Staying Ahead Of CMMS And EAM Cybersecurity Risks

Facility managers need to mitigate the risk of their software, IoT devices, or operational tech from being compromised.

By Paul Lachance

The Internet of Things (IoT) has changed manufacturing for the better. Industry 4.0 technology such as IoT devices, more traditional programmable logic controllers (PLC), distributed supervisory control and data acquisition (SCADA) systems, and more have all increased productivity and quality control for facility managers. But as operational tech has grown in adoption, these industrial systems—and the untold number of devices and access points they contain—have become attractive targets for hackers.

According to an NTT Global Threat Intelligence report from May 2021, the manufacturing sector experienced a 300% increase in worldwide cyber-attacks since the start of the COVID-19 pandemic. These attacks include well-publicized incidents such as that of JBS USA Holdings, Inc. in 2021, which forced one of the world's largest meat processors to shut down its North American and Australian plants and lose millions of dollars in both downtime and ransom.

These hacks cause reverberation in the industry and ultimately with consumers. Some 40 additional attacks on food producers occurred in the 12 months preceding the JBS attack, and companies around the globe continue to face attacks everyday that don't necessarily make the news. Despite this increase in cyber-attacks, manufacturing leaders often overlook the importance of cybersecurity. Whereas physical security, such as making sure the facility is properly secured and all doors and windows are locked, has been top of mind for decades, assessing cyber risk isn't quite as intuitive. The truth is that any device connected to the internet is at risk of unauthorized access, phishing, data theft, supply chain, and ransomware attacks. Any digitally-connected supplier can pose a risk as well. When malicious actors can steal credentials, expose sensitive data, and hold intellectual property ransom, among other nefarious acts, where should facility managers begin when it comes to mitigating the risk of compromising their software, IoT devices, and operational tech?

With more operational tech in use than ever before, there's a greater risk that sensitive information may be compromised.

PHOTO: ADOBE STOCK BY ANDISS

Best Practices For Mitigating Risk

Beyond understanding the threats applicable to a specific operation, the first step in mitigating potential cyber threats is to understand the different roles and responsibilities associated with information technology (IT) and operational technology (OT).

OT is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. OT systems are found across a large range of asset-intensive sectors, performing a wide variety of tasks ranging from monitoring critical infrastructure (CI) to controlling robots on a manufacturing floor. And while OT is similar to IT in that they both include networks, computers, cloud, PLCs, and more, OT can be much harder for managers to pinpoint and is often overlooked as a result. The importance of cybersecurity across IT and OT cannot be overstated—both are highly susceptible to cyber-attacks from external hackers.

Next, to begin the process of remediating these risks, it's important to adopt a formal OT cybersecurity program with a dedicated internal champion. In most organizations, OT cybersecurity will fall under the scope of IT cybersecurity. However, this synchronization can be challenging because some standard IT security practices do not translate directly within the OT world. For example, a routine IT activity such as patching vulnerable software can be problematic in OT if it results in equipment downtime. To get ahead

of this issue, it's important to create an accurate inventory of all technology assets within an OT environment and, where possible, implement a patch and vulnerability management program for these assets. In the same way computers, mobile phones, and other devices need routine security patches, so do "smart" assets, devices, sensors, and other more "behind the scenes" tech. Given the multitude of possible hackpoints, managers need a combination of high-level organization protection as well as trusted individual device suppliers.

Beyond this program creation, there are several cybersecurity considerations that are broadly applicable to a variety of manufacturing use cases—especially software and network users. These include providing employee training on how to recognize and respond to phishing attempts, developing a business continuity plan that includes off-site backups of all business-critical systems, and restricting device and system access to only authorized personnel, among other considerations. Facility managers will need to determine the best course of action for their specific team and enterprise.

Leaning Into The Shared Responsibility Model

Computerized maintenance management systems (CMMS), one of many industrial software solutions, are becoming ubiquitous in the industry. The security of a CMMS is an important consideration in a facility's overall security program, and it should be a shared responsibility between the software vendor, the CMMS administrator, and the actual end-users.

This "shared responsibility" model of cybersecurity is already widely used within IT. But before a facility can adopt this model, an important distinction must be made: Is the CMMS on premise (installed on an organization's servers) or cloud-based (Software as a Service, or SaaS)? In a SaaS implementation (by far the most common today), many of the security controls fall to the vendor, and using a SaaS vendor will provide an organization with advantages including mitigation of risk, cost savings, scalability, and resilience.

With the risk to the manufacturing sector on the rise, embracing and adhering to cybersecurity best practices now will be well worth the investment when—and not if—a cyber-attack occurs.

However, it is critically important to thoroughly vet a vendor's security program.

A good vendor will look beyond external threats to consider the many ways everyday users can inflict damage inside the software, be it by a simple mistake or an intentional, harmful act. With CMMS, managers can prevent these threats by limiting what users can and can't do within the platform, for example. These checks should go beyond strong passwords, which is why it's critical for managers to sit down with a SaaS partner and other stakeholders to ensure effective policies and controls are in place. A good example of effective controls could be found in work orders. Rather than allowing users to "delete" work order history, an alternative work order status, such as "archived," could be implemented. There are many stories about unhappy users deleting this history to hide work not performed or even to be malicious.

Facility managers should also insist their SaaS vendors provide transparency about their security program, practices, and policies. A few focus areas for a SaaS vendor evaluation include the SaaS vendor's patching policies, Single Sign-On (SSO) options, Role-based Access Controls (RBAC) which allow the software to control what a user can edit and delete, and the storage of backup data. In addition to these considerations, facility managers should:

- Ensure the SaaS terms of service restrict data sharing by the vendor.
- Ensure the SaaS vendor complies with relevant regulations. In the U.S. this includes the California Consumer Privacy Act. At the global level, organizations must comply with General Data Protection Regulation.
- Identify sub-services used by the SaaS vendor. Most SaaS vendors work with a variety of sub-service providers such as Amazon AWS or Microsoft Azure for data center hosting. Ensure these sub-service providers are reputable and do not introduce the potential for unexpected data storage locations.
- Review SaaS vendor third-party audits. Third-party audit reports such as penetration testing and risk assessments will help confirm the effectiveness of the vendor's security controls.

While implementing additional precautions isn't always convenient, the consequences of weathering a cyber-attack with little or no planning can be incredibly damaging to a business of any size. Sharing the responsibility of cybersecurity and having a trusted SaaS vendor will pay dividends in the long run.

With the risk to the manufacturing sector on the rise, embracing and adhering to cybersecurity best practices now will be well worth the investment when—and not if—a cyber-attack occurs. Cybersecurity for IT and OT devices is just as important as physical security in this increasingly digital and connected world, and it's time for facility managers, vendors, and stakeholders to prioritize a safe and secure network together.

Lachance is a senior manufacturing advisor for Brightly (brightlysoftware.com). As a life-long entrepreneur and company-builder with a focus on industrial software, Lachance has organically grown and successfully sold two software companies. His journey has taken him from micro-startup into the growth years, all the way to integrating and thriving within a large organization.

Do you have a comment? Share your thoughts in the Comments section of the online version of this article at FacilityExecutive.com. Or send an e-mail to the Editor at jen@groupc.com.