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