BALANCING A PLANT SECURITY PROFILE

Even in a cyber-focused world, it is still important for thermal processing plant operators and owners to focus on physical security.

By NELSON DURAN

In today's technology-driven world, where cyber threats dominate headlines and organizations invest significant resources in safeguarding their OT and IT infrastructure from digital threat vectors, the importance of physical security of a process facility can sometimes be overlooked. However, it remains an essential component of enterprise risk mitigation.

Process industries are no place for uncertainty and risk. With the increasing concerns related to energy shortage and carbon emission issues worldwide, sustainable and safe operations of thermal processes are consistently attracting extensive attention. A comprehensive security strategy should prioritize and address both cyber and physical vulnerabilities. After all, a malicious actor in either area can cause significant undesirable outcomes (e.g., compromised employee health and safety, damage to equipment, lost production, etc.). Supply chain disruptions can lead to huge complications such as shortages of key goods, significant delays, and negative economic impacts.

Over the past 50 years, U.S. infrastructure has been consistently subject to attack, though at a relatively low number of incidents per year. According to the Global Terrorism Database, between 1970 and 2020 there have been 102 attacks on U.S. infrastructure. Since 2009, there has been a period of increased attacks on all targets in the United States — infrastructure, specifically. Infrastructure attacks rose 70 percent in 2022 compared to 2021, according to Politico.

OLD THREATS, NEW TECHNOLOGY

Despite advancements in technology, some hazards will continue to exist. Insider threats, for example, always pose a significant risk to organizations. Typically, these types of attacks are orchestrated by individuals (e.g., employees, contractors, trusted partners, etc.) who have authorized access to systems, data, or facilities but misuse that access for malicious purposes. The threat they present can range from accidental breaches due to negligence or lack of awareness to deliberate acts of sabotage, espionage, or data theft.

Insider threats can be particularly challenging to detect and mitigate because the individuals often have legitimate access and can exploit their privileges without raising suspicion. Some of the best prevention methods for this type of risk are implementing robust access controls, regular monitoring, and employee awareness programs. Promoting a culture of security and vigilance can minimize the potential impact of insider threats, and valuable assets such as sensitive information can be better safeguarded.

Vandalism, theft, and release of toxic or flammable substances are also an ever-present risk to thermal-process facilities. In recent years, many organizations have upgraded their assets to include the latest digital monitoring equipment, promoting the rapid uptake of industrial cybersecurity measures. However, this doesn't eliminate the risk of physical attempts at vandalism, theft, or purposeful releases, nor does it negate the need to defend against such attempts. Organizations should remain vigilant of these threats, even in a cyber-focused world.

EVOLVING PHYSICAL THREATS

Cyberattacks are typically the first things that come to mind when discussing the impact of increased digitalization on thermal industrial plant security. However, physical attack vectors have also evolved with technology.

One prominent physical attack vector example involves the use of unmanned aerial vehicles (UAVs) or drones. Several high-profile drone attacks on critical infrastructure outside the U.S. have raised questions about how process facilities can protect against aerial attacks. While most of these incidents originate from nation-states or designated terrorist groups with military-grade UAVs, access to recreational drones is now ubiquitous.

Whether operating within the bounds of the process plant incidentally or with malicious intent, even the most unsophisticated of UAVs can easily penetrate traditional physical security measures (e.g., fences, gates, perimeter cameras, etc.). Most enterprises did not have to consider this when their plant was originally built, thus potentially leaving them exposed to such modern-day threats.

Even on projects today, the implications of a drone attack are not always incorporated into a facility's risk assessment. Part of this is attributable to the perception that nothing can proactively be done to prevent such an occurrence. However, this is only true in some cases, as certain critical areas of the plant and facility can be hardened.

By incorporating the threat into a facility risk assessment, personnel will be forced to think about reactive measures if an event does occur, which is important to help minimize its impact and better preserve safety after the fact.

Embracing the concept of "Security-By-Design," which prioritizes integrating security features into the plant during its development, is also important. By addressing physical threats as early as possible with the same rigor and focus as those in the digital space, organizations can enhance their overall security posture, mitigate threats, and help ensure business continuity.

Countries such as Singapore are leading physical security regulations in up-front building design through their Infrastructure Protection Act (IPA). In the future, as threats to mission-critical facilities continue to evolve, it is expected that other countries will implement similar regulations.

THREAT, VULNERABILITY, AND RISK ASSESSMENTS

To help better ensure all physical security risks are addressed, it is beneficial for enterprises to perform either Security Vulnerability Assessments (SVAs), Threat and Vulnerability Risk Assessments (TVRAs), or both. Each constitutes a comprehensive approach to risk mitigation and can help facilities develop an effective physical security strategy by:

» **Better understanding the unique threats they face:** When conducting a threat assessment, process facilities can start by identifying potential adversaries, their intent and capability, then review tactics from past attacks at similar locations to estimate the threat to the organization.

With the increasing concerns related to energy shortage and carbon emission issues worldwide, sustainable and safe operations of thermal processes are consistently attracting extensive attention. (Courtesy: Shutterstock)

» **Assessing vulnerability:** Understanding the threat is essential, but the ability to deter attack is amplified by understanding vulnerability. Vulnerability can be considered as the psychological, sociological, or physical characteristics that leave an asset unprotected or exploitable for attack. Typically, the emphasis is on physical security vulnerabilities, but the human factor can make or break security efforts. Thinking, "It will never happen here," or "It will never happen to me," can add to vulnerability.

» **Quantifying risk:** Risk is defined in the basic form as "R = L x C," where R is risk, L is the likelihood of the event occurring, and C is its consequence. When it comes to performing risk calculations, most organizations focus heavily on the consequence term of the equation without measuring it against its associated likelihood. This makes it difficult to accurately prioritize risks and efficiently allocate resources toward mitigation measures. It also shifts the focus away from identifying critical vulnerabilities in infrastructure and can leave plant operations unprotected from "low probability" events. To develop a complete risk profile, both the consequence and likelihood terms of the risk equation should be thoroughly evaluated.

After quantifying the risk, organizations can begin to take preventative action by physically hardening infrastructure, such as using perimeter protection, blast analysis and design, facade strengthening, disproportionate collapse mitigation, local hardening of security command centers, and more. Another important step is security systems evaluation and design (i.e., intrusion detection, monitoring and surveillance, access control systems, security policies and procedures, redundancy evaluations, etc.), along with the implementation of dependency mitigation measures related to emergency backup power, spare parts, supply chains, emergency response, and so on.

CONCLUSION: AN INVESTMENT, NOT A COST

Adversaries will continually seek the weakest link in their target's security. Therefore, a balanced and well-thought-out security profile that includes both cybersecurity and physical security can be vital for effective facility protection and safety.

In the ever-evolving landscape of cybersecurity threats, physical security continues to play an indispensable role in protecting organizations. While cybersecurity measures are vital and growing in importance, they should be accompanied by robust physical security measures to provide comprehensive protection. In the process and manufacturing sectors, organizations of all types and sizes should be able to adapt themselves to the latest technologies and international best practices.

In both the physical and cyber worlds, security should never be viewed as a cost but as an investment to improve the overall safety of a facility. Organizations should remember that one of the primary goals of any security measure is to preserve the safe, reliable operation of physical infrastructure.

ABOUT THE AUTHOR

As the Director of Operations for the Protected Design Group within ABS Group, Nelson Duran heads up a highly talented team that spans the world, helping customers mitigate the threat potential of both man made and natural disasters.