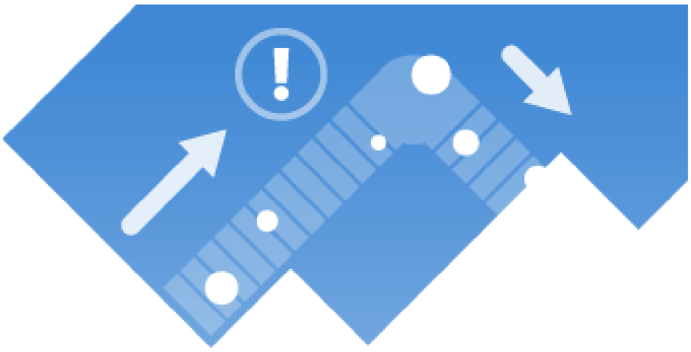
Manufacturing Risk Advisor



Q2 2025

Mitigating Cybersecurity Risks in Manufacturing

Although technological advancements in the manufacturing industry provide several benefits, they also present cybersecurity exposures. The expanded use of digital tools such as artificial intelligence (AI), digital sales platforms and smart machinery expand the attack surface for cybercriminals, and resulting cyberattacks can cause significant business disruptions, reputational damage and financial losses. Robust cybersecurity measures are vital to protect sensitive data and ensure business continuity. Manufacturing business leaders should take proactive steps to safeguard against these cyber risks.

Why Do Cybercriminals Target Manufacturing?

There are several reasons cybercriminals target manufacturers. The industry often possesses valuable intellectual property (e.g., proprietary designs), and malicious actors may perceive it to have weaker cybersecurity compared to other sectors. Additionally, due to manufacturing's role in the global supply chain, cybercriminals know that cyberattacks can lead to major final losses and may believe that manufacturing organizations are more likely to give in to their demands against recommendations in doing so. The interconnected supply chain also could provide entry into numerous entities through one weak link, making it an appealing target.

Common Types of Cyber Risks

While cybercriminals have many methods of infiltration, certain types of cyberattacks are common in manufacturing. These include ransomware attacks, industrial espionage and supply chain attacks. Insider threats present additional risks. These threats occur when individuals with authorization to enter an organization's network or data—including current or former employees, contractors and business partners—intentionally or accidentally steal sensitive information, sabotage systems or facilitate internal attacks.

Cybersecurity Best Practices

To help combat cybersecurity risks, manufacturing business leaders should take proactive steps and bolster their digital defenses. In particular, these companies should consider the following best practices:

- Adopt zero-trust architecture and assume that any user or device could be an entry point for a breach.
- Implement strict role-based access controls.
- Utilize multifactor authentication (MFA) and encryption.
- Bolster supply chain cybersecurity and only partner with third-party vendors and suppliers with strict cybersecurity protocols.
- Include cybersecurity requirement clauses in vendor contracts.
- Conduct regular security audits and vulnerability assessments with penetration testing.
- Establish a cybersecurity incident response plan.
- Vet employees and provide regular and robust cybersecurity training.
- Foster a culture of cybersecurity, encouraging employees to report suspicious activity.
- Backup data and safely store it.
- Install advanced antivirus and malware protection software and use patch management systems.
- Leverage technologies such as AI and machine learning to detect unusual activity within a system.

- Segment networks to limit malicious actors’ access to sensitive information by restricting their lateral movement within the network if they gain entry.
- Secure cyber insurance to help mitigate a business’s exposure to cyber-related damages.

Conclusion

Implementing strong cybersecurity protocols and obtaining a cyber insurance policy can help address cyber risks and safeguard businesses’ data, finances and reputations. Contact us today for more information.

This document is not intended to be an exhaustive source of information nor should any discussion or opinions be construed as legal advice. Readers should consult legal counsel or a licensed insurance professional for appropriate advice.