Safeguarding data in the digital factory

How to protect a connected factory from cyberthreats

verizon

From SmartBrief

Security threats facing manufacturing

The manufacturing industry is grappling with cybersecurity threats that are growing in frequency and sophistication, putting sensitive data at risk. These threats include:

Ransomware attacks, where data or even factory operations are held hostage until a ransom is paid.

Phishing, where a fraudulent email or web page is used to trick someone into revealing sensitive data or downloading malware.

Man-in-the-middle attacks, where hackers intercept conversations and communicate with each party so they think they are sharing information with each other but are inadvertently sending it to the hacker.

Breaches like these can compromise many types of data, such as confidential R&D material, intellectual property, market research, sensitive customer information and financial records.

Manufacturing is now the most targeted sector for cyberattacks, surpassing financial services and insurance.1 For example, a suspected cyberattack on a supplier caused a Japanese care manufacturer to close all of its plants in Japan earlier this year. The one-day shutdown affected 14 factories and the manufacturing of 13,000 cars.[2] An attack involving a provider of cloud-based security cameras, allowed hackers to access cameras in the factories and warehouses of a prominent U.S. car manufacturer.[3]

The COVID-19 pandemic, which caused supply chain shortages, brought attention to the unique cybersecurity risks of having long, complex supply chains and time-sensitive processes. It also brought about an increase in the number of employees working remotely and using personal devices to access company networks and information. Employees may be using inadequately protected devices and might connect to unsecured Wi-Fi networks in public places. This creates new challenges for managing and controlling the devices that have access to an organization's data and networks.

Cybersecurity and Industry 4.0

New challenges are also emerging inside the factory, as manufacturers shift to Industry 4.0, connecting machines, products, people and a variety of partner companies.

As part of this shift, operational technology (OT) like equipment sensors and HVAC systems – traditionally separate from IT – is now becoming integrated with both corporate IT infrastructure and supply chain partners because of advanced manufacturing technologies.[1]

OT is typically not secured as well as laptops, phones and tablets, and many companies aren't adequately monitoring this technology, which may include older systems without modern threat detection and response capabilities.[4] This can limit manufacturers' ability to assess their full technology ecosystem and potential threats.

Further, OT may not be subject to the same data governance requirements as IT.[5] Decisions on operational technology are typically made in the manufacturing environment, without the involvement of corporate IT and security staff.[4]

These challenges and limitations, along with the fact that OT supports tasks that are essential for manufacturers, can make it a tempting target for hackers. In fact, there was a 50% increase in operational technology breaches last year.

The integration of OT and IT, increased connectivity with partners and the variety of connected devices and factory equipment used by an organization and its employees create new opportunities for cyberattacks. This means manufacturers with advanced technology infrastructure need even more advanced cybersecurity standards and protections.[4]

However, a 2019 survey found that less than half of manufacturers had conducted a cybersecurity assessment in the previous six months.[4] Many companies are failing to protect their data due to a lack of understanding the risks associated with their systems, as well as a lack of investment in IT/OT cybersecurity.

Companies that aren't adequately protected face:

- Financial consequences
- Loss of intellectual property or sensitive information
- Decreased productivity
- Supply chain problems
- Loss of trust from customers and partners.

Building essential protections

There are a variety of actions that organizations can take to protect themselves, and most already have cybersecurity budgets and provide employee training to protect against threats.

The first is to make sure employees are familiar with the use of security software, and that it is regularly updated and includes all available patches. Outdated internet of things (IoT) devices are an attractive target, but manufacturers making firmware updates must keep in mind that IoT devices run on low bandwidth and connectivity, so it is important to ensure that updates don't overload the system and affect critical functions.

Manufacturers should also make use of IoT credentialing, allowing only "credentialed" devices into the network. Eighty percent of data breaches are associated with stolen credentials, making it more important than ever to secure all devices that can access the organization's information, network and systems.

Manufacturers need proper configuration of data stores in the cloud and on premises. Important data should not all be stored in the same place. Use of cloud services, managed security and other resources can help manufacturers keep abreast of and stay vigilant against emerging cyberthreats.

Before implementing any new technologies, companies must assess their cybersecurity maturity, risk profile and readiness for a cyberattack.[4,6] Vulnerability testing that mimics a cyberattack can help find flaws in an organization's IoT network.

Finally, it is crucial to have a strong cybersecurity governance program to guide the organization.

A recent survey from the Manufacturing Leadership Council found that 83% of manufacturers rank cybersecurity as a highly important business issue and 79% expect an increase in attacks in the next year.[8] However, just 40% have a high level of confidence about their internal expertise about cybersecurity.

Cybersecurity governance program

A good cybersecurity governance program should include:

- Risk maps that show the company's risk profile.[6]
- A risk escalation framework with reporting thresholds.
- A rapid response and containment plan that prioritizes actions based on risk profiles.[4]
- An up-to-date inventory of all OT and IT assets, the data they collect and any interconnectivity between the two.[5]
- Staff training with special considerations for remote workers and for high-risk employee groups that handle sensitive data, industrial control systems or connected products.[6]
- Encryption of data with securely stored and backed-up encryption keys.[7]
- Backup of mission-critical systems so data can easily be restored.
- Security patches and updates for industrial control systems and security features.

sponsored by

verizon✓

Manufacturers must ensure they have the right leadership assigned to address risks and make decisions on investments and new technologies, particularly for industrial control systems and connected products.[6] Chief information security officers should make sure their organizations take these essential steps, and should identify partners that can bring additional expertise, guide manufacturers through these changes and help them secure their data and processes. Manufacturers, in turn, should be prepared to invest in strong protections and evaluate the results of these solutions.

As OT and IT continue to become more integrated in the factory environment, manufacturers need full visibility into threats across their organization. They need a strong strategy for prevention, detection and response, as well as edge computing and 5G for low-latency, high-bandwidth connectivity. With the right action plan, solutions and partners, today's manufacturers can protect their most valuable resource – their data.

References

1. Pfeifer, S. Smart factories need smarter cyber defense. Financial Times. May 31, 2022. https://www.ft.com/content/b95be8d7-e6f7-4227-a42b-1a582e9226a4

2. Sugiyama, S.; Kelly, T.; Shiraki, M. Toyota suspends domestic factory operations after suspected cyber attack. Reuters. Feb. 28, 2022. https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/

3. Gartenberg, C. Security startup Verkada hack exposes 150,000 security cameras in Tesla factories, jails, and more. The Verge. March 9, 2021. https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals

4. Hajj, R. et al. Cybersecurity for smart factories. Deloitte. 2020. https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/smart-factory-cybersecurity-manufacturing-industry.html

5. Hightower, S. Manufacturing cyber security: How to enhance threat visibility across IT and OT environments. Verizon. https://www.verizon.com/business/resources/articles/s/how-to-enhance-threat-visibility-across-it-and-ot-environments/

6. Cyber risk in advanced manufacturing. Deloitte. https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html

7. Sultan, O. What are common cyber threats to manufacturers and how can they secure themselves. Hackread. July 3, 2022. https://www.hackread.com/what-common-cyber-threats-manufacturers-security/

8. Brousell, D. Survey: Manufacturers get tough on cybersecurity. ML Journal. August 2022. https://www.manufacturingleadershipcouncil.com/survey-manufacturers-get-tough-on-cyber-security-28556/?stream=ml-journal-august-2022