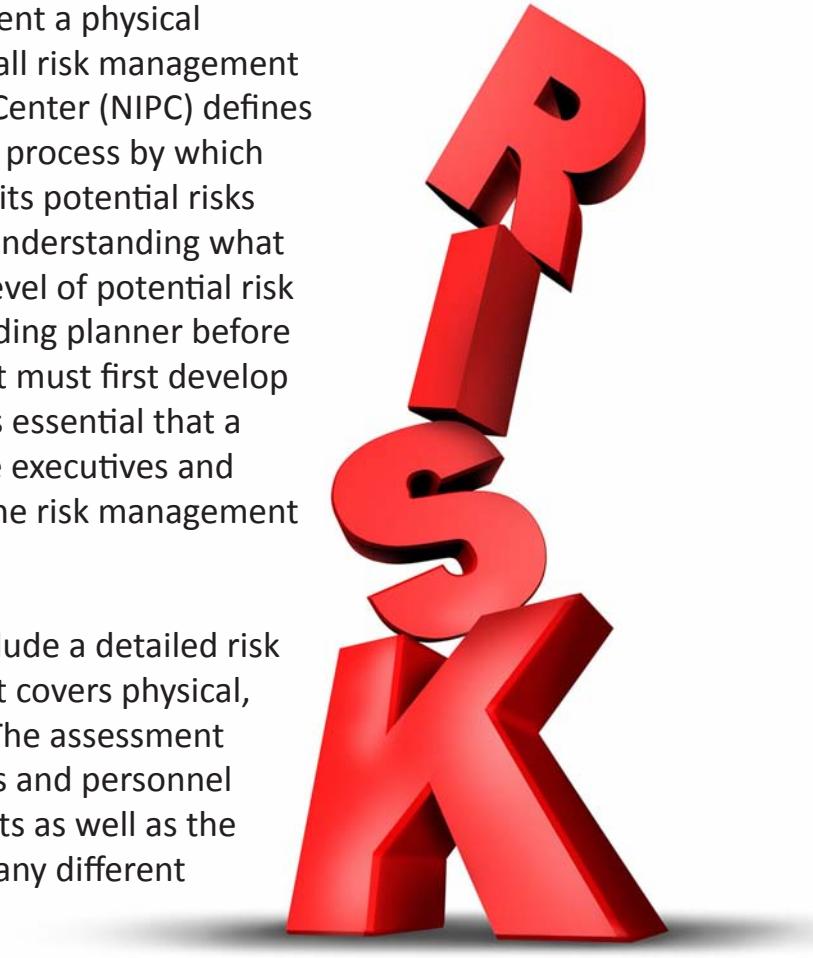
HIGH IMPACT TRAINING SOLUTIONS®

HITS

RISK AND THREAT ASSESSMENT

RISK AND THREAT ASSESSMENT

Before any organization can successfully implement a physical security program, they need to consider an overall risk management strategy. The National Infrastructure Protection Center (NIPC) defines risk management as "a systematic and analytical process by which an organization identifies, reduces, and controls its potential risks and losses." Hiring a security firm without first understanding what threats the organization is exposed to, and the level of potential risk from these threats, is equivalent to hiring a wedding planner before you have met the bride. Corporate management must first develop a comprehensive risk management strategy. It is essential that a risk management team be set up from corporate executives and security management to evaluate and develop the risk management strategy.



The corporate risk management strategy will include a detailed risk and threat assessment and a security survey that covers physical, informational, and operational considerations. The assessment will look at total organizational assets, properties and personnel and evaluate vulnerabilities from potential threats as well as the level of risk posed by these threats. There are many different methodologies used to qualify and quantify risk. However, most risk management strategies will contain four major functions:

1. **Identification of potential threats**
2. **Evaluate the level of risk from these threats**
3. **Assess the vulnerability of critical assets to these threats**
4. **Propose ways of mitigating risk and prioritize risk reduction measures**

Identifying Threats

Organizations face a variety of threats every day. A good threat assessment will consider an all hazards approach, meaning all conditions are evaluated, whether they are natural or manmade. Additionally, threats will be evaluated at varying scales, such as those threats affecting a local area or those impacting an entire country. This strategic perspective helps to better understand the broader impact threats have on an organization.

Threats are typically qualified as High, Moderate, or Low. These categories are determined by the likelihood of occurrence, vulnerability of the organization, and other factors. For example, an organization located in a third world country known for periodic violence could be categorized as having high-threat vulnerability. Factors contributing to threats can be determined by evaluating the following:

- **Political**
- **Environmental**
- **Economic**
- **Social**
- **Technological**

In business, these factors are often referred to as a PEEST analysis. The five factors have significant strategic influence on the strengths, weaknesses, opportunities, and threats a company faces on a daily basis. For the purposes of a risk management strategy, these factors are very useful in determining vulnerabilities within the micro and macro conditions that a company finds itself.

Evaluating Risk

Within each threat category, there are four risk levels. The first level of risk is considered negligible, as it has little likelihood of loss and a very low consequence. Such risks will not affect daily business operations. However, such risks may still need to be considered, as they may have a safety implication for the organization. For example, a negligible security risk may be someone falling and incurring a minor injury. The second level of risk considers the effects of short-term disruptions to organizational performance from a threat. A minor power outage lasting a few hours may fall into this category. The third level of risk considers the ramifications of damage beyond the immediate organization to external customers, suppliers, or partners. Such disruption may be temporary or permanent to organizational performance and business operations. An example of a third level risk might be a cyber-attack to corporate networks, which could have serious implications to business operations. Finally, the fourth level of risk looks at devastating consequences that have enormous impact and may affect public safety, potential loss of life, and financial stability of the organization. An example of a fourth level of risk might be a terrorist attack on the corporate structure. A simple method of visualizing the risk categories is to create a risk matrix. The risk matrix combines a consequence and likelihood of risk to provide a range or ranking to the risk levels.

Accessing Vulnerability

Once the threats have been identified and risks levels determined, the security assessment will look at vulnerabilities to the organization's security program. A vulnerability check list is often useful to evaluate the physical security of a structure and its potential weaknesses. However, checklists alone are not adequate. Assessing vulnerabilities requires interviewing employees, conducting field surveys of the site and building structure, and reviewing the security manual for the organization. When interviewing staff, it is critical to include all staff – from the janitorial department to the security personnel. The result will be a more comprehensive assessment. A vulnerability assessment should also include recommendations for fixing security issues and a proposed budget for the costs to these fixes.

Mitigating Risk

Risk management is about balancing the cost of mitigating risk versus the cost of potential damage to the organization from the associated risk. The method of mitigating risk is through controls. These controls may be in the form of technologies, such as CCTV cameras, or it may be the physical presence of security officers patrolling the grounds. The risk and threat assessment will determine what security parameters are needed, based on the vulnerability to threats and corresponding level of risk. No one security control is enough to completely mitigate risk. Instead, a series of mitigation measures are needed to remedy vulnerabilities. This is often referred to as defense in depth. Defense in depth simply means it is more difficult to defeat a complex layered approach to security than it is to penetrate one security control. However, most organizations will evaluate the cost of mitigating risks based on the likelihood of occurrence and the probability of damage to the organization. For example, a retail outlet may know that shop lifting will occur. However, they balance the annual loss to theft with the cost of hiring a security team and determine what level of security they want in place. The more vulnerable an organization is to a potential threat, balanced with the potential damage to the organization, will determine the security response.

Another aspect of risk management is the policies and procedures put in place to control human behavior. When it comes to security, the use of best practices to create a culture of security consciousness goes a long way to keeping an organization safe.

Periodic threat and risk assessments are necessary to evaluate the security program. A risk assessment needs to be completed at least every three years, and perhaps annually, depending on the type of facility and other risk factors. Risk assessments should be done internally by the risk management team; however, having an outside firm review the security program and all security controls, in order to make recommendations for improvement is also a good idea.

References

Gillick, Terrence J., *Assessment and Mitigation of Risks to Physical Security, Information Security, and Operational Security*, TradePress, http://www.facilitiesnet.com/security/article/Taking-Security-To-the-Next-Level--2566#

Ahrens, Sean A., *Security Analysis Should Go Beyond Checklists, Include Recommendations*, TradePress, http://www.facilitiesnet.com/security/article/Security-Analysis-Should-Go-Beyond-Checklists-Include-Recommendations--11405#

Peterson, Kevin E., *Security Risk Management*, Certified Protection Officer, 8th Ed., International Foundation for Protection Officers

Wikipedia, PEST Analysis, http://en.wikipedia.org/wiki/PEST_analysis

HITS Institute is a division of:

smarthorizons.
The Smart Choice in Innovative Training Solutions



All images used according to license permissions. ©2012 123RF Limited and ©2012 Jupiterimages Corporation