SECURED ASSETS, PEACE OF MIND

Get the most out of a capital budget by understanding critical assets and their vulnerabilities.

In 2013, an attack on a large urban substation on the West Coast resulted in more than $15 million in equipment damage, changing the utility industry's understanding of physical security and emphasizing its importance. The ripple effect brought changes to regulations, requiring that organizations have a detailed grasp on their facilities and assets, as well as what physical threats are possible in relation to those assets.

This paradigm in thinking has caused organizations across multiple industries to consider making large expenditures on physical security projects. Unfortunately, unless an extreme event takes place, security budgets are normally among the first things to be cut, primarily because the return on investment cannot be measured in dollars and cents. Rather, success in security is measured in the absence of an event occurring. In the reactive world of physical security planning, establishing a proactive approach on security-related spending is the key to creating effective plans that meet industry core requirements and are cost-effective.

UNDERSTANDING ASSETS AND VULNERABILITIES

Knowing the criticality of an organization's assets to ongoing uninterrupted operations is imperative to seeing what pieces of a business need the most attention. Because every industry benefits from physical security measures, the process of identifying those assets and understanding how to appropriately protect them is paramount.

"What is the critical asset that can cause a catastrophic failure if taken out by a threat?" asks Andrei Ivan, a security consulting manager at Burns & McDonnell. "When clients understand the assets on this level, they can then begin to understand the physical security measures on a tiered basis, from most critical to least critical."

When determining which assets are critical to a business, it is important to include the correct stakeholders in the evaluation process. In a workshop-type environment, critical assets and their vulnerabilities can be accurately identified before the evaluation process commences. Without these stakeholders, assets can be missed or misidentified.

IDENTIFYING THREATS

Identifying threats is difficult. Doing so is dependent on asset type, as threats are tied to a variety of factors, including industry, location of facility or assets, and overall criticality. Once the criticality of assets is understood, it is easier to identify the threats that are present or potentially could be directed against those assets.

“Analyzing past events in the specific industry is useful in understanding existing threats,” Ivan says. “Referencing open-source information, which might include FBI Uniform Crime Reports and crime statistics evaluations, helps in understanding how a vulnerability was exploited in the past and how to develop hardening measures.”

These hardening measures can then be strategically developed and implemented to detect, deter, delay, deny, assess and respond to specific threats to a facility or asset.

> *Analyzing past events in the specific industry is useful in understanding existing threats.*
>
> ANDREI IVAN

CLARIFYING THE ASSESSMENT PROCESS

Armed with a better understanding of assets and vulnerabilities, an organization’s key stakeholders or decision-makers can more readily engage with an experienced assessment team. This team will have the knowledge necessary to provide a comprehensive overview of the physical security needs of that organization.

From there, the organization can play a crucial role in the planning process by providing root-cause analysis rather than educated guesses.

GAINING INSIGHT

After assessments are completed, a Minimum Security Design Standard (MSDS) document often is developed. This document is a form of benchmark or tool, based specifically on the different assets and varying levels of protection.

The MSDS provides a tiered list of assets based on criticality, showing the minimum security standards for each. These standards include all necessary pieces of technology — from fencing and lighting to physical access control systems — in order to meet minimum industry requirements.

“The MSDS can be kept by the organization as a living document, periodically updated as an asset’s criticality changes or as new assets are incorporated into the inventory,” Ivan says. “In this way, the MSDS codifies their business security standards.

“Through this document, the physical security needs for an entire facility or organization can be laid out, viewed and understood. This allows organizations — specifically corporate security leaders — to understand exactly where to apply security spending and improve the organization’s overall approach to threat and risk management.”

Curious about core physical security competencies?
Find out more at **burnsmcd.com/PhysicalSecurityPlan**.