Chapter 3

Threat Assessments

In this chapter . . .

- Threat Formula
- Threat Identification and Classification
- Threat Information Sources
- Assessing Threats
- Emerging Threats
- Threat Dynamics
- The Homeland Security Advisory System

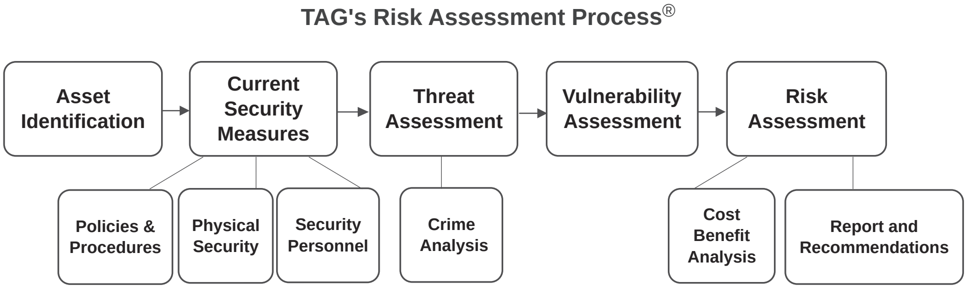

Figure 3-1.

Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Threat Formula

THREAT = INTENT + CAPABILITY + MOTIVATION

Following the asset identification and security inventory steps of the risk assessment process, the third step is to perform a threat assessment. As discussed previously, a threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Threats are classified as either human or natural. Threat can also be defined as an adversary's intent, motivation, and capability to attack assets. Threat assessments, then, are evaluations of human actions or natural events that can adversely affect business operations and specific assets. Historical information is a primary source for threat assessments, including past criminal and terrorist events, whereas real-time information is also being used with increasing frequency owing to its availability in some arenas. Threat assessments can be quantitative or qualitative. Crime analysis is a quantitative example of a threat assessment, while terrorism threat analysis is normally qualitative. An important distinction is that threats are acts or conditions that can harm organizational assets, whereas adversaries are the people, groups, and organizations that are hostile to the assets. Adversaries are also characterized by their history of attacking assets, the intention to attack assets, and the capability and motivation to continue to attack assets.

Threat assessments are used to evaluate the likelihood of adverse events, such as terrorism and crime, against a given asset as well as other hazards such as natural disasters that may affect business operations. As such, the focal points of threat assessments are assets (targets) and the threats that seek to compromise those targets. Threat assessments also ask who the bad guys are by evaluating each threat on the basis of capability, intent, and impact of an attack. General threat assessments estimate the likelihood of adversarial attacks, including the type of adversary, their tactics, and their capabilities. Facility-specific threat assessments also define the number of adversaries and their method of operation or attack. With this information, security decision makers use threat assessments as a decision-making tool that helps to establish and prioritize safety and security program requirements, planning, and resource allocation. The process of threat assessment includes:

Threat identification—identify potential adversaries and their characteristics.

Asset classification—identify targets and determine their criticality.

Consequence/Criticality analysis—assess the effect of an assets compromise.

Whether security professionals are in the business of national security or in the commercial and industrial sectors, threat assessments should be conducted as often as necessary to meet the needs of the organization. While threat assessment is a continuous activity for the U.S. government, businesses and other organizations should strive for annual threat assessments. Crime analysis is the most common type of threat assessment undertaken by American businesses. It is done every year at minimum, and it is sometimes completed as often as once a quarter. Location-specific threat assessments at infrastructure facilities, such as ports, are carried out less frequently, but threat data is usually updated constantly. It should be noted that the biggest failing in threat assessments is a lack of specificity. For example, when the national terror alert system was first introduced, a move in the threat level required all industries and agencies, regardless of geographic location, to change their readiness level. Upon further reflection, the Department of Homeland Security adjusted the model to consider location or sector-specific information. Since this change, the United States has seen increases in threat levels to certain parts of the country or within certain sectors. For example, after the London Underground (subway) bombings in 2005, the threat level in the United States did not rise, but U.S. mass transit was put on alert. Similarly, the United States has experienced increased threat in the Northeast while the rest of the country has remained at a lower level. It is the task of security professionals to use a targeted approach to threat assessment, whether the target be by geography or asset classification. Of primary concern with regard to raising the threat level across all jurisdictions or across all organizational operations is the cost associated with a higher level of preparedness. Depending on the threat, security professionals can assess the likelihood and types of potential attacks if specific information on potential targets is available. Based on their assessment, specific, targeted countermeasures can be implemented.

Threat assessments evaluate the full spectrum of threats that can impact assets, including natural disasters, criminal activity, terrorism, safety-related accidents, and common security breaches such as unauthorized access. Each potential threat must be analyzed using all available information to establish the likelihood of occurrence. Gulf coast states such as Texas, Louisiana, and Mississippi, for example, have a wealth of historical data that can be used to plan for hurricanes during high-risk months. Urban convenience stores also have ample evidence of their general crime threat level. Despite an awareness of general threats, security decision makers must refine their assessments to include specific scenarios in the protection of assets. A convenience store located in a high-crime area that experiences an inordinately high level of crime on its premises should elevate its site-specific threat level and allocate security resources accordingly.

Asset attractiveness should also be considered in the threat assessment. Certain assets and businesses have a higher inherent threat level because of their attractiveness to the criminal element. One obvious example is jewelry stores. Despite the lack of previous crimes at a particular jewelry store, the threat level for robberies and burglaries is still high. This is not to say that jewelry stores are inherently vulnerable, only that the threat level is higher. Another example of a business with an intrinsically elevated threat level is the construction site, which, compared to other sites, typically has a higher rate of accidents resulting in injury to workers. Again, the threat exposure is there, but the vulnerability need not be. This concept will be discussed further in the vulnerability assessment chapter (Chapter 5).

Threat Identification and Classification

The best predictor of the future is the past. This same idea holds true when assessing adversaries. A thorough understanding of how adversaries operated in the past can assist security decision makers in predicting future adversarial operations. Without fear of jumping to conclusions, many security professionals knew immediately that Osama Bin Laden was responsible for the World Trade Center and Pentagon attacks on September 11, 2001 as soon as the second plane hit the World Trade Center. This accurate assessment was based on knowledge of prior attacks by a terrorist organization that the world came to know as al-Qaeda.

While the al-Qaeda example is universally understood in the security industry, the same logic can be applied to commercial and industrial targets. If security decision makers understand the adversary's perspective, effective protection measures can be efficiently allocated to reduce the threat. How do adversaries select targets? What types of assets have been targeted in the past? What are their intentions, capabilities, and motives? Bank and financial institution security professionals have made excellent use of threat information sharing to prevent certain crimes. Similarly, retailers have shared information to track baby formula thefts.

Although the goal of any security decision makers should be to quantitatively identify threats, it is not always possible to do so, and some threats must therefore be assessed qualitatively based on assumptions and educated guesses. Crime threats can normally be assessed quantitatively based on historical crime data, whereas understanding a particular criminal must be qualitatively addressed. This is a key difference of crime analysis, the examination of historical crimes with little regard to the criminal himself, the adversary.

In this chapter, the focus will be on understanding the adversary or the qualitative perspective. In the crime analysis chapter (Chapter 4), a data-driven, quantitative method will be discussed. So what type of information is needed to describe a threat qualitatively?

- The type of adversary
- The adversary's intentions
- The adversary's motivations
- The adversary's capabilities

Threats can be classified as either human or natural. Human threats are those involving people working on the inside of the organization such as employers and contractors (insiders), people who attack from outside of the organization (outsiders), or a combination of the two. Natural threats are those events that are not man-made such as tornados, hurricanes, floods, fires, and other environmental events.

Human threats can be further categorized as insiders, outsiders, and insiders working with outsiders. Insiders may be subclassified as criminal employees, dissatisfied employees, criminal contractors, and disgruntled contractors. Threats from insiders are considerable given their security program awareness, opportunity, and unfettered access to the facility. Insider threats may be active and violent or stealthy, perpetrated by silent participants with outsiders. Although workplace violence poses a high risk to other employees, insiders who are blackmailed or threatened by outsiders create a more difficult problem for security decision makers. Since the insider threat is typically the result of policies and procedures, security decision makers cannot rely on traditional security measures such as alarms, cameras, and lighting to thwart this kind of threat. Good mitigation strategies may be put in place to protect against the insider threat, though strong policies and procedures are among the most reasonable and effective. Policies should include personnel reliability programs, recurring background checks, and limitations on access to sensitive areas of the facility.

Outsiders may be subclassified as foreign governments and militaries, gangs, criminals, extremists, and terrorists. The depth of classification should meet the security organization's needs. For example, the U.S. government classifies terrorists as political, religious, or environmental. Terrorist characteristics may include a willingness or desire to die or martyr oneself, inflict a high level of damage, injuries, and deaths, cause psychological pain to citizens, and showcase abilities to terror fund raisers. Outsiders may be motivated by ideological goals, economic gain, or personal reasons.

Insiders colluding with outsiders pose the greatest threat of all and may be classified as coerced or willing participants. Coerced insiders are unwilling participants in the attack who are forced by threat of harm to themselves or family or who are blackmailed. Willing insiders may have a financial interest (bribes) or may be ideologically sympathetic to the outsiders' cause.

Threat assessments should consider the possibility of all three types of human threats and should be based on reasonable intelligence available from multiple sources, including internal information, law enforcement data, red teams, specialists, media reports, and federal and private intelligence sources. Only rarely do security decision makers have accurate knowledge of a specific threat beforehand. Information may be incomplete or vague, and as such, educated judgments must be made in defining a threat. The more complete the available threat information is, the better the assessment.

Adversary Motivation

Adversaries may be motivated by any number of factors, but the most usual motivations are economic, personal, and ideological. And the most common of these three is economic where the gain of valuables, including money, is the driving force behind a criminal attack. Economic criminals include robbers, burglars, and thieves. While this description appears quite simplistic, it may be more complex than it seems as these criminal perpetrators may actually be driven to commit economic crimes for personal reasons. Drug addicts are a great example: they commit the economic crime purely to obtain valuables to exchange for drugs, a personal motivation. A similar example is the teenager who steals electronic music players, such as the Apple iPod, or basketball shoes, such as Air Jordan's, to raise his self esteem and fit in with his peers.

As already suggested, personal motivators are often emotionally driven; examples include an angry husband who abuses his wife, or a disgruntled employee who commits acts of workplace violence. Motivations for the insider threats are often personal and driven by poor workplace management, real or perceived, resulting in an unhappy worker who bears a grudge usually against management. Personal crimes are sometimes difficult to prevent because they can be committed as a spontaneous act of rage or because of a mental disorder. Andrea Yates, the Texas mother who drowned her four children in a bathtub, is an example.

Ideological motivations are linked to philosophical beliefs. Environmental criminals are those who seek to harm those whom they believe are damaging the environment. Take the example from California where environmental terrorists, such as the Earth Liberation Front (ELF), committed an act of arson at car dealerships that sold high-fuel-consumption sport utility vehicles. Other terrorist groups are ideologically motivated to protect animals and attack laboratories that experiment on animals. Of course, most of the world understands what motivates terrorist groups like al-Qaeda. The 1993 World Trade Center attack, though not indicative of al-Qaeda's capability, showed that terrorists were motivated to attack landmark buildings.

Adversary Capability

Assessing adversarial capability relies heavily on good intelligence. No better example exists than the failure of U.S. intelligence to forecast the Japanese attack on Pearl Harbor, precipitating U.S. entry into World War II. Without delving into the politics of this event, it is fair to say that incomplete and slow intelligence underestimated Japan's capability. Time and time again, history has shown that faulty intelligence over- and underestimates adversarial capability.

In the commercial and industrial sectors, where companies are in competition with one another, good intelligence is difficult to come by. Industry sharing of threat information is rare but not impossible. Through informal organizations, some industries have successfully shared information about adversaries with each other in an effort to thwart a problem before every company is affected. Again, the banking industry does this with regularity and with great success.

For security decision makers, assessing the capability of an adversary includes the following factors:

- Number of attackers
- Skills
- Knowledge of the facility's security
- Types of weapons
- Other equipment
- Methods and tactics (deceit, force, stealth)
- Means of transporting attackers, weapons, and equipment
- Possible collusion with an insider

Terrorist capabilities may include providing highly trained and skilled military units with shoulder-fired weapons and explosives; developing unsophisticated nuclear weapons, known as dirty bombs or other improvised explosive devices; and funding operations and furnishing fake identification, including passports and driver's licenses. Terrorists may also be trained in sabotage, hostage taking, and homicides.

Each threat should be specifically described in sufficient terms and relative to its ability to attack particular assets. This description is known as the design basis threat (DBT) because it forms the basis for the design of security programs. The DBT includes statements of intent, motivation, and capabilities of each threat. The description also includes the known tactics and methods, weapons and equipment, and other details of past attacks by the adversary. Studying past security breaches is critical in forming the design basis threat.

Threat Information Sources

As we have discussed briefly, security decision makers should endeavor to seek out all possible sources of threat information. Threat information should come from multiple and redundant sources. Depending on the nature of the assets in need of protection, the sources of threat information may include internal information, security breach investigative reports, law enforcement data, red team penetration analysis reports, security consultants, media news reports, and both federal and private intelligence sources.

For security consultants and other security decision makers who are not intimately familiar with the facility they are assessing, the best starting point in gathering threat assessment data is through interviews and surveys of people who are more familiar with the site. A security consultant, for example, may begin a threat assessment by speaking with line-level security personnel, including police working at the site and proprietary and contractual security officers. Other line-level personnel working on site make for good sources as well. Among the basic questions that should be asked of line personnel regarding each asset are the following.

- What assets have been targeted in the past?
- When were assets attacked?
- Who targeted the assets?
- Why is that asset(s) targeted?
- How was the asset attacked?
- Were any remedial security measures implemented in response to the attack?

Many security-conscious organizations also maintain internal records of security incidents, breaches, and crimes. Security decision makers should review this information on a regular basis while looking for trends and patterns that might indicate existing threats or that might point to a vulnerability that can be solved with remedial measures. An often overlooked source of threat information is prior threat assessments. Many organizations conduct risk assessments on a continual basis and have the associated reports filed away. For security consultants, this is among the documents they request from the organization during the initial days of a risk assessment, or even prior to setting foot on the premises.

External threat information, including crime data from the local law enforcement where the facility is located, should also be reviewed. (This is known as crime analysis and will be discussed in depth in the next chapter.) Other external sources include private threat specialists, who are especially useful for executive protection. Some companies that specialize in threat assessments for other countries go far beyond the basic information provided by the U.S. State Department. Even before September 11, the FBI created InfraGard, a partnership between the government and private industry to share terrorism, intelligence, criminal, and security information about critical national infrastructures.

Assessing Threats

After collecting, reviewing, and summarizing threat information from all available resources, security decision makers must apply the threat to specific assets. Although critical assets are the primary concern during the assessment, other assets may also be considered during the assessment phase. The goal of the assessment then is to estimate, quantitatively or qualitatively, the likelihood of occurrence that a threat will attack an asset.

The better the understanding of the intent, motivation, and capability of an adversary, the better the assessment. Of course, a history of attacks against a particular asset may be beneficial to satisfy the intent and motivation criteria. Capability assessment requires good intelligence about the adversary's current status. Looking back on the 1993 World Trade Center attack, we can see that al-Qaeda was motivated to destroy the World Trade Center towers but that their capabilities did not correlate with their intention. With the towers still an attractive target and assuming there was no credible intelligence that planes would be used as guided missiles, al-Qaeda certainly did not seem to have the capability to destroy the Towers. Obviously, before September 11, any intelligence about the plane scenario was reasonably treated as non-credible.

Because of a lack of quantitative data, scenario-driven, qualitative assessments are appropriate for high-value assets that have suffered no prior attacks. A qualitative threat assessment is defined as a type of assessment that is driven primarily by the characteristics of the threat and is highly dependent on the skills of the assessment team. The threat assessment team or individual, using a qualitative approach, considers each asset in light of the given threat information for that asset, and develops scenarios that adversaries may use to estimate the likelihood of attack. Using a qualitative rating system, the threat assessment team assigns a linguistic value to each scenario.

An example of a qualitative rating scale is as follows.

- Level 5—the adversary has a history of attacks as well as the intent, motivation, and capability to launch a renewed attack.
- Level 4—the adversary has a history of attacks and the capability to execute an attack, but may lack the intent and motivation to launch new attacks.
- Level 3—the adversary has a history of attacks and the intent and motivation to launch new attacks, but lacks the capability to execute an attack.
- Level 2—the adversary has a history of attacks but no longer has the intent, motivation, and capability to launch new attacks.
- Level 1—the adversary has no history of attacks and lacks the intent, motivation, and capability to execute an attack.

As can be seen in the qualitative assessment scale, good threat intelligence is necessary to accurately assign threat levels. An example of a threat that can be assessed qualitatively is weapons of mass destruction (WMD). WMDs are made up of chemical, biological, and nuclear weapons. Because these threats have a low likelihood of occurrence historically, little data is available for assessing them quantitatively.

U.S. Army Physical Security Field Manual/FM 3-19.30

THREATCON Levels

Specific security measures should be directly linked with THREATCON levels. These considerations are:

⤷

THREATCON Normal. This THREATCON level exists when a general threat of possible terrorist activity arises but warrants only a routine security posture.

THREATCON Alpha. This THREATCON applies when there is a general threat of possible terrorist activity against personnel and facilities (the nature and extent of which are unpredictable) and when circumstances do not justify full implementation of THREATCON Bravo measures. It may be necessary to implement measures from higher THREATCONs either resulting from intelligence or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

THREATCON Bravo. This THREATCON applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, or aggravating relations with local authorities. While in Bravo, the installation should bring manning levels and physical-protection levels to the point where the installation can instantly transition to THREATCON Charlie or Delta.

THREATCON Charlie. The transition to THREATCON Charlie must be done on short notice. It is a result of an incident or the receipt of intelligence indicating that some form of terrorist action against personnel and facilities is imminent. Charlie measures should focus primarily on manning adjustments and procedural changes. Security forces will usually enhance their security presence by acquiring additional manning or by adjusting the work-rest ratio (such as moving from a 3 : 1 to a 6 : 1 ratio). At Charlie, off-installation travel should be minimized.

THREATCON Delta. Since the transition to THREATCON Delta is immediate, Delta measures should focus primarily on manning adjustments and procedural changes. THREATCON Delta applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. The security force's manning level usually peaks in Charlie; therefore, Delta's additional manning will often come from an augmentation force. Once in Delta, nonessential operations will cease in order to enhance the security and response posture. Normally, this THREATCON is declared as a localized condition.

Where a fair amount of threat data is available, a quantitative threat assessment is possible. A quantitative threat assessment is a type of assessment in which metrics are used to assign numeric values to the threat level. With vast amounts of prior incident data, a quantitative assessment can include mathematical projections to forecast future incidents. Using mathematical projections, quantitative threat assessments can achieve high levels of confidence, but the forecast range widens. Forecasting will be discussed in the next chapter since it is most commonly used with crime data. A quantitative threat assessment uses a numeric threat rating scale, normally employing probability ratings. An example of such a scale is as follows.

- Level 5—90 percent or higher likelihood of attack because the adversary has a history of attacks as well as the intent, motivation, and capability to launch a renewed attack.
- Level 4—70 to 89 percent likelihood of attack because the adversary has a history of attacks and the capability to execute an attack, but may lack the intent and motivation to launch new attacks.
- Level 3—50 to 69 percent likelihood of attack because the adversary has a history of attacks and the intent and motivation to launch new attacks, but lacks the capability to execute an attack.
- Level 2—10 to 49 percent likelihood of attack because the adversary has a history of attacks but no longer has the intent, motivation, and capability to launch new attacks.
- Level 1—less than 10 percent because the adversary has no history of attacks and lacks the intent, motivation, and capability to execute an attack.

Despite a given threat rating, threats are not static; rather, they are dynamic and rise or fall over time. Threats can and should be reassessed as needed and when new information becomes available. A good example might be the increased threat level near the anniversary of the Oklahoma City bombing on April 19, 1995, which itself coincided with the Branch Davidian standoff in Waco, Texas, between cult leader David Koresh and the Bureau of Alcohol, Tobacco, and Firearms (ATF) which occurred two years prior to the day.

Emerging Threats

Accurate threat assessments are critical for security decision makers; however, not even the best threat assessment can anticipate every possible scenario which may emerge. Terrorists and criminals always adapt to and overcome updated countermeasures. In today's high-technology world, state-of-the-art countermeasures are outdated at an increasing pace, and adversaries usually move at a similar pace. Security decision makers should keep abreast of the latest threat information using the best available sources of information. Using the threat information sources discussed above and adding to them where possible will help keep the security professional abreast of the latest threats and ensure that the assessment report is up to date.

The mitigation of emerging threats requires the ability to think and act like the adversary. Historical data, specifically data on the adversary's modus operandi (method of operation), sheds significant light on what security decision makers should watch for in the future, but truly thinking like a criminal or terrorist will allow security decision makers to think outside the current wisdom.

Maintaining a current profile of adversaries is important for the threat assessment. W. Dean Lee, Ph.D, in an article entitled *Risk Assessments and Future Challenges,* which was published in the FBI's July 2005 *Law Enforcement Bulletin*, developed the acronym CAS-DRI-VARS to characterize the adversarial tactics and methods currently being used by adversaries operating around the world.

- Creative—applying innovative use of the ancient arts of unconventional warfare
- Asymmetrical—launching multifaceted physical, political, informational, and cyber attacks
- Secretive—cloaking in multiple layers and compartmented cells
- Deceptive—misleading and manipulative in their intent and behavior
- Resourceful—maximizing the use of available resources to achieve their objectives
- Intelligent—capitalizing on detailed planning and orchestration
- Visionary—foreseeing the third and fourth order of effects of their actions
- Adaptable—evolving and adjusting with each new countermeasure
- Ruthless—striking with brute violence against the innocents
- Sophisticated—employing intricate ploys and strategies

Beyond these characteristics, security decision makers should continually study the goals and objectives that adversaries are attempting to achieve. Their motivation and intent must also be evaluated. Keeping a watchful eye on adversarial capability is by far the most important way to keep the threat assessment current. For example, commercial businesses, retailers in particular, know that an incarcerated shoplifter has little to no capability. Thus, they lobby for prosecution, stiffer sentencing guidelines, and strong enforcement of existing laws. The United States government understands that terrorist capability is highly dependent on funding for terror operations and thus has implemented various worldwide strategies to stop the flow of funds to and between terrorist leaders and operations personnel.

Adversaries' skills may deteriorate or, alternatively, improve over time as well. Without recent experience and training, some adversaries may lose their capability to attack successfully. Security decision makers, depending on the nature of the organizations they protect, can keep abreast of the latest tactics and methods of their most common adversaries. Here again, the United States government recognizes this and has also attempted to close down terrorist training camps in hopes of reducing the overall skill level of terrorists.

Asset knowledge is critical to adversaries, and moving targets are more difficult to attack successfully. Although most businesses are not able to move assets to throw criminals off the track, they are able to keep information about some assets confidential and prevent adversaries from knowing exactly where they are or how they can be accessed. While most criminals will be familiar with people who store their money under a mattress, few criminals will be privy to the knowledge of where the family's safe is located within the house. One of the more interesting home protection ideas from the past came from the homeowner who posted a sign on his door which stated, "This house protected three days a week by Smith and Wesson. You pick the days." Amusing as the sign may be, one would have to believe that the unmotivated house burglar may have been deterred by the existence of such a sign.

Threats may also change depending on the adversary's access to tools and weapons. Arguably, the point of the now defunct assault weapons ban in the United States was to reduce the availability of high-capacity weapons to criminals, in particular street gangs. Passports have long been sought-after tools for terrorists and spies. In recent years, many countries have improved their country's passports to prevent duplication. Some countries have even canceled all existing passports and reissued new ones to their citizens with better security features.

Opportunities can impact the threat level more than any other factor. Fortunately, security decision makers can control opportunities largely through the careful monitoring of asset vulnerabilities. An example is the assassination of John F. Kennedy in Dallas, Texas, in November 1963. Not only was the president traveling in an open-top automobile, but the motorcade was traveling with many points of higher ground surrounding it. As a result of that tragic fateful day, the United States Secret Service will not likely ever allow a president to travel in a convertible automobile. Reducing opportunities will be discussed in depth in Chapter 5.

Threat Dynamics

The daily assessment of terror threats applies primarily to security decision makers who are charged with protecting critical infrastructure assets, such as chemical plants, oil refineries, airports, and maritime ports. Most security decision makers focus on terrorism as a high-risk, low-probability concern that needs to be addressed on an irregular basis. Once terrorism contingency plans, emergency procedures, and business continuity plans are established, security decision makers can once again turn their attention to the day-to-day issues that threaten the organization's assets. Everyday crimes are the most common threat facing security decision makers in protecting their assets; a thorough assessment of the specific nature of crime and security breaches can reveal possible weaknesses in the facility's current security posture and provide a guide to effective solutions. A full understanding of the dynamic nature of everyday crime allows security decision makers to select and implement appropriate countermeasures to reduce the opportunity for these incidents to occur in the future. Thus, the remainder of this chapter focuses on the dynamics of everyday threats, identifying their key elements and describing how to analyze these elements to block specific threats.

In discussing threat assessments thus far, we have laid out ideas in an effort to help the reader understand the conceptual perspective of threats. Everyday threats can now be discussed to enable the reader to understand the practical nature of common threats and to evaluate the threats to the organization's assets. Before selecting countermeasures, security decision makers should be well versed in a number of threat dimensions. As conceptually outlined previously, these dimensions include:

- The facility's situational elements
- Target/Asset characteristics
- Adversary motivation and capability
- Adversary target selection factors
- Opportunity-reduction strategies

Situational elements are those characteristics of the facility that create an environment that is more or less conducive to certain types of crimes or security violations. For example, a retirement home may suffer more from thefts within the community than from auto thefts due to the nature of the business. Another example of situational elements affecting crime may be the proximity of the facility to escape routes such as dense fields or wooded areas that can be used to conceal the offender on foot or quick escapes via highways used by the criminal in a motor vehicle. Situational elements also include the nature of the activities that occur on the property. Businesses face different problems than residential areas. The type of business that is conducted on a property may attract more crime. For example, bars and nightclubs may be more prone to assault-type crimes and sexual offenses because alcohol consumption lowers inhibitions. Hotel, motel, and other lodging facility customers are often victimized on or near the property because they are not as aware of the area's crime history. Criminal perpetrators know this and take advantage of the situation.

A target's characteristics are often determined by the nature of the business. Jewelry stores possess two types of attractive assets—large amounts of money and small, easily concealed property. Sometimes, the characteristics of targets are self-evident. For example, banks can be assured that their primary concern is the money stored on-site, whereas the retail store's primary concern is usually shoplifting. Analysis of past crime data may reveal other threats that may not be evident. For example, a retail store that has a history of car-jacking robberies and assaults of customers may only be fully known by reviewing internal security reports or police crime information. Facilities with high levels of auto thefts can narrow the field of targets by using threat assessments and crime analysis to determine which cars are more theft prone. If the ideas presented in the asset identification chapter (Chapter 2) are followed, security decision makers will have identified the organization's critical assets and their attractiveness as well as past history of attack.

Adversary motivation and capability are key to understanding the nature of crime on the property. Criminals, more often than not, are rational decision makers capable of being deterred or enticed to commit their acts. In modern criminal justice, it is widely accepted that certain people can be generally deterred from committing crimes given swift and severe punishment. Specific deterrence measures can be taken at the property level by introducing countermeasures that increase the risk of detection by security personnel. For example, the presence of security dogs or closed circuit camera systems (CCTV) may deter many adversaries. By the same token, given ample opportunity and a low risk of detection, people may also be encouraged to commit crime. An adversary's capability must also be considered. The same adversary who attempts to enter the property secured by security dogs may have the capability to bypass the dogs by way of poisoned treats or a distraction method. The security decision maker's goal is to reduce encouraging elements and increase the risk. For instance, hiding assets in a safe is often a good way to make valuables "out of sight, out of mind."

Through an ability to select specific targets the rational criminal will select the easiest target that provides the highest reward. An open and inviting property provides a high level of opportunity for criminals. University campuses are a good example of an easy target since they are typically open environments with minimal perimeter security measures. It is quite a challenge to secure university campuses without creating impediments to the institution's primary goal of Education. Adversaries also select targets where the rewards are high. Malls, for example, provide ample auto theft opportunities for the perpetrator who specializes in stealing cars. One may think of target selection primarily as a force of opportunity. The goal for security decision makers, then, is to reduce the available crime opportunities at the facility.

Opportunity-reduction strategies address the characteristics of the facility that either encourage or deter crime. Each facility will be different in terms of the solutions that are effective because each property has its own unique characteristics and unique threats. Unfortunately, what works at one facility may not work at a similar facility in a different geographic area. Opportunity-reduction strategies may take the form of enhanced policies and procedures, physical security measures, or security personnel. Although the focus of this text is on cost-effective solutions to everyday crime concerns, the reader should not feel limited to using what is discussed herein, but rather is encouraged to be creative in the search for appropriate solutions for particular concerns. Although it may sound basic, one of the fundamental opportunity-reduction strategies for litter prevention is the installation of trash receptacles.

The following section is not intended to be comprehensive in addressing every possible threat, but it will endeavor to cover the more common crimes that affect many facilities. Security decision makers are encouraged to study in depth the particular crimes that have historically occurred at their facilities.

Assault-Type Crimes (Assault, Aggravated Assault, and Murder)

Assault, aggravated assault, and murder are evaluated together because their threat dimensions are similar. Assault-type crimes can escalate to aggravated assault crimes and aggravated assault can escalate to murder. The facility's situational elements may either encourage or discourage assault-type crimes. For example, as noted earlier, bars, nightclubs, and other venues where alcohol is served can be prone to assault-type crimes because alcohol tends to lower inhibitions and cause people to become more combative. South American soccer games are also more prone to assaults than American football games, primarily because of the passion of the fans. European soccer fans were satirized in the 1990s in an old *Saturday Night Live* skit about Scottish soccer hooligans who were so aggressive and passionate about their teams that they beat each other up. It is the task of the security decision maker to determine what threats are inherent to their facility. Residential communities, such as apartment buildings, may also suffer from assault-type crimes. Demographic and crime data would indicate that interpersonal, or domestic, assaults are more likely to occur in lower socioeconomic communities.

Criminological data indicates that assault-type crimes are committed by and against people who are similar in age, race, and gender. Thus, for assault-type crimes, the target's characteristics will often be substantially similar to those of the adversaries. Schools provide a good example of this correlation: in schools the victim and the offender are typically the same age and race because of the very nature of schools. Security decision makers can identify threats using this information.

Adversarial motivation and capability for assaults, aggravated assaults, and murders are typically rooted in emotional issues. Here again, soccer games provide the emotional, passionate high wherein fans may express their excitement in violent ways. Gun control laws are society's method for reducing the capability of adversaries to commit violent crimes. Though sometimes effective, gun control laws are certainly not without controversy. Many schools have implemented zero tolerance policies for guns to protect students. Some have even installed metal detectors to reduce the capability of bringing a gun into a school.

Target selection methods vary according to assault-type criminals. Although many assaults are driven by anger, some targets are carefully selected. Serial killers, for example, normally select their victims based on certain characteristics. Ted Bundy's victims were attractive girls with long, dark hair normally parted down the middle, while Jeffery Dahmer's victims were young males.

How do security decision makers prevent assault-type crimes? Those assaults, aggravated assaults, and murders that are not interpersonal are called stranger-initiated. Stranger-initiated assault-type crimes are easier to prevent than interpersonal assaults. Opportunity-reduction strategies include deterrence and response measures designed to create an environment perceived by the adversary as risky with a high chance of apprehension. Some assault-type crimes are very difficult to prevent. Interpersonal assaults, for instance, which occur between two known parties, are not typically deterred by security measures. For example, an apartment community may have a security fence and gate, parking lot lighting, and high security locks on doors, yet none of these measures can prevent a husband from striking his wife.

Robbery

Robberies are a big concern for most security decision makers and adversely affect business in a number of ways, including causing injuries, loss of property, negative reputation, and liability. There are two primary types of robberies: robberies of people and robberies of business. Bank robberies, shoplifting escalation, and retail holdups are business-related robberies; personal robberies include car-jacking, purse snatching, and mugging.

A facility's situational characteristics that contribute to a robbery-prone environment are easily identified by experienced security decision makers once they understand the precise type of robbery impacting the property. Poor lighting, the existence of hiding places, and unprotected assets provide ample opportunity for personal robberies. Poor employee training, unfettered access, and easy escape routes can create an environment conducive to business robberies. Among the better security concepts developed in recent years is improved parking lot design at retail stores and shopping malls. Additional curbing has been used to control the flow, direction, and speed of traffic, all of which constitute a deterrence to robbery and other crimes by creating obstacles to a robber's escape from the property.

Robbery target characteristics depend on the nature of the robbery. Purse snatchings obviously require an unaware female holding a purse, whereas carjackings are limited to areas where cars can travel or park. Why does a convenience store experience more business robberies than another convenience store located across the street? Poor lighting and store windows cluttered with signs and posters at the robbery-prone location might be contributing factors.

A robber's motivation is typically a rational balancing of risk and reward. If an asset is valuable (high reward) and unprotected (low risk), the probability of attack increases. Banks are susceptible to robbery because of the high reward for perpetrators. As such, bank security professionals institute various strategies for protecting bank assets. Capability is dependent on the type of robbery executed. Bank robberies require greater skill than simple purse snatchings.

What does a robber look for in an attractive target? Regardless of the type of robbery contemplated, targets are rarely selected randomly. Obviously, the balancing test of risk and reward is a factor. Purse-snatch robbers seek out unaware women to target, with the reward being higher in higher socioeconomic areas.

Like assault-type crimes, robbery opportunity-reduction strategies vary with the type of robbery occurring on the property, but generally increased physical security measures, enhanced natural and artificial surveillance, and security personnel provide protection. Banks may implement silent alarms or install bullet-proof glass to protect against robbery. Residential homeowners may install alarm systems with sensors mounted on all entry points and may even have the alarms monitored by a private company or the police. Convenience store owners may remove obstructive signs from windows to increase surveillance both into and out of the store. Car manufacturers have also started to include automatic locks on their vehicles to prevent car-jacking. Often, simple and inexpensive changes in policies and procedures can have a positive impact on robbery reductions.

Theft and Auto Theft

As is true of robbery, there are many types of thefts. Situational elements at a facility are a primary determinant of the types of theft that may occur. Retail stores are prone to shoplifting, while large parking structures experience auto thefts and burglaries of motor vehicles (BMV). Laundromats may experience high levels of theft from the coin-operated machines, and schools may report a large amount of bicycle thefts.

Each year the automobile insurance industry releases data on the nation's most frequently stolen cars and trucks. Although it might surprise some readers that BMWs and Mercedes don't make the top ten list, it won't be news to most security professionals. Cars such as Hondas, Toyotas, and Chevrolets are more easily hidden among the masses, and they are also more easily fenced or stripped for use in other cars. It is for these characteristics that certain cars are more likely to be stolen than BMWs.

The thief's motivation and capability are subject to the risk- and reward-balancing test. Grocery stores, for example, often suffer from high levels of baby formula and over-the-counter drug thefts because of the high value of both items. These items are often turned over to a fence, or middle man, who will pay decent amounts to the thief and then sell the items back to the retailers. The thief's capability is limited only by his or her skills and creativity. Some thieves work alone committing petty thefts, stealthy thieves may be pickpockets, and organized thieves may band together to commit larger thefts.

Normally, an asset has the same value and attraction to property owner and thief alike. Jewelry, for example, is both valuable and easy to conceal because of its size. Financially motivated thieves will seek assets that they can later sell for a profit. Personally motivated thieves will steal assets such as drugs or expensive basketball shoes that they can personally use.

Opportunity-reduction strategies for theft range from the simplest to the most complex, from moving an asset out of sight to installing vaults, alarms, and camera systems. Auto theft reduction may take the form of simple alarm systems to monitored tracking systems. Some grocery stores have now begun to store baby formula and over-the-counter drugs in locked cabinets. Clothing retailers use electronic security tags to prevent their clothes from being shoplifted. Here again, in order to implement appropriate countermeasures, the security decision maker must fully understand the type of theft experienced at the facility.

Political Crimes (Terrorism)

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.

What situational elements of a facility lend themselves to terrorism?. Without delving into the politics of terrorism, it is safe to say that groups angry with a government's policies and actions can create the justification for terrorists to take action. In 1995, Timothy McVeigh bombed the Murrah Federal Building in Oklahoma City because of his outrage over the U.S. government's actions in Waco against the Branch Davidians in 1993. And Osama Bin Laden claims that one of the reasons al-Qaeda is angry at America is because the United States established a military base in Saudi Arabia during the first Gulf War.

The Adversary's Target Election Factors

Obviously, national monuments and critical infrastructure assets are the terrorist's most likely targets; areas where large numbers of people (targets) gather make good terrorist targets. Therefore, bus stops are frequent terrorist targets in Israel, while trains have been attacked in both Great Britain and Spain. In the United States, one of the homeland security specialists' greatest fears is a terrorist incident at a large significant sporting event, such as football's Super Bowl or baseball's World Series games. As Timothy McVeigh taught government security professionals, government buildings with a concentrated level of enforcement agencies such as the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco, and Firearms make better targets than government buildings with agencies such as the Social Security Administration or the Equal Employment Opportunity Commission.

Reducing the motivation and capability of terrorists is the prime method for reducing the threat of terrorism. It might make one wonder whether Osama Bin Laden considered the risk- and reward-balancing test before launching the September 11 attacks. For now, that issue will be left to the experts to figure out. Reducing capability, as we have already discussed, is a good way to lower the threat level. Certainly, too, cutting terror funding and destroying training camps are good opportunity-reduction strategies.

The Homeland Security Advisory System

Despite its relatively short existence, the most well-known threat-rating scale is the Homeland Security Advisory System. The system is qualitative in nature with color-coded levels indicating the threat level. The rating scale includes general responses and countermeasure deployments that should be considered, depending on the nature of the organization the security decision maker is protecting.

1. Low Condition (Green)—This condition indicates a low risk of terrorist attacks.
   - Refine emergency operation plans and business continuity plans.
   - Conduct emergency response drills.
   - Train personnel in emergency response.
   - Assess vulnerabilities and develop mitigation strategies.
   - Continue to monitor threats.
2. Guarded Condition (Blue)—This condition indicates a general risk of terrorist attacks.
   - Follow the responses and countermeasures described under Level 1.
   - Ensure communications with designated emergency response personnel.
   - Review and update emergency response procedures.
   - Provide employees with information that would strengthen its ability to act appropriately.
3. Elevated Condition (Yellow)—This condition indicates a significant risk of terrorist attacks.
   - Follow the responses and countermeasures described under Levels 1 and 2.
   - Increase surveillance of critical assets.
   - Coordinate emergency plans as appropriate with other businesses and law enforcement.
   - Assess and refine mitigation strategies with the characteristics of the current threat.
   - Implement additional contingency and emergency response plans as needed.

4. High Condition (Orange)—This condition indicates a high risk of terrorist attacks.
    - Follow the responses and countermeasures described under Levels 1, 2, and 3.
    - Coordinate security efforts with all organizational departments and law enforcement.
    - Take additional precautions at public events and possibly consider alternative venues or even cancellation.
    - Execute appropriate elements of emergency response and business continuity plans.
    - Restrict facility access to essential personnel only.
5. Severe Condition (Red)—This condition indicates a severe risk of terrorist attacks.
    - Follow the responses and countermeasures described under Levels 1, 2, 3, and 4.
    - Prepare emergency response personnel.
    - Preposition emergency response equipment.
    - Evacuate the facility.

Basic Threat Assessment Report

The threat assessment is based on the Uniform Crime Report (UCR) data from the City of Stafford Police Department. Using the Federal Bureau of Investigation's UCR coding system, all crimes were reclassified to meet the FBI standard. Twenty-four (24) crimes were analyzed for each facility for the period January 1, 2002 through December 31, 2004. These crimes include:

1. Murder
2. Rape
3. Robbery
4. Aggravated Assault
5. Burglary
6. Theft
7. Motor Vehicle Theft
8. Arson
9. Other Assaults
10. Forgery and Counterfeiting
11. Fraud
12. Embezzlement
13. Stolen Property—Buying, Receiving, Possessing

14. Vandalism
15. Weapons—Carrying, Possessing, etc.
16. Prostitution and Commercialized Vice
17. Sex Offenses
18. Drug Abuse Violations
19. Gambling
20. Offenses Against the Family and Children
21. Driving under the Influence
22. Liquor Laws
23. Drunkenness
24. Disorderly Conduct

Site 01

Administrative Offices

Property crimes, including vandalism, theft, and auto thefts are the primary concerns at the administrative offices. During the three years analyzed, no crimes against persons occurred on the premises.

Site 02

Park Meadow

Park Meadow is a medium population facility located on the Town's west side. There have been a number of violent crimes, primarily robberies, at this location; however, there has been a significant downward trend since 2002. Property crime is considerably low at Park Meadow despite the violent crime level. Crime rates for this property were calculated using the facility's population and violent crimes for each year analyzed. In 2002, the violent crime rate was 54.8 violent crimes per 1,000 persons, while 2003 marked the beginning of the downward trend to 30.8 per 1,000 persons, and 2004's rate of 24.2 per 1,000 persons.

Site 03

Haley Gardens

Haley Gardens, a medium population facility centrally located, has seen a remarkable drop in crime in 2004 with no violent crimes occurring during the past year. This is likely the result of enhanced security measures implemented at the facility in 2003. Burglaries of motor vehicles (BMV's) and acts of vandalism have also decreased.

Site 04

Waverly

Waverly is a low population facility located on the Town's south side. There have been very few violent crimes on the premises, and none occurred in 2004. Property crimes, on the other hand, are still prevalent.

Site 05

Autumn Hill

Autumn Hill is a medium population facility located on the Town's west side in close proximity to Park Meadow. This facility also received additional security measures in 2003, and both violent and property crime declined substantially in 2004. The violent crime rate dropped from 30.7 in 2003 to 6.0 per 1,000 persons in 2004.

Site 06

Broadknoll

Purse-snatch robberies are the primary crime occurring at Broadknoll. While the rate of violent crimes dropped in 2004, there is still a high threat level. In fact, property crime escalated significantly in 2004. Despite a decrease since 2002, the threat level is notable considering this is a low population facility.

Site 07

White Sands

White Sands is a high population facility with a high threat level. Thirty percent of all the robberies at the ten facilities occurred at White Sands. Though the crime rate has dropped from 2002, the threat level is still significantly high. In addition to the high robbery rate at this location, two rapes occurred, though both incidents were domestic in nature and posed no threat to other residents. One murder also occurred at White Sands and is still under investigation by the Police Department.

Site 08

Ashland Grove

Ashland Grove is a medium population facility located on the north side. Similar to Broadknoll, purse-snatch robberies are the primary concern; however, the violent crime rate is relatively low. BMVs are also a concern as most thefts occurring on the property are burglaries of motor vehicles. The violent crime rate doubled in 2004; however, there was still a low level of crimes of violence.

Site 09

Meadow Gardens

Meadow Gardens is the highest population facility of the 10 sites analyzed. Given this high population, the violent crime rate is relatively low in comparison to the other sites, however the crimes tend to be more violent in nature, with two rapes and numerous car-jacking robberies. Domestic assaults are also prevalent.

Site 10

Hyde Heights

Hyde Heights is a low population facility located on the Town's east side. No violent crimes occurred during 2004 on this property. Thefts are a major concern on this property, with the vast majority being Burglaries of Motor Vehicles.

Site 11

The Terrace

Veteran's Terrace is a medium population facility on the Town's north side and is considered by residents and management to be a crime-prone property given its size. UCR data confirms this with the highest 2004 violent crime rate of all the properties. Two murders and five rapes and a significant amount of robberies and aggravated assaults in the past three years have led to a high threat level and a general fear of crime by residents.

Summary

Of the 10 residential properties, White Sands, The Terrace, Park Meadow, and Broadknoll have the highest threat level and fear of crime by residents. Robberies are most prevalent at White Sands, and crime trends are discernible at each property. Simple assaults were also common at all facilities, although most were domestic in nature and not likely a result of inadequate security. Property crimes at the 10 residential facilities include thefts and auto thefts; however, burglaries of resident apartments are notably absent.