Guidepost

PHYSICAL SECURITY. RISK MITIGATION. WHERE TO BEGIN?

Why are you operating your physical security program? What threats are you trying to protect against? What specific risks to your organization and enterprise are you trying to mitigate?

If you cannot quickly and succinctly answer these questions, you may have skipped the critical step to developing a foundation for your physical security program – conducting a Threat and Vulnerability Risk Assessment (TVRA). Basing your physical security program on the results of a formal TVRA process defines the reasoning and goals of the program, provides the information needed to make informed decisions on how to allocate limited resources, and aligns the program with the core business strategy.

The big picture:

Traditionally, a physical security risk assessment is a qualitative and quantitative evaluation based on the vulnerability of assets to threats. The qualitative portion evaluates elements such as how employee recruitment and retention is affected by the perception of safety and security. The quantitative portion estimates monetary loss using the probability times impact equation. Both the qualitative and quantitative evaluations are relative – comparing various threat scenarios on a continuum from low probability/low impact events to high probability/high impact events.

Why it matters:

Fundamentally, threats take advantage of vulnerabilities in order to gain access to assets. Therefore, it is important to clearly identify and document your organization's critical assets. Asset identification starts with people – your most important asset – and includes tangible goods such as facilities and equipment. However, it is important not to forget intangible assets such as reputation and intellectual property. Risk reduction activities focus on addressing vulnerabilities to reduce a threat's access to these assets.

Architectural, operational, and technological countermeasures and mitigation measures can be applied to address the vulnerabilities in order to lower the residual risk.

- Architectural countermeasures include doors and door hardware, lighting, fences and gates, signage, and landscaping as well as the security zoning layout of buildings and facilities.
- Operational countermeasures include employee, visitor, and contractor identity management, alarm monitoring and response, security personnel staffing, business continuity planning, emergency preparedness, and crisis management as well as the supporting security policies and procedures.
- Technological countermeasures include electronic security systems such as access control, video surveillance, intrusion detection, and security communications as well as incident management software and alarm metrics tracking and reporting.

These mitigation measures are mutually supporting and act interdependently to directly respond to vulnerabilities identified in the TVRA process.

The effectiveness of the physical security program is evaluated over time using the Plan-Do-Check-Act (PDCA) cycle. This will help determine where risks and vulnerabilities remain, or have changed or shifted, as a result of the applied mitigation measures. The assessment and evaluation process then continues to apply additional mitigation measures to the evolved threats and vulnerabilities to further lower the residual risk.

The goal is not to eliminate all risk, as this is not realistic or feasible. Not only is such a goal cost prohibitive, but it interferes with normal business operations and restricts opportunity risks which could produce desirable business outcomes. Instead, the goal is to reduce residual risk to an acceptable level with manageable identified risks.

Tailoring your physical security program to reduce the risk from specific, identified threats and vulnerabilities based on the TVRA process allows physical security risk management to be a business enabler. It's imperative that your physical security program is not siloed. It must be incorporated into supporting initiatives and operations and work in alignment with organizational objectives and core mission goals.

What's next:

Independent third-party security consulting firms leverage their experience with many different types of organizations and threat environments to conduct TVRA assessments. By incorporating lessons learned from various facilities across different industries they integrate many different points of view such as Environment, Health, and Safety (EH&S), business continuity, HR, IT, workplace violence threat assessment, investigations, and Crime Prevention Through Environmental Design (CPTED) in addition to physical security in order to develop comprehensive asset, threat, vulnerability, and mitigation profiles. The resulting TVRA not only establishes a solid foundation of data to build upon, but also documents how the mission and strategies of the physical security program align with the core business strategy.

DAVID RICKERSON PSP, CPP, PMP

Senior Project Manager, Team Leader

David Rickerson has more than 19 years of professional experience in security program planning and consulting as well as the design, engineering, specification, and project management of a diverse array of technology solutions. His project experience spans a wide variety of markets including healthcare, higher education, K-12, corporate, public sector, data centers, and museums. Technical areas of expertise include access control, alarm monitoring, video surveillance, intrusion detection, Crime Prevention Through Environmental Design (CPTED), Security Operations Centers (SOC), emergency communications, telecommunications, and various other low-voltage systems.