Safeguarding data in the digital factory

How to protect a connected factory from cyberthreats

verizon business

As manufacturers embrace advanced connectivity and technologies, it also opens the door to potential cyberthreats that can compromise sensitive data and disrupt operations. Protecting the connected factory from cyberattacks is crucial to ensure the integrity, confidentiality and availability of critical information.

Explore the following insights to discover strategies and best practices for safeguarding data in the digital factory.

Key threats impacting the manufacturing industry.

Cybersecurity threats are on the rise; becoming more frequent and sophisticated by the day. This unsettling trend puts sensitive data at constant risk of compromise and poses a significant challenge. These risks include:

- Ransomware attacks: Data is held hostage until a ransom is paid.
- Phishing: A fraudulent email or web page is used to trick someone into revealing sensitive data or downloading malware.
- Man-in-the-middle attacks: Hackers intercept and manipulate conversations, tricking parties into sharing information with them instead of each other.

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

Manufacturing is now the most targeted sector for cyberattacks.

It is targeted even more so than financial services and insurance.

The COVID-19 pandemic highlighted cybersecurity risks in supply chains and remote work: supply shortages, time-sensitive operations and employees using personal devices on unsecured networks. As a result, managing device access to organizational data has become a daunting task.

A suspected cyberattack on a supplier caused a Japanese car manufacturer to close all of its plants in Japan in 2022. The one-day shutdown affected 14 factories and the manufacturing of 13,000 cars.

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.

Cybersecurity and Industry 4.0: Why smart factories need more advanced protection.

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

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

OT is typically not as well secured 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. This can limit manufacturers' ability to assess their full technology ecosystem and potential threats.

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

Amidst these challenges and limitations, coupled with OT's critical role in manufacturing, it becomes an enticing target for hackers. Alarmingly, operational technology breaches surged by 50 percent last year.

But, within this advancing landscape, there are also many opportunities for cyberattacks. Subsequently, manufacturers equipped with cutting-edge technology infrastructure find themselves in need of even more advanced cybersecurity standards and robust protection measures.

Many smart factories are not adequately protected.

A 2021 McKinsey survey assessed the cybersecurity maturity level of over 100 companies and institutions across various industry sectors. The findings indicate that while there has been significant progress in the banking and healthcare sectors, the majority of organizations in all industries still have a long way to go in safeguarding their valuable information assets against evolving threats and attacks. It seems many companies are failing to protecttheir data due to a lack of understanding of 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

Constructing critical cybersecurity defenses.

The first step companies can take to protect themselves 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 can be quite tempting for attackers. However, manufacturers who are proactive in making firmware updates should consider the limitations of these devices. IoT devices often operate on low bandwidth and connectivity, so it's crucial to strike a balance during updates to avoid overloading the system and potentially disrupting critical functions. Finding the sweet spot between keeping the devices secure and maintaining optimal performance is key.

80 percent of data breaches are associated with stolen credentials. Manufacturers should make use of IoT credentialing, allowing only "credentialed" devices into the network.

Proper configuration of data stores both in the cloud and on the premises is needed – important data should not all be stored in one place. Leveraging cloud services, managed security and other resources can aid manufacturers in staying proactive and vigilant against emerging cyberthreats.

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

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

Building a robust cybersecurity framework for enhanced protection.

A critical step in cybersecurity defenses that can often be overlooked is a good cybersecurity governance program. This should include:

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

Manufacturers need to appoint capable leaders who can effectively manage risks, make informed investment decisions and navigate the complexities of industrial control systems and connected products. Chief Information Security Officers (CISOs) play a crucial role in ensuring these steps are taken, including seeking external partners with expertise to guide them through necessary changes and secure data and processes. Manufacturers, in turn, must be willing to invest in robust security measures and diligently evaluate the outcomes achieved by these solutions.

As OT and IT systems continue to become more integrated in the factory environment, manufacturers need full visibility into threats across their organization.

Verizon offers a strong strategy for prevention, detection and response. Additionally, advanced technologies including edge computing and private 5G enable low-latency, high-bandwidth connectivity through solutions like Verizon's Private 5G, mobile edge computing, and cloud-based services.

With the right action plan, solutions and Verizon as your partner, today's manufacturers can better navigate their journey to Enterprise Intelligence while protecting their most valuable resource – their data.

Discover how Verizon can transform your cybersecurity operations, allowing your team to focus on what really matters: driving your business forward.

verizon✓
business