for inadequate security after she was abducted and sexually assaulted in the parking lot. The hospital did provide cameras and an employee monitored 30 camera feeds simultaneously. It was discovered later that the suspect's van was visible on camera circling the garage with duct tape obscuring the license plate. Within the previous year, there had been several incidents of assault, battery, abduction, and robbery.

The hospital management had plenty of notice due to prior acts that this particular event was foreseeable. In this case, it was deemed that the video system proved inadequate to keep the employee safe. The hospital attempted to have the case dismissed, claiming it was not responsible for the criminal actions of third parties. The Supreme Court of Oklahoma denied the hospital's motion and sent the case back for trial.

Suppose an incident occurs in the parking garage—like a strong-arm robbery. If basic security measures had been taken—such as proper lighting, security patrol, and emergency call boxes—then there may be a good defense for the hotel in the lawsuit that arises. In most cases, a good security manager will re-assess the area and determine what security measures could have prevented the incident entirely. Perhaps adding cameras, increasing patrols, and gating the entrance points would be considered appropriate. If a similar incident occurs again, there is likely a good defense that the management is doing everything reasonable to prevent such events and protect its guests.

Suppose after the first robbery, the company decides that its security measures are adequate and changes nothing. If a second robbery occurs, the company is going to be in a very difficult position to defend itself because the second incident was foreseeable.

MANAGING FORESEEABILITY

The word *foreseeability* is not found in many dictionaries. Legal and risk professionals created it and it means that one should have the "ability" to "foresee" events based on previous events that occurred. In other words, if a crime or incident happens, there is foreseeability that it will happen again.

In 2010, a man who was attacked in his motel room sued a popular U.S. motel chain. The perpetrators had knocked on the victim's door; he allowed them entry and was severely beaten. The suit claimed that the motel chain had a duty to ensure his safety and prevent criminal acts. The plaintiff also alleged that the motel lacked security cameras and patrols, among other things. The motel responded that the attack was "unforeseeable" because motel employees were not aware of the attackers' presence

on the property and that there were no known similar incidents at that motel or within the immediate vicinity. The court agreed with the motel, stating that even if the motel had the security measures in place, the crime would not have been prevented because the victim had opened his own door, resulting in the attack.

As we learn in this chapter, even though the motel won this case, they are now on notice. If a similar crime were to occur at that property again, they may be held liable because it is now foreseeable. Strike one.

Some legal professionals refer to foreseeability as the "one-strike rule." The company can defend against that first incident if it was unexpected and reasonable precautions had been taken (strike one). But, the second event is one that should have been expected—foreseen. Therefore, the liability falls more on the property that should have taken steps to prevent the event (strike two—you're out).

The remainder of this book is written with the expectation that security directors want to keep their employees and guests as safe as they can and that reasonable steps will be taken to prevent crime and accidents.

Most security directors are reading this and thinking that they have already done their Risk Assessment in their head. This is a great skill, but there are two important reasons for documenting the process. First, collecting written data and compiling it in written form is likely to catch some errors or some omissions that may occur during the thought process. Second, and most importantly, the documentation is vital for litigation. It is difficult to remember and to defend a mental determination, especially if it is years old. If another director or management team takes over, he or she will have no idea how the original assessment came to the conclusions that it did. The written assessment allows the company's legal counsel to show how and why certain security measures were taken if they are challenged. "If it isn't written, it didn't happen."

In November 2005, a man walked into a shopping mall with a rifle, pistol, and guitar case full of ammunition. He shot mall patrons at random, hitting eight of them before being arrested by police. The eighth man sued the mall for inadequate security, claiming the mall could have provided better security measures to prevent the shooting. The mall filed for summary judgment and was at first denied, but upon reconsideration, the court granted the dismissal. The court agreed with the mall that a random shooting in the mall was not foreseeable and the mall had no duty to protect against it. Now that the mall has "notice" of this type of incident, it will likely take some additional security measures (revise its security plan) because it will not be able to use the same defense if a shooting happens again.

In the next chapter, the Security Plan will be introduced and implemented. First, it is important to realize that the Risk Assessment is never completed. Each time a new aspect of the security plan is implemented, that part of the Risk Assessment will have to be

re-assessed. Severity may not change, but probability definitely changes each time an area is fortified. Ideally, all of the values in the Risk Assessment are low and maintained low. Other factors may change the Risk Assessment. Seasonal factors, demographic changes in the area, special events, economy, regional crime, police patrol, and even the company marketing strategy may change probability and require a new assessment. These specifics will be discussed later throughout the book.