# FAQ

## How to Prepare for the

# Cybersecurity Battle Amid Industry 4.0

*Many manufacturing enterprises are adopting smart technologies such as Industrial Internet of Things (IIoT) and artificial intelligence (AI) capabilities to achieve efficiencies and competitive advantage. However, this shift to Industry 4.0 is leaving organizations vulnerable to a wide range of threats including malware, distributed denial of service (DDoS) attacks, and device hacking.*

*Only 16% of manufacturers are prepared to address these cybersecurity threats, as reported by the Institute of Electrical and Electronics Engineers (IEEE). This FAQ addresses the factors manufacturers should consider as they push forward with smart technology objectives. It also offers guidance toward overcoming cybersecurity challenges associated with Industry 4.0 initiatives.*

### Why must manufacturers rethink their cybersecurity strategies?

Smart manufacturers and engineering firms are increasingly vulnerable to malware, DDoS attacks, device hacking and exploitation. The rapid adoption of Industry 4.0 technologies—such as IIoT, AI, blockchain and digital twins—is causing major disruption for manufacturers. These implementations are causing IT complexities, as well as data and device security vulnerabilities.

In addition, many manufacturers are bringing together industrial control systems with IT and OT processes to gain data insights. However, this convergence creates new cyber risks resulting from unauthorized changes, misconfigurations, legacy devices not structured for today's sophisticated cyberattacks, and more.

Another challenge stems from digital transformation projects. As part of their Industry 4.0 efforts, manufacturers are ramping up the digitization of processes and workflows. COVID-19 has added to this: 67% of manufacturing organizations have accelerated digital transformation efforts due to the pandemic. These initiatives increase the risks of security vulnerabilities and misconfigurations.

Overarching these challenges is the rapidly evolving cyberattack landscape. There has been an increase in remote work and remote access to machines due to COVID-19, creating new cybersecurity concerns. Threats have become more sophisticated, including the rise of ransomware-as-a-service and automated cyberattacks.

All of these trends have made it urgent for manufacturers to address cybersecurity as a means to futureproof for business resiliency and agility.

Sponsored by

REDSEAL

IndustryWeek

## What are the risks of not adequately addressing cybersecurity?

Several factors make it untenable for manufacturers to ignore the need for a modern cybersecurity strategy. A significant challenge is sheer growth in devices; IoT connected devices are expected to triple in volume by 2030. Every sensor and device is a potential risk, especially if it is connected to the network. The more people and machines that access the network, the more gateways that cybercriminals can exploit. For example, individuals remotely accessing network printers via unsecured Wi-Fi connections can inadvertently create security risks.

In addition, although digital transformation efforts are accelerating, they are being carried out in piecemeal fashion. Legacy systems are difficult and time-consuming to modernize; as they co-exist and connect with modern apps and systems, the risk of misconfigurations and vulnerabilities rises.

At the same time, many manufacturers are moving data to the cloud and edge. In these cases, risks include the potential exposure of sensitive or mission-critical stored data, especially when there is a lack of visibility across disparate or hybrid IT environments. Also, if patches or upgrades aren't rapidly and consistently installed, gaps and vulnerabilities can be exploited by cybercriminals.

Amid these challenges is one more: Cyberattacks continue to evolve. However, many manufacturing organizations lack cybersecurity expertise to keep up with existing security threats, let alone new ones.

## These challenges sound overwhelming. Where should we start?

Start with a war-like mentality. Consider this analogy: Before troops go into battle, they first gain an understanding of the parameters such as terrain, their existing arsenal and allies, and battle locations.

Similarly, manufacturers need reliable information to make educated decisions for both Industry 4.0 initiatives and cybersecurity. They require visibility into the potential cyberattack landscape, the assets they have—personnel, systems, solutions and partners—and the IT environment, such as the use of on-premises data centers, private and public cloud, and edge computing.

Next, dig deep and conduct a comprehensive risk assessment. Ask questions such as:

- Where is sensitive data stored?
- Who has access to data?
- Is there an inventory of all devices that connect to the network?
- Are data, IoT devices, and systems segregated on the network according to business- and mission-critical importance?
- How secure are the connected ICS systems?
- What are the potential vulnerabilities in the remote workforce and supply chain?
- If your organization is undertaking a merger or acquisition, can you identify all the critical assets that must be protected in merging or acquired business?

Use this risk assessment, which is akin to a risk inventory, to lay the groundwork for two important best practices: developing an incident response plan and a cybersecurity plan. After all, you must first know what to protect in order to determine how to protect it.

## What if our organization has gaps, such as a lack of cybersecurity or risk management skills?

There are solutions that help overcome gaps and ensure manufacturers can mitigate cyber risks. For example, the right security and analysis solution can run on your network and find any potential risks or vulnerabilities. It will identify all assets and resources, determining whether any of them have been unintentionally exposed to the internet and who has access to them. It can also validate your segmentation policies to ensure that mission-critical or sensitive data is safe.

The right risk solution offers multiple benefits including the ability to develop incident response and cybersecurity plans; enhance existing security and network investments; improve compliance efforts; and achieve greater visibility across IT environments. Also, those organizations with lean IT teams can quickly prioritize vulnerabilities to reduce the burden on staff.

Finally, and critically, a security risk and analysis solution helps manufacturers future-proof their Industry 4.0 and digital transformation initiatives while providing robust cybersecurity throughout the organization. ●

**Ready to get started?**

**Find more information here or sign up for a live demo of RedSeal for manufacturers.**