Driving Cultural Change in Manufacturing Cybersecurity

As hackers become more sophisticated and dangerous, manufacturers need to step up their cybersecurity efforts

RAY CHALMERS
Contributing Editor

Reported in 2014, hackers infiltrated the IT network of a German steel plant with a successful email "spear-phishing" attempt. Once they were into the system, the hackers subsequently were able to access the operational technology (OT) of the plant's operating system. That's when the crime turned deadly. The attackers compromised settings on the temperature controls of a major blast furnace, causing it to overheat out of control and explode, resulting in massive damage and the death of two workers. To date, no identification or arrests have been made.

The tragic event is part of a growing wave of cyber attacks around the world, and underscores the potential severity of their consequences.

Fast-forward to 2022. On April 13, several U.S. government agencies—the Department of Energy (DoE), Cybersecurity and Infrastructure Security Agency, National Security Agency, and Federal Bureau of Investigation—issued a joint Cybersecurity Advisory warning that some advanced persistent threat (APT) actors are showing the capability of gaining full system access to multiple industrial control system (ICS)/supervisory control and data acquisition

By infiltrating a steel plant's IT system with email spear phishing, hackers migrated to the plant OT system and overrode a blast furnace's temperature controls, causing it to explode and kill two workers.

(SCADA) devices, including Open Platform Communications Unified Architecture servers and the programmable logic controllers of a number of suppliers.

According to the alert, APT actors have developed custom-made tools to scan, compromise, and control targeted ICS/SCADA devices once they have established initial access to a company network. By compromising and maintaining full system access to such systems, hackers could elevate privileges, move laterally within an OT environment, and disrupt critical devices or functions.

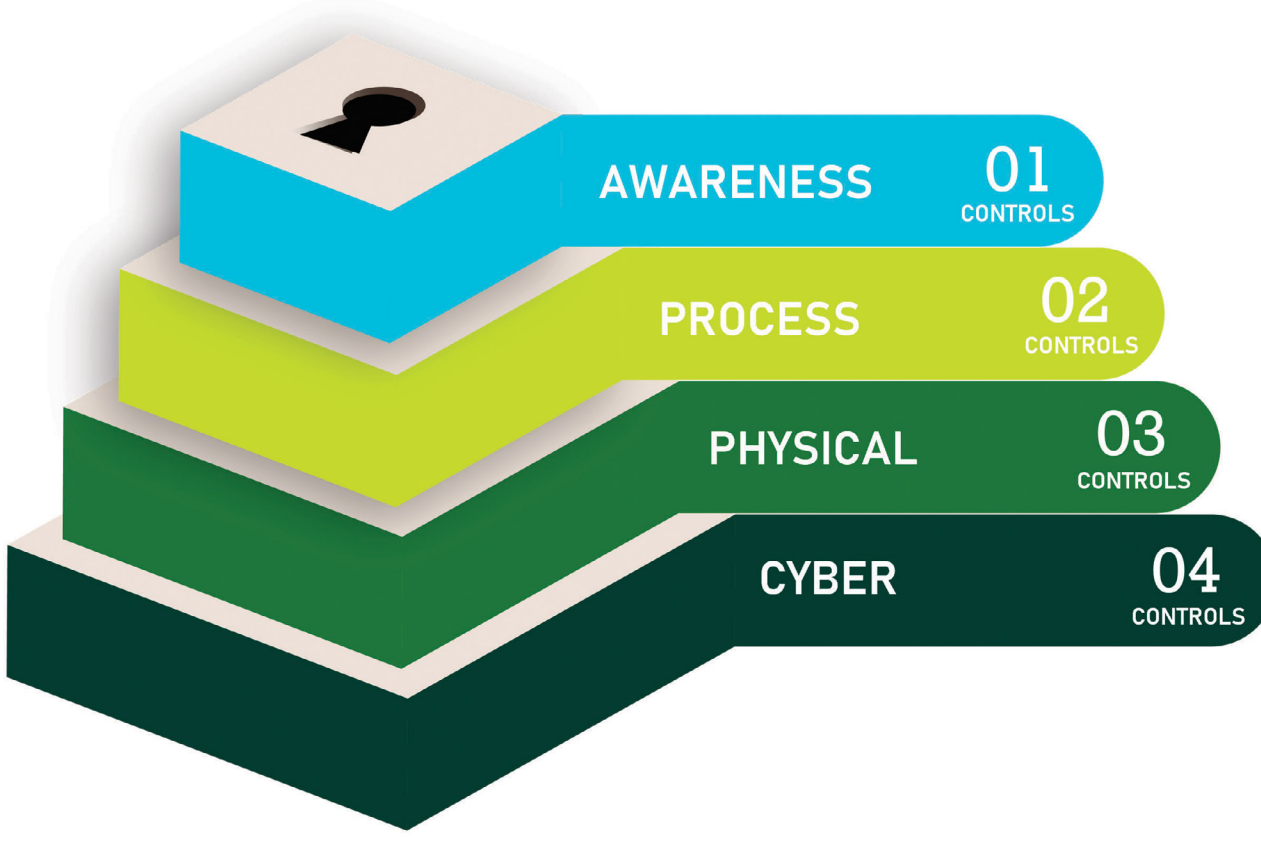
Sound familiar?

"Whether we like it or not, major cybersecurity threats are real, they're here, and manufacturing is the No. 1 target," said Paris Stringfellow, vice president of TrustWorks as-a-Service (TrustWorks-aaS), which is part of the Cybersecurity Manufacturing Innovation Institute (CyManII).

Launched in 2020 by the DoE at the University of Texas at San Antonio, CyManII, along with 15 other manufacturing innovation institutes (sponsored by either the DoE or one of two other U.S. agencies—Commerce and Defense—bring together manufacturers, academia, national research labs, and other government agencies. The focus is on major, industry-critical research and development projects, as well as training people on advanced manufacturing skills.

"The Department of Energy fully understands the volume and veracity of the cyberattack vectors aimed at U.S. manufacturers, and this is why they support a Manufacturing Innovation Institute focused squarely on these threats," said CyManII CEO Howard Grimes. "CyManII has already developed cyber innovations that offer significant security gains and will continue to develop and deploy these with industry leaders like GE, Cisco, Lockheed-Martin, and many more."

One reason manufacturing is a top global concern is the increasing speed of digitization. "Manufacturers are digitizing at twice the speed of other industries. We estimate an average energy savings of 20 percent for those who digitize," Stringfellow said.



Hardening your systems against cyber threats means taking a layered approach to cybersecurity and implementing cyber-aware controls across all system tiers.

With upwards of 50 billion smart connected devices being installed, the attack surface for hackers is expanding in tandem. This is creating a lot of easy-access doorways into a company's operations.

CyManII spent most of 2021 working with manufacturers to identify the challenges of protecting their digital migration programs. Four main areas of concern emerged:

- Supply chains are unsecured and lack transparency. Risk extends beyond factory walls, up and down the entire supply chain, often beyond a single manufacturing organization's control.
- There is a growing IT and OT convergence for which the workforce is largely unprepared, with a lot of questions. Whose job is it to secure the system, identify risks, and make ongoing plans for implementation? Maintenance? IT? "Our employees lack sufficient skills to manage these growing vulnerabilities on the plant floor," Stringfellow said. "The effective cyber workforce gap is only getting bigger."
- Securing legacy systems creates production uncertainties. Newly connected networks often involve older computers with outdated operating systems. While many have worked for years without fail, adding them to new plant networks exposes vulnerabilities. "Even securing old equipment can create unknown impacts to production," Stringfellow added.
- The approach to vulnerability management in manufacturing cybersecurity is largely reactive. This means companies are patching when they should be planning, which isn't surprising considering the non-stop pace of cyberattacks with new malware, ransomware, and direct takeovers.

Secure, interconnected, and energy-efficient manufacturing is a journey. No matter where a company is along the way, from seeking assistance on risk assessments and training to hardening IT/OT networks, the goal is to have cybersecurity baked-in throughout the manufacturing process, according to Stringfellow. "This is a future where your products and operations are secure by design."

Effective Collaboration

CyManII recently launched the Manufacturing Information Sharing and Analysis Center (MFG-ISAC) and the Global Resilience Federation (GRF) to further defend U.S. manufacturers from malicious cyber activity. The nonprofit group expands companies' threat awareness and allows members to crowd-source best practices to enhance warning, mitigation, recovery, and resilience.

Through a collaboration portal for vetted security practitioners, member companies exchange threat data from phishing attacks, malware signatures, IoT vulnerabilities, risks to operational technology, and other hazards. Members can share information anonymously or with attribution, depending on sensitivity and the desired level of feedback from peers. Additionally, MFG-ISAC staff monitor and send relevant alerts from government, private security vendors, and open sources, to the community.

"MFG-ISAC provides a vital space for the industry to gain early warning of attacks, (and) the best means to recover from and prevent future attacks," Grimes said. "We're pleased to be working with GRF to launch this group, especially given the threat environment we find ourselves in today. Awareness and training for cybersecurity has never been more critical."

Harden With Defense in Depth

In addition to embedded security, CyManII promotes a "defense-in-depth" strategy to hardening industrial processes. The program takes a four-tiered approach:

1. Awareness: Building and keeping an awareness of cybersecurity status and risks throughout your organization.
2. Process: Developing, establishing, updating, and sharing organizational processes and people to mitigate security risks.
3. Physical: Assessing and implementing the right physical devices to protect your equipment and harden your defenses.
4. Cyber: Deploying cyber safeguards and tools to protect your digital infrastructure.

Although CyManII is still in the early stages of defining and establishing its programs, efforts abound at developing new tools for manufacturers to deploy to increase their cybersecurity effectiveness. One is the development of a Secure Manufacturing Architecture (SMA). Meant to embed security from the ground up, SMA uses a "digital passport" technique to log each product through its value chain, making manufacturers aware of security exposure throughout a product's lifecycle.

Integrating digital security with existing systems can be challenging—especially in a live production line. CyManII

is establishing what it calls the Secure Research and Development Infrastructure (SRDI) to give developers and companies a safe space to design and test security upgrades. This is a federated set of secure cyber/physical testbeds located throughout the U.S. “Product developers and manufacturers can assess the energy profile, cybersecurity, and production alternatives before new designs reach the factory floor,” Stringfellow said.

Accurate information-sharing on current threats is critical to keeping equipment protected, but there is limited structure for sharing ICS-related threats. CyManII is working to better define these classification schemes for the manufacturing environment. This work will not only help security teams better protect their assets, they’ll also be able to improve the efficiency of their patching and updating efforts.

Employees lack sufficient skills to manage growing cybersecurity vulnerabilities on the plant floor, according to CyManII. The effective cyber workforce gap is only getting bigger.

CyManII is building TrustWorks-aaS to help manufacturers utilize these solutions and gain competitive advantages. The organization provides education, training, and live support for individuals and companies who want to “level up” their industrial security competency, according to Stringfellow. The services focus on enhancing IT/OT cybersecurity at the design level, enhanced energy efficiency using secure practices, and on securing the supply chain.

“Manufacturers should be clear this is not an offer for generic cyber training,” Stringfellow said. “We are developing manufacturing-specific material and formalizing partnerships with training experts like Tooling U-SME and the Cisco Networking Academy. We are coming out with a ‘CyManII Seal’ showing the content is up to date and meets our standards. We intend to really move the needle in terms of upskilling the manufacturing workforce. We need to reach people at scale and meet them where they are.”

CyManII believes a large part of its mission is to continue driving a cultural shift in manufacturing cybersecurity akin to the great shifts in plant safety from the 1960s and ’70s to today. In a connected world, cyber threats are real and at our doorsteps, if not already in our organizations. The U.S. urges critical infrastructure organizations such as manufacturing to improve detection, mitigate threats, and achieve superior cybersecurity. CyManII is the manufacturing-specific response.

For more on the latest efforts and offerings and how to join CyManII, visit www.cymanii.org.

IMPROVE YOUR
CYBERSECURITY
TODAY

CONTACT US FOR MORE INFORMATION:

CYMANII Officially Endorsed Educational Content

TOOLINGU | sme

info@toolingu.com or 866.706.8665