Manufacturing and Distribution Cyber Challenges

Manufacturing and distribution facilities stand as the backbone of global supply chains, yet this critical sector is increasingly targeted by sophisticated cyberattacks. The cost of a successful cyberattack on a manufacturer can be crippling, with the average incident costing $2.8 million in 2023. Further, ransomware attacks continue to plague the industry, with reports indicating that over 30% of manufacturers have fallen victim to such attacks. Disruptions in manufacturing and distribution have far-reaching consequences, impacting everything from the availability of consumer goods to critical infrastructure.

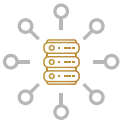
12 cybersecurity risks that threaten the manufacturing and distribution industry and strategies to combat them:

1. Cybersecurity Collaboration Across Departments

THE CHALLENGE: Manufacturing companies often struggle when it comes to defining clear cybersecurity roles, consolidating budgets, and synchronizing priorities across IT and OT (Operational Technology) departments. These silos can lead to vulnerabilities in cyber defense mechanisms and inefficiencies in resource allocation.

THE SOLUTION: Establish a unified cybersecurity framework that outlines the cybersecurity services the company employs, assigns clear roles across IT and OT, and ensures alignment with overall business objectives. Offer training programs tailored to OT cybersecurity, assess ongoing effectiveness through established metrics, and form a cross-functional cybersecurity governance committee to harmonize goals and strategies across departments. Regularly review these strategies to maintain alignment with broader business objectives, and actively foster leadership buy-in to promote a culture shift towards heightened security awareness.

2. Visibility of OT Assets



THE CHALLENGE: In many manufacturing environments, OT asset details are collected manually, which creates inconsistent inventories and outdated OT assets that may lack necessary security patches and proper configuration. This creates significant security gaps and exposes the infrastructure to potential cyber threats.

THE SOLUTION: Shift to a proactive, technology-driven approach using automated tools that monitor assets continuously, IoT (Internet of Things) security platforms for visibility and control of your OT assets, and machine learning for advanced threat detection and anomaly identification. Additionally, ensure you understand how your technology systems communicate with each other to identify and evaluate potential security risks.

Understand how your technology systems communicate with each other to identify and evaluate potential security risks.

dla@dlallc.com | 973-575-1565 | www.dlallc.com

Fairfield, NJ | New York, NY | Shrewsbury, NJ | Boston, MA | Chicago, IL

3. Network Segmentation

THE CHALLENGE: Manufacturing networks often lack sufficient segmentation across IT and OT systems, leading to intertwined assets that blur the lines between informational and operational domains. This increases the risk of cyberattacks spreading from one domain to the other, potentially causing widespread operational disruption.

THE SOLUTION: Start by establishing a secure separation between IT and OT networks through physical firewalls and reduce the OT network's direct connection to the internet. Perform routine testing and validation of network segmentation rules and implement Windows Active Directory structures for OT to allow more detailed access control. Consider using adaptive segmentation techniques that adjust to changes in network traffic and threat landscapes.

4. Access Management

THE CHALLENGE: Manufacturing operations tend to struggle with inconsistent access management across different locations, extensive third-party access, inadequate password hygiene, and privileged account abuse.

THE SOLUTION: Restrict and refine administrator permissions and establish a secure remote access protocol. Conduct periodic reviews of granted access, audit access rights, and implement stringent controls over removable media and roaming engineering laptops. Strengthen password security with comprehensive policies and multi-factor authentication (MFA) and consider Privileged Access Management (PAM) solutions for just-in-time access and enhanced privileged accounts monitoring.

5. Cybersecurity Monitoring

THE CHALLENGE: Many manufacturers lack the skilled cybersecurity personnel who can fully utilize advanced monitoring tools, making it harder to detect cybersecurity incidents.

THE SOLUTION: Establish a Security Operations Center (SOC) for centralized monitoring, specifically focusing on OT processes for quick identification and response to cybersecurity events. Using cloud-based SIEM platforms, you can centralize monitoring of both IT and OT environments. Explore managed security services (MSS) providers for continuous monitoring.

6. Ransomware Threats

THE CHALLENGE: Ransomware groups like LockBit and ALPHV are employing more sophisticated social engineering and zero-day exploits against the manufacturing sector.

THE SOLUTION: Patch your systems regularly, implement secure data backups, and conduct threat hunts to spot potential early indicators of compromise. Conduct incident response planning and drills for effective security breach handling. Apply proactive strategies such as network segmentation to curb lateral movement and reduce internet exposure and employ Managed Detection and Response (MDR) services for advanced detection capabilities that will reduce the likelihood and impact of a successful ransomware attack. Also, consider investing in cyber insurance as a financial safety net.

7. Nation-State-Aligned Threats

THE CHALLENGE: The manufacturing sector is a prime target for nation-state actors who aim to steal intellectual property and exploit critical infrastructure and supply chains as gateways into broader networks.

THE SOLUTION: Maintain robust defenses against sophisticated attacks on intellectual property theft and network infiltration and collaborate with industry peers and government agencies to share threat intelligence and stay ahead of advanced tactics.

8. Compliance with Cybersecurity Maturity Model Certification (CMMC)

THE CHALLENGE: Compliance with CMMC is mandatory for DoD contractors. Even for those not working with the DoD, achieving CMMC compliance demonstrates a strong commitment to cybersecurity and safeguarding sensitive data and trade secrets.

THE SOLUTION: Adhere to the CMMC standards to protect sensitive data and demonstrate a commitment to cybersecurity. To navigate the complexities of CMMC compliance, conduct a maturity assessment to gauge your current cybersecurity measures against CMMC standards, then collaborate with cybersecurity experts to create a detailed compliance roadmap. Proactively arrange for CMMC audits and conduct regular reviews to ensure ongoing adherence to these critical standards.

9. Third-Party Risk

THE CHALLENGE: Manufacturing environments prioritize productivity and efficiency. Cybersecurity measures can sometimes be perceived as causing friction or slowing production processes. The need to prioritize operational efficiency in manufacturing and distribution environments can sometimes lead to compromises in cybersecurity measures, increasing vulnerability to cyberattacks.

THE SOLUTION: Develop a risk-based cybersecurity strategy that aligns with operational goals. Conduct thorough risk assessments to prioritize the most critical assets and implement proportionate security controls. Focus on technologies like behavior analytics, network segmentation, or zero-trust architectures that offer robust protection without hindering production processes. Train employees to understand how security measures support operational efficiency and the consequences of non-compliance. Regularly review and adapt the strategy to address evolving threats and maintain a balance between security and efficiency.

10. Establish an Industrial Demilitarized Zone (IDMZ)

THE CHALLENGE: The convergence of IT and OT networks in manufacturing environments increases vulnerability. A cyberattack on the IT network could easily spread to critical OT systems, potentially disrupting production and causing significant damage.

THE SOLUTION: Establish an Industrial Demilitarized Zone (IDMZ) to create a secure buffer between IT and OT networks. This specialized zone facilitates controlled data exchange, allowing essential information to flow while shielding sensitive OT assets from broader network threats.

11. Supply Chain Vulnerabilities

THE CHALLENGE: The extensive network of suppliers and vendors in the manufacturing and distribution industry introduces numerous potential entry points for cyber-attacks. A breach in one part of the supply chain can have cascading effects that impact multiple organizations.

THE SOLUTION: Strengthen your supply chain security by implementing stringent vendor risk management practices that include routine security assessments and establishing secure communication protocols to ensure all suppliers meet your cybersecurity standards.

12. Legacy Systems and Infrastructure

THE CHALLENGE: Many manufacturing facilities rely on outdated systems and equipment that lack essential security features or no longer receive adequate support from vendors, creating vulnerabilities that make them susceptible to cyber-attacks.

THE SOLUTION: Modernize your vulnerable legacy systems with security features that include encryption, multi-factor authentication, and regular patching. When full system upgrades aren't possible, consider employing alternative protective measures such as rigorous network isolation, implementing Privileged Access Management (PAM) to secure critical access points, and intensifying surveillance for unusual activities.

As the risk landscape continues to evolve and grow more complex in the manufacturing and distribution industry, staying ahead of security threats is more critical than ever. At DLA, our team of seasoned cybersecurity experts can help you protect your manufacturing company from emerging threats. Contact us to learn more.