THREAT ASSESSMENTS:
The Final Pillar of a Tailored Security Program

by ITG Consultants, Inc.

©2014. All rights reserved.
INTRODUCTION

Threat assessments are the final, but crucial, component in developing a comprehensive safety and security program. Threats are imminent in nature, affording organizations little or no time to formulate an appropriate response. This makes proactive evaluation and a planned, tailored response essential. Conducting a threat assessment, continuously monitoring the threat’s evolution, and utilizing the assessment’s findings, is imperative. To succeed as an organization or business in the face of devastating natural disasters or malicious criminal actions requires both awareness of those threats and a plan to address them immediately.

Though the words are often used interchangeably in common vernacular, for the purpose of security planning, threats are distinct from risks. Risk, in security terms, is simply the possibility of loss, whereas a threat is the impending manifestation of risk in the near-term timeline. For example, an organization might find itself exposed to risk in day-to-day operations should a natural disaster arise, but that risk becomes a threat when that natural disaster begins to occur. Conversely, the threat can dissipate while the underlying risk does not. Threats are related to, but distinct from, vulnerabilities, as well. A threat causes the most damage to an organization at points of vulnerability, whether through environmental causes or malicious human intent.

HISTORY OF THREATS

Threats typically arise in one of two forms: natural or human. Natural threats are largely unchanged over the course of history: environmental disasters such as hurricanes, earthquakes and tornadoes occur in the same form they always have. Yet population growth and centralization in large metro areas, as a modern development, raise the impact of those disasters to a much higher level.

Threats posed by human malicious intent have evolved in tandem with growth of civilization and evolution of technology. The oldest social groups on record undoubtedly targeted one another in some fashion, which still occurs in today’s social and political landscapes. The tools and weapons available in the current day, however, shape the manifestation of those threats. Advances in technology have been utilized for criminal and inhumane purposes. The advances and evolution of threats driven by human intent necessitate specialized skill to assess and formulate appropriate responses to them. This paper seeks to specifically address human threats.

Being able to recognize that a threat is being made isn’t always as simple as it might seem. Threats can be vague or ambiguous, perhaps causing the target
Threat Assessments: The Final Pillar of a Tailored Security Program

by ITG Consultants, Inc

To dismiss them without thought or consideration. Knowing what constitutes a threat is of fundamental importance. The Critical Incident Response Group delineates threats into four categories:

1) **Direct threats** are the most explicit threats, noting specific action to be taken against a specific target, and perhaps on a specific timeline. “I’m going to kill you before the sun sets!”

2) **Indirect threats** are far less explicit, implying a possibility or ability to cause harm. In most cases, they are tentative. “If I wanted to, I could cause this company to cease to exist!”

3) **Veiled threats** lack definite terms and are meant to cause the target concern by lacking specific meaning. By nature, they are ambiguous. “Everyone here would be better off if you were dead.”

4) **Conditional threats** pose action against the target that will occur if specific terms or demand aren’t met. “If I don’t get your recommendation for a promotion and a raise, I’ll see to it that you’ll be six feet under!”

Many persons make threats yet never carry out the actions. Of those who make a threat and do carry it out, most make a direct threat. Yet those who do consummate their intent make public threats merely 13% of the time. For example, the perpetrators of the 2013 Boston Marathon bombing made no threat, publicly or directly to the event planners. The fact that most people who commit targeted violent acts do not communicate their intentions by making threats complicates the process of planning to respond to them.

**ISSUES AND MAIN POINTS**

**Goal of threat assessments:**

The expressed purpose of conducting a threat assessment is to identify threats and then prepare a plan of action with which to respond to or counter them. A previously completed risk assessment provides the vantage point from which to then evaluate potential threats, determining whether any of those identified risks are escalating to a pending threat. The threat assessment refines the evaluation of risk and tailors the response to account for the ways the threat could be manifested and the severity of impact on the organization. The risk assessment process should have resulted in the development of preliminary contingency plans to address the risk. The threat assessment tailors those plans

---


Threat Assessments: The Final Pillar of a Tailored Security Program by ITG Consultants, Inc

To respond to the now-pending threat. Threat assessments, as the final step in developing a security program, cannot be relegated to a shelf in the office. If a threat has been identified in the course of conducting an assessment, that threat must continuously be monitored until it has dissipated.

**Purpose of threat assessments:**

1) To determine the credibility of that threat and the likelihood it will be carried out.

2) To identify any person or group posing a threat to the organization.

3) To approximate the means and method by which the person or group would execute their threat, their ability to do so, and the timeline on which they might act.

**Challenges**

Knowing how to conduct a threat assessment and determine whether identified threats are credible poses a challenge in many organizations. Some entities have trained personnel on staff who are charged with evaluating potential threats and have cultivated the skill of doing so. Yet even in-house security personnel or human resource managers may wish to enlist the services of private security and mental health professionals who can help identify threats and hone the predictions of human behavior related to them. Furthermore, trained security personnel, or individuals with experience in law enforcement, will aid in interpreting the findings of an assessment. They can help identify the likely means and methods by which a threat could be enacted and assist in formulating actionable policies to tailor the planned response.

Privacy laws pose problems in garnering information on potential threats. HIPPA protects private medical information that might aid in establishing whether an individual might execute threatened action. FERPA protects student records that document previous discipline issues that could help establish the likelihood (or lack thereof) a student would enact a threat. Similarly, criminal history records are subject to laws governing the release of that information. The same is also true of juvenile criminal or sealed court records. Privileged communication between doctors, lawyers and spouses dictate that the protected parties cannot be legally compelled to release information that might aid in establishing the credibility of a threat.

Budgetary considerations are also legitimate obstacles to conducting threat assessments. However, the potential losses incurred from a threat being successfully executed, as measured in dollars, injury or loss of life, are exorbitant when set alongside the comparatively nominal cost of the assessment. Contracting with security and mental health professionals to facilitate the assessment process will incur costs comparable to that of a lawyer dealing with routine legal matters.
Another challenge associated with evaluating the credibility of a threat is ascertaining the mental state of the person making the threat. In some cases, enlisting the expertise of a mental health professional (or criminal profiler, as required) may be warranted. However, many times in-house resources have enough of a knowledge base to aid in establishing a basis for addressing that objective.

**Obstacles to overcome:**

Many organizations fail to conduct the preliminary risk assessments, establish the indicated contingency plans and appoint a team to oversee the process of assessing threats during the initial security planning phase. As a result, when the crisis of a threat is thrust upon them, they are forced to operate from a completely reactive posture. This reactive posture can utilize only one tool when a threat is imminent: the Boyd Cycle, also known as the OODA Loop. OODA stands for Observe, Orient, Decide and Act. Without a plan of action formulated from a threat assessment, responders will have to rely on the observations they can readily make and will be forced to orient themselves to the situation, and assess the resources that can be brought to bear, during a time of extreme stress or shock. Then, decisions are made and acted upon. Yet with every new development presented by a threat, the OODA loop must begin anew, making the Boyd cycle not only reactive in nature, but also time-consuming and less effective in mitigating threats. With a completed threat assessment and a related action plan formulated on the assessment, organizations and their personnel are equipped to meet the challenges of a threat and more able to formulate an appropriate response in spite of extremely stressful conditions.

Some organizations develop issue-specific policies after a crisis has occurred, resting on the benefit of hindsight and post-incident review. If the only time policies are developed is post-incident, the policy manual is merely a compilation of ad hoc, reactive responses to occurrences, instead of being a comprehensive, proactive, and strategic manual. Documenting and developing policies in the wake of a problem is valuable for responding to future similar incidents. Yet without a policy or procedure in place, the first time an incident of that nature occurred, the staff would be ill equipped to manage it. Contingency plans, formulated upon risk assessment findings, pre-empt such occurrences by preparing in advance. Conducting a threat assessment when the underlying risk escalates to a threat is what tailors the planned response to address the specific threat. In the absence of a contingency plan against a specific risk factor, the threat assessment serves as the initial step in developing a response.

---

BEST PRACTICES

Who should assess?

Organizations, businesses, government entities and schools should all develop the capability to conduct, and then engage in the practice of, assessing threats as part of a comprehensive security program. Regardless of size or scope of work, all entities can benefit from the exercise and could potentially avert catastrophic impact resulting from threats.

When to assess?

There are two occasions upon which a threat assessment should be conducted. The first is after the completion of a risk assessment. At this juncture, a threat assessment focuses on a particular risk to determine whether it is currently a pending threat, not merely a risk. The second is upon receipt of a threat in one of the forms noted previously or upon clear indication that a threat is about to materialize.

Who is responsible?

The person or group within the larger entity charged with the task of conducting the threat assessment will vary according to the organization. In the case of a public/government office, that duty is likely to fall within the purview of law enforcement. A corporate firm of reasonable size may have security on-site, whether as an in-house operation or outsourced to a security firm. Smaller businesses may allocate these duties as part of an employee or executive’s larger role. Public educational institutions may rely on the school resource officer, if one is assigned, whereas private academic institutions may need to hire a consultant.

In any of these scenarios, having a multi-disciplinary, team approach to conducting the assessment is most conducive to obtaining thorough and conclusive results in the assessment. Establish a threat assessment team (TAT) comprised of personnel from across the organization. Representation from across the organization, and perhaps from outside it, provides different perspectives with which to build a more comprehensive understanding of the threat. In the case of an academic institution, the TAT should include administrators, counselors, and school resource officers. Corporations should involve human resources, information technology and executives. According to the type of threat, contracting a forensic or criminal behavior expert may be warranted, as well. If an identified threat indicates the likelihood of specialized weaponry, enlisting an expert in that field would be necessary to have on the TAT. Any threat that constitutes a crime if enacted must be reported to law enforcement officials, who would then become part of the team. If the threat doesn’t constitute a crime then the addition of a private security practitioner to the team will provide valuable assistance and guidance.
Who follows through?

Merely conducting an assessment is insufficient. Determining whether a threat has been made, and establishing its credibility, likelihood and severity is the starting point. The value in having completed the assessment is truly found in the resulting plans that will deter, avert or mitigate the damages that could result from the threat being enacted. It is especially important to know when to engage law enforcement officials based on the nature of the threat (which may be a crime in itself) and the potential impact of its enactment.

HYPOTHETICAL CASE ILLUSTRATION

The following scenario depicts the workflow that precedes and includes threat assessments:

**Step 1:** A corporation conducts a risk assessment and decides to prioritize the potential risk that the CEO might be targeted if a workplace violence incident arises.

**Step 2:** A vulnerability assessment is conducted and the following implementations occur to bolster defenses:

- Corporate access controls are enhanced to include photographic identification cards and proximity card readers, permitting the system to deny access to terminated employees even if the badge is not returned.
- Closed circuit television systems are installed at the workplace and in the home of the CEO.
- The CEO is trained in personal security, evasive driving and detecting surveillance.
- Due to the CEO’s frequent international travel a vendor is retained to assess risk in foreign countries.
- Establishment of 24-hour hotline security department and active monitoring of internet for issues relevant to the corporation’s business and/or the CEO himself.
• A contingency plan is written to specify actions to be taken if the risk of the CEO being targeted escalates to a threat. The plan includes hiring of outsourced executive protection agents to support CEO with direct security while threat issue is navigated. The executive protection program will include a security driver, a personal security officer, and an advance agent, for a total of three agents.

• A threat assessment team (TAT) is identified.

**Escalation of risk to threat:** A hostile employee termination occurs. The CEO’s executive assistant receives a call from the former employee in which he makes a direct threat against the life of the CEO. The contingency plan is implemented and the company obtains the services of a previously vetted, licensed vendor. The local law enforcement agency is notified, also as per the contingency plan, and it is determined that the mere threat constitutes a crime. Law enforcement alerts the corporation that an arrest attempt was unsuccessful and the former employee remains at large.

**Step 3:** The threat assessment team convenes, conducts a threat assessment, and realizes the terminated employee served in the military as a Demolitions Sergeant in the US Army Special Forces with two combat tours in Iraq. Though not diagnosed with Post-Traumatic Stress Disorder upon discharge, the mental health professional on the TAT indicates that the behavior he exhibited that precipitated his termination is consistent with such a diagnosis.

While the contingency plan written after the risk assessment provided a good baseline response, the TAT realizes the executive protection effort is not robust enough to avoid, detect and counter the Improvised Explosive Device threat that this person is fully capable of delivering.

**Step 4:** The formulated response must be adjusted to meet the demands of this specific threat. The following additional implementations are made:

- Addition of extra executive protection agents to the team to conduct more thorough sweep of areas the CEO will utilize.
- Services of outsourced explosives detection dog team are secured.
- The CEO’s public exposure and time/place predictable event participation is curtailed until the person is located and arrested.

**Resolution:** The person is located and arrested. The threat assessment process does not cease, however. This person is likely to make bail and be released, so the TAT continues to meet regularly to evaluate the status of the threat, possibly hiring a private detective agency to conduct periodic surveillance of the person. Active monitoring is sustained until (a) the threat has dissipated and it no longer credible, (b) the high level of executive security support can
no longer be afforded, therefore the threat must be tolerated to some extent, or (c) the individual is convicted and incarcerated (though the threat should be evaluated again when the individual is released).

CONCLUSION

Conducting a threat assessment doesn’t ensure crises can be averted. Yet through continuous monitoring, having an awareness of threats positions organizations to respond to them effectively when they arise. Together with the foundational elements of risk and vulnerability assessments, the findings of a threat assessment empower businesses, schools and government entities to employ refined countermeasures in a composed, effective manner.

Given the immediacy of potential impact caused by threats, conducting assessments on an on-going basis is an organization’s best strategy. Threat assessments are the final, but indispensible, step in developing a comprehensive plan for safety and security.
ABOUT ITG CONSULTANTS

ITG Consultants, Inc., is a Veteran-owned small business based in Pennsylvania providing training, consulting and security management services.

David L. Johnson, president of ITG, is certified in Homeland Security – Level V, by the American Board for Certification in Homeland Security, previously served on its Executive Advisory Board and also serves as Chairman of The American Board for Certification in Dignitary and Executive Protection.

Gale R. Ericksen, vice-president of ITG, is a Certified Protection Professional by the American Society of Industrial Security and is certified in Homeland Security – Level III.

Together, the leadership team of ITG Consultants has nearly 6 decades of experience in international law enforcement, executive and dignitary protection and training.

For more information or a no-obligation discussion, visit our website at www.itg4.com or call (866) 904-4ITG.