BURNS McDONNELL

WHITE PAPER

A Risk-Based Approach to Security Can Maximize Your Security Budget and Mitigate Your True Risks

By Landon Jones and Jared Oakden

Many clients know they need security but don't know where to start. The challenge is knowing how to provide enough security without overspending. There are numerous security measures to choose from including cameras, guards, metal detectors, fences and gates. Considering all of these options raises key questions for owners, such as: What is the best return on investment? What new technology should we consider? How much security is too much?

The security team at Burns & McDonnell has conducted hundreds of assessments across the country and often sees faulty approaches to security planning. Among the most common:

1. The reactive approach chooses security based on past security incidents alone. This is an impulsive response that tries to see that a recent attack doesn't happen again. However, not considering the root cause of such incidents and other risks leaves assets vulnerable.
2. The get-what-you-pay-for approach assumes that spending a lot of money on the latest technology equals reduced risk. Sadly, hundreds of thousands of dollars of security resources have been wasted this way.
3. The piecemeal approach tries to address security without an overall strategy or plan. We often see this at older facilities that have been pieced together over the years.

The better solution is a risk-based approach. This may take more work upfront but yields improved security for less money. The risk-based approach is a systematic analysis of the underlying risk factors to determine where security is needed most. This approach evaluates frequency and impact of adverse threat events on identified company assets.

The result of this analysis shows what assets are vulnerable and what security countermeasures are cost-effective. Identifying key assets is a commonly overlooked first step but it is foundational for security planning. One of the key benefits of a risk-based approach is that the true cost of an attack is quantified in terms of dollars. Costs can include lost production, lost reputation and lost business. Once the cost of an attack is quantified, it can easily be compared to the cost of security countermeasures to reveal which countermeasures are cost-effective. In this way, owners can be confident that

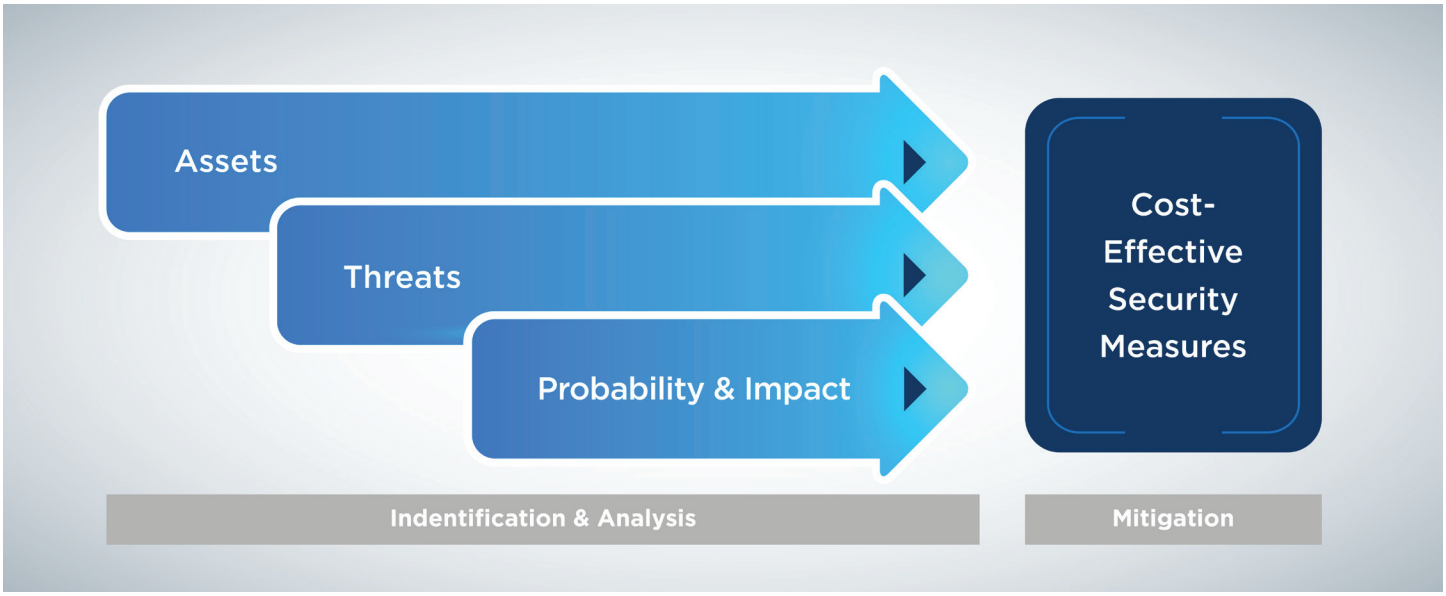

***Figure 1:** A risk-based approach to security involves identifying key assets, assessing intent and capability of potential threats, and the probability that a security-related event will occur.*

they are not overspending on security and that they have reasonable security in place. Applying a risk-based approach and industry-recognized security principles can help clients identify security-related threats, mitigate vulnerabilities and manage risk.

Risk Assessment Process

Current and emerging threat tactics can include sabotage, theft or violence, using items such as firearms, drones or explosives. The motivation for threats has also evolved over the years to include ideologic, economic and disruptive intentions. Whether you are seeking to protect a utility substation, a wastewater treatment facility or a gas pipeline, understanding and identifying risk and selecting appropriate security countermeasures is a multistep process that requires many considerations.

Identify Assets

Facility Characterization

- What are the physical conditions of the facility and how does it operate?
- What is the square footage or acreage of the facility?
- What are the facility's current policies and procedures?
- Are there any regulatory requirements or safety considerations?
- What are the company's goals and objectives?
- How many employees work at the location and what are the hours of business operation?

Target Identification

- What business operations are conducted at the facility that are vital to the organization?
- What assets are considered critical and would cause the greatest disruption if they were damaged or destroyed?
- What intangible value would be lost?
- What assets are the most valuable for resale?

Identify Threats, Frequency and Impact

Define Adversaries

- What is the likelihood that a facility could be a target?
- What is a potential adversary's motivation, goal, tactic and capabilities?
- After a threat is identified, what is the probability of an attack and expected frequency for attacks?
- What would the consequence be if assets were adversely impacted?

Select Countermeasures

Detection

- What security countermeasures, such as surveillance cameras or motion sensors, should be considered?
- Who will evaluate the effectiveness of each countermeasure?

Delay

- How long would delay elements such as fences, locks or vehicle barriers protect the asset?

Response

- If an attack happens, how long would it take for the appropriate response to be successfully executed?

Cost-Benefit Analysis

Feasibility

- How much risk will be accepted versus the cost of implementing countermeasures to reduce the risk?

Not all sites are created equal and not all sites are critical to warrant advance security protection. The physical security team can implement the steps, above, in the following three phases

Phase 1: The physical security team collects information and documentation from a client such as a facility's floor plans, a list of prior security incidents, any previous vulnerability assessments, and existing security policies and procedures. The information gathered is then coupled with crime data for that area and any other location-specific security concerns.

Phase 2: Physical security team members meet with a client on-site to assess the current physical, technical and operational security controls in place and identify any vulnerabilities. The on-site assessment also helps clarify which assets require protection and which ones do not. Not all assets are critical and need protection, especially if any loss would have a minimal impact on operations and if the cost to protect the asset outweighs the cost to replace it.

Phase 3: Team members analyze information gathered from the site visit to determine security needs and risk. The team then provides a report that outlines key observations, potential impacts from identified vulnerabilities and specific recommendations on how to reduce risk to organizational assets.

After recommended security controls are identified and installed, it is important to develop a plan to reevaluate the measures to see that they are doing what they are designed to do and, if not, what adjustments are necessary. The frequency of reviews can be based on state or federal guidelines and industry best practices, but can also be influenced by other factors, such as:

- The purchase of a new facility or site.
- A change in a facility's purpose or operations.
- Any internal or external structural changes at a facility.
- The timing of such a review, for instance it being prior to or after a merger or acquisition, or after a security event has occurred.

Conclusion

Owners and security managers often make important decisions about how to invest their security budget for maximum impact. Hundreds of critical infrastructure owners have trusted Burns & McDonnell to create strategic plans for their security program. Using a risk-based approach can help owners understand their true risks and spend their security dollars where they are needed most. This approach helps clients achieve a strong return on investment, reduce risk and ultimately keep people safe for years to come.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

79497-0123