Manufacturing: CYBERSECURITY RISKS *(And How To Be Prepared)*

The manufacturing industry is going through some challenging times. As it continues to expand digitally, innovate, and incorporate new technologies to improve productivity and efficiency, it's also facing numerous attacks.

We've put together this guide on what risks the manufacturing industry faces and how it can best protect itself.

WHY THE HIGH RISK?

Updated digital infrastructure = increased attack surface
An increase in IoT devices, warehouse management systems, and cloud-based monitoring and maintenance solutions, the manufacturing industry has a much wider digital footprint that's potentially at risk.

Increased targeting as part of supply chain ecosystem
Threat actors know the value of attacking a supply chain and have been dramatically ramping up their attacks over the last few years.

Government incentives creating new regulatory requirements
The U.S. government is making a concerted effort to grow the manufacturing industry and with that, comes new regulatory requirements and scrutiny, making cybersecurity a priority for this industry.

WHAT THE MANUFACTURING INDUSTRY SHOULD LOOK OUT FOR

Device compromise attacks
Now that devices are digitally connected and accessible via the internet, attackers can leverage vulnerabilities, exploits, compromised credentials and specifically target IoT devices, maintenance equipment, and even entire warehouse systems.

Disconnect between IT/OT
Operational Technology (OT) and Information Technology (IT) often work in silos, making it harder to address cybersecurity issues and create a comprehensive strategy for proactive protection.

Devices aren't built with security
This disconnect increases the risk that's often built-in with these devices. Assets and devices remain easily discoverable, hardcoded or default passwords are often unchanged, and known vulnerabilities may stay unpatched.

Disrupted business operations
These compromises can be heavily disruptive, pausing business operations, delaying product delivery or, as can often be the case with ransomware attacks, stopping manufacturing altogether.

IN THE NEWS

Manufacturing was the MOST ATTACKED industry in 2022

2,204%

The increase in reconnaissance in OT by attackers

92%

the increase in ransomware attacks against manufacturing industries from 2021 to 2022

TOYOTA

Toyota's 2022 Supply Chain Attack Halts A Third of Production
Toyota's plastic parts and electronic component supplier was hit with a ransomware attack, causing Toyota to suspend operations in 14 plants across 28 production lines.

NVIDIA

Attackers Steal NVIDIA's employee credentials and proprietary information
The notorious hacking group LAPSU$ claimed responsibility for numerous attacks against NVIDIA. An employee device was compromised via a virtual machine which led to a data breach of over 1TB of proprietary data.

HOW THE MANUFACTURING INDUSTRY CAN BE PREPARED FOR CYBER RISKS

Invest in cyber security!
Cybersecurity needs to be a top priority and manufacturing companies need to build a comprehensive strategy that includes risk and vulnerability assessments, patch management, device, and account security, and implementing tools and processes to operationalize security.

Secure both OT and IT
The silos of IT and OT need to be eliminated and OT should be rolled up as part of IT's overview, allowing them to properly develop strategies and solutions to secure these devices.

Secure your network against attacks
Securing devices starts at the network and access level. Organizations should invest in a zero-trust approach to minimize overall access to sensitive data and assets and implement network segmentation, and identity access management to minimize lateral movement and widespread attacks.

Stay proactive with recovery and response partners
Few companies can have comprehensive cybersecurity in-house. To best protect themselves from the inevitable ransomware attack or data breach, an organization should consider having cyber insurance, an incident response retainer, and a managed security program provider that offers 24/7 security and response.

When attacks are so common, organizations need to prioritize swift response and recovery to minimize impact.

To learn more about how we can help your organization,

Check out SolCyber

SolCyber

solcyber.com