Cybersecurity for Operational Technology in the Iron and Steel Industry

This article is part of the Digitalization Applications 101 Technology Training Course, which provides a comprehensive understanding on the basic concepts of digitalization terminologies, technologies and its applications in the steel industry. The course was developed by the Digitalization Applications Technology Committee as an introductory course to educate industry personnel in digitalization.

Authors

Scott Christensen
Cybersecurity Practice Lead,
GrayMatter, Warrendale, Pa., USA

Jeremy Boren
GrayMatter, Warrendale, Pa., USA

Nathan Smith
Director of Strategic Innovation,
GrayMatter, Warrendale, Pa., USA
nsmith@graymattersystems.com

A Brief History of Industrial Cyber Attacks

Cybersecurity attacks on production systems date to at least 1982, when a Trojan virus triggered the Trans-Siberian pipeline explosion. In *At the Abyss: An Insider's History of the Cold War,* author Thomas C. Reed writes that the compromised control software made “pumps, turbines and valves” go haywire, resulting in “the most monumental non-nuclear explosion and fire ever seen from space.”[*]

Fast-forward to 2010, when cybersecurity for operational technology drew public attention with the STUXNET malware attack, which targeted Iranian centrifuges. While the application was much more sophisticated compared to the Trans-Siberian pipeline incident, the result was similar. While updating the control system code, malware manipulated the rotation speed of centrifuges during the refinement of uranium. No one has publicly acknowledged carrying out the attack, but in the 2016 documentary *Zero Days,* writer/director Alex Gibney[†] contends it was a joint operation between two nation-states to circumvent the “air gapped” or siloed Iranian ICS network.

Today, ransomware is among the most common types of malware attacks that affect operational technology environments. Ransomware is a cyber attack in which a cybercriminal gains access to an organization's sensitive files, such as customer data, financial records or intellectual property, and encrypts them so the owner can no longer access them without a decryption key. The cybercriminal offers to provide the key in exchange for a ransom of up to six or seven figures. Paying the ransom is no guarantee that the data will be returned, which has led many professionals to advise against paying. In some cases, not only does the cybercriminal refuse to return the data, they instead release it publicly, damaging an organization's reputation and pocketing the money.

In May 2020, Australian steel producer BlueScope reported that it was the victim of a cybersecurity attack, possibly ransomware. The company said it had to shift some steel production to “manual operations” as it sought to recover from the disruption to manufacturing and sales operations in Australia.

[*] *At the Abyss:* “The Cold War . . . was a fight to the death,” notes Thomas C. Reed, “fought with bayonets, napalm, and high-tech weaponry of every sort — save one. It was not fought with nuclear weapons.” With global powers now engaged in cataclysmic encounters, there is no more important time for this essential, epic account of the past half-century, the tense years when the world trembled at the abyss. Written by an author who rose from military officer to administration insider, this is a vivid, unvarnished view of America's fight against Communism, from the end of WWII to the closing of the Strategic Air Command, a work as full of human interest as history, rich characters as bloody conflict.

[†] ZERO DAYS: A documentary focused on Stuxnet, a piece of self-replicating computer malware that the U.S. and Israel unleashed to destroy a key part of an Iranian nuclear facility, and which ultimately spread beyond its intended target. https://www.imdb.com/title/tt5446858.

Cyber Risk and Resiliency Defined

To think about how companies in the steel and iron industry should approach cybersecurity risk and build resiliency to protect physical plant systems, it's helpful to follow a five-point framework developed by the National Institute of Standards & Technology (NIST), which is part of the U.S. Department of Commerce and strives "to promote innovation and industrial competitiveness."[2]

Cyber Risk — Cybersecurity risk is any risk of financial loss, disruption or damage to the reputation of an organization from a failure in critical operational systems.

Cyber Resiliency — Resiliency is an organization's ability to identify, protect, detect, respond and recover (each detailed in the next section) from process or technology failures and to achieve the goals of minimizing harm, damage to reputation and financial loss.

National Institute of Standards & Technology Framework

NIST defines five functions as the focus of cybersecurity. As maturity develops within an organization, these functions become less reactive and more proactive.

Identify — Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities. The focus here is to understand your environment at all levels. The tendency is to focus on assets or vulnerabilities, but a more complete picture focuses on both, in addition to communication behaviors. Once you identify assets and version levels, you can measure risk and potential impact on your network. Solutions such as vulnerability assessments, networks mapping and asset discovery are often the focus in this stage.

Protect — Develop and implement appropriate safeguards to ensure delivery of critical services. One of the key components to minimizing risk is hardening and protecting critical assets. Often this can involve network segmentation, antivirus or encryption, but it can also include reviewing firewall policy/rules, patch management and microsegmentation.

Detect — Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. Actively hunting for potential threats and new risks is critical. One advantage operational networks have over their information technology (IT) counterparts is that they are static in nature. This allows us to identify a baseline of good behavior and focus on anomalous or negative behaviors. This often means deploying tools such as network intrusion detection systems (NIDS) and security incident and event management (SIEMS). Correlating events across multiple tool sets is key to success.

Respond — Develop and implement an appropriate plan when a cybersecurity incident is detected. The most overlooked factor in cybersecurity is often the response plan. How quickly an organization can respond to an incident is a measure of the organization's maturity. The key to successful response is training, awareness and a culture developed around cybersecurity readiness.

Recover — Develop and implement appropriate activities to maintain plans for resilience and restore capabilities impacted by a cybersecurity incident. Even the most secure organizations can be affected by a cyber incident. Having a detailed recovery plan is critical. Critical infrastructure should have a manual operation plan in place.

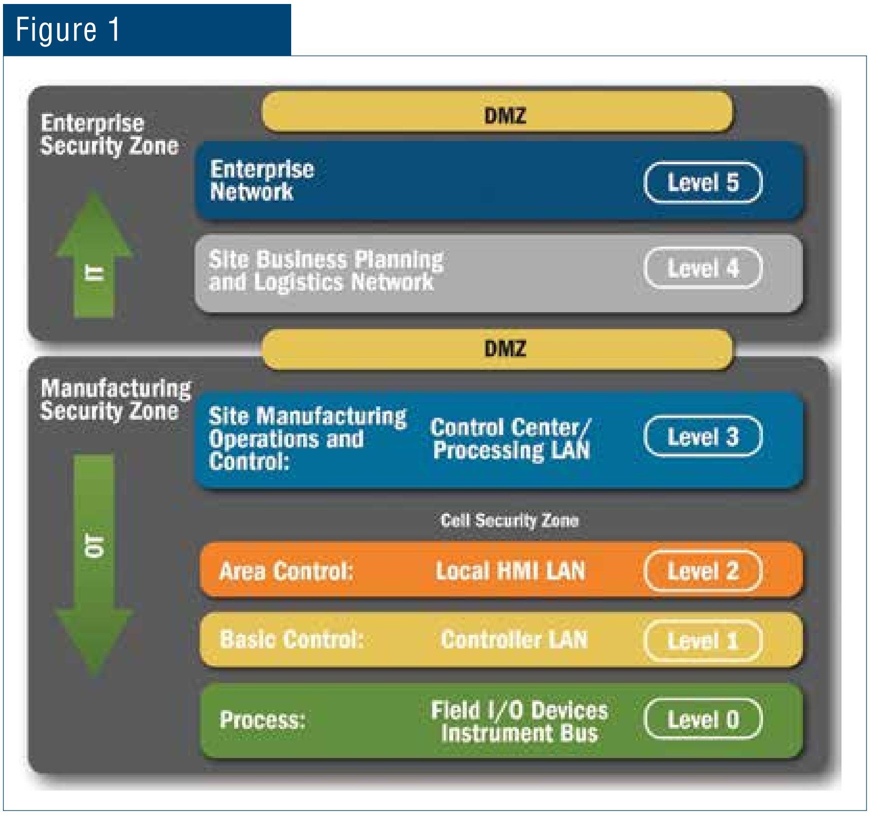
Defense in Depth

To minimize risk and add resiliency to an operational environment, companies in the iron and steel industry must adopt a defense-in-depth strategy. That means taking NIST guidelines into account and protecting critical assets and systems with multiple layers of security and risk mitigation, and not allowing a single failure to expose critical assets to risk. It also means partnering with experts in operational technology environments, instead of relying solely on in-house IT expertise.

The concept of defense in depth isn't new. What's new is its application to industrial control systems (ICS). In the past, companies have not prioritized ICS cybersecurity because the need wasn't as apparent as it is for the IT-related systems (desktops, laptops, printers, etc.) that most employees interact with directly every day.

"Defense in depth is not one thing, but a combination of people, technology, operations and adversarial awareness," according to the U.S. Department of Homeland Security.[3] "Thinking and doing solves problems, and technology enables problem-solving by providing a set of tools that can reduce risk. The best technology in the world will not prevent humans from making mistakes — whether intentional or unintentional. Organizations must constantly adjust and refine security countermeasures to protect against known and emerging threats."

Figure 1


Enterprise Security Zone
DMZ
Enterprise Network
Level 5
IT
Site Business Planning and Logistics Network
Level 4
DMZ
Manufacturing Security Zone
Site Manufacturing Operations and Control:
Control Center/ Processing LAN
Level 3
OT
Cell Security Zone
Area Control:
Local HMI LAN
Level 2
Basic Control:
Controller LAN
Level 1
Process:
Field I/O Devices Instrument Bus
Level 0

Example of how an industrial organization can segment their business to improve cybersecurity.

IBM and the Ponemon Institute in 2020 released an annual report that estimates the average cost of a cybersecurity breach is US$3.86 million and rising, but the cost can vary widely. For example, Norwegian aluminum producer Norsk Hydro estimates a 2019 ransomware attack cost it US$71 million to US$75 million as production lines slowed or stopped at 170 plants worldwide and workers were forced for a time to use pen and paper to keep records.

Companies must prioritize building a cybersecurity strategy to protect their operational technology assets. Permitting the IT department to protect everything — from the so-called "front door" systems like websites, e-commerce platforms and company-issued laptops — underestimates the value of the organization's industrial assets, which cyber attacks can exploit as a back door. Instead, companies should dedicate resources and planning to protect physical, plant floor assets from attacks to ensure they're not simply bolting the front door but leaving the back door unlocked.

Conclusion

Cybersecurity for operational technology is not only intended to reduce exposure to risk but to have a robust strategy in the event of a cybersecurity attack that results in a sensitive data leak, loss of data or temporary interruption in operations. It's simply too big to ignore. As a result, many corporations now provide regular cybersecurity preparedness briefings to their boards of directors — the same level of attention given to strategic workforce and investment decisions, which can shape a company's future.

References

1. https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS- CERT_Defense_in_Depth_2016_S508C.
2. NIST Cybersecurity, U.S. Department of Commerce, https://www.nist.gov/topics/cybersecurity.
3. U.S. Department of Homeland Security, "Recommended Practice: Improving Industrial Control System Cybersecurity With Defense-in-Depth Strategies," September 2016. ✦