REPORT

# Manufacturing security trends and the impact of artificial intelligence

April 2025

LUMEN®

# Table of contents



LUMEN®

# Introduction

The manufacturing industry has long depended on technology to boost productivity, maintain quality, and stay ahead of the competition. Today's factory floors are more connected than ever, powered by a web of integrated digital systems—from computer-aided design (CAD) and manufacturing (CAM) tools, to robotics, connected supply chains and Enterprise Resource Planning (ERP) platforms.

The adoption of Industry 4.0 technologies, including the Industrial Internet of Things (IIoT) and cloud-based platforms, has accelerated the digital transformation of manufacturing, bringing advanced connectivity, automation, and real-time data-driven decision-making to the forefront.

**Industry 4.0** encompasses the use of the Industrial Internet of Things (IIoT), Artificial Intelligence (AI), and cyber-physical systems to create smart factories. These technologies enable real-time data collection, analysis, and decision-making, leading to enhanced efficiency, productivity, and flexibility in manufacturing operations. The adoption of Industry 4.0 technologies has expanded the attack surface and introduced new vulnerabilities.

Artificial Intelligence (AI) is playing a pivotal role in this transformation. In addition to optimizing production and quality control, AI is being leveraged to improve predictive maintenance, streamline logistics, and, increasingly, strengthen cybersecurity defenses.

However, AI is increasingly becoming a double-edged sword in the manufacturing sector's cybersecurity landscape. While manufacturers are leveraging AI to enhance their defense mechanisms, cyber adversaries are simultaneously exploiting AI to orchestrate more sophisticated attacks.

## Purpose of the report

This report explores current cybersecurity trends within the manufacturing sector and analyzes how AI is influencing these trends. As digital maturity increases across factories, so do the attack surfaces and the sophistication of threats targeting these environments. We will examine how AI helps mitigate risks, the challenges it introduces, and what manufacturers can do to build secure and resilient operations.

# Security trends in manufacturing

## Vulnerabilities in manufacturing

The manufacturing industry is a top target for cybercriminals worldwide. This is due to several vulnerabilities which threat actors attempt to exploit.

- **Automation and Industrial Internet of Things (IIoT) expansion**: In North America, manufacturers are under immense pressure to boost efficiency, leading to widespread adoption of automation and IIoT technologies. According to a Manufacturing x Digital report, the number of connected devices worldwide is expected to double from 2023-2029. This expansion significantly increases the attack surface, making it easier for cybercriminals to find entry points.
- **Operational Technology (OT) Integration**: Manufacturing environments often integrate IT and OT systems, making them attractive targets for cybercriminals. Phishing attacks can compromise OT systems, leading to disruptions in production processes.
- **Supply Chain Vulnerabilities**: Manufacturers rely heavily on complex supply chains. Phishing attacks targeting suppliers or partners can lead to credential theft and subsequent breaches in the supply chain.
- **Legacy systems and infrastructure:** Many manufacturing environments still rely on outdated operational technology (OT) and industrial control systems (ICS) that were not designed with cybersecurity in mind. As these systems become integrated with modern IIOT devices, they become more vulnerable to advanced threats.
- **Employee Awareness**: Manufacturing employees, especially those on the production floor, may not be as aware of phishing threats as office staff. This makes them more susceptible to social engineering attacks.
- **Cloud security issues**: As manufacturers adopt cloud-based solutions, vulnerabilities in cloud security become a major concern. Misconfigurations, inadequate access controls, and insecure APIs are common issues that attackers exploit.[2]

## Increasing cyber threats

In today's digital landscape, cybersecurity threats are evolving at an alarming rate, posing significant risks to various industries, particularly manufacturing. As cybercriminals become more sophisticated, they employ a range of tactics to exploit vulnerabilities and disrupt operations. This section delves into the most pressing cybersecurity threats facing manufacturers, highlighting the need for robust security measures to safeguard against these dangers.

## Ransomware attacks

Ransomware continues to be a major threat, with attackers increasingly targeting manufacturing operations to disrupt production and demand ransoms. The trend is toward more sophisticated and aggressive ransomware tactics, including double extortion, where data is both encrypted and stolen.[2] Ransomware attacks on manufacturers commonly begin with data theft and exfiltration, with attackers stealing sensitive information and threatening to release it unless a ransom is paid. This trend is driven by improved backup and restoration capabilities, forcing attackers to find new ways to extort victims.[2] JBS Foods, a global meat producer, faced a debilitating ransomware attack that forced them to temporarily shut down operations for over five days, disrupting the global food supply chain.[3]

According to a recent Trustwave report, ransomware and phishing are the primary attack vectors used by attackers against manufacturing targets.[2]

- **87%** of attacks originated from phishing
- **54%** of ransomware attacks were in the US
- **14%** of ransomware attacks targeted machinery manufacturers.

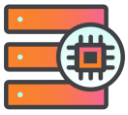
## Phishing and social engineering leading to credential theft

Phishing remains a prevalent attack vector in the manufacturing industry, with cybercriminals using increasingly sophisticated techniques to deceive employees and gain access to sensitive information. Social engineering tactics are evolving to be more convincing and harder to detect, often leading to credential theft where attackers use stolen credentials to gain unauthorized access to IT systems and intellectual property. Manufacturing environments face unique challenges such as the integration of IT and OT systems, which can be compromised by phishing attacks, causing production disruptions, costly downtime, and operator safety incidents.[2]

## Supply chain attacks

Manufacturers are increasingly targeted through their supply chains. Cybercriminals exploit vulnerabilities in third-party vendors to infiltrate larger networks. This trend is expected to grow as supply chains become more interconnected.[2]
According to a report from Iron Edge, "In 2023, Applied Materials (a multi-billion dollar business) experienced a supply chain attack that resulted in significant production delays, affecting their ability to deliver critical components to tech companies worldwide. This led to a $250 million loss.[3]

## AI-driven attacks



Artificial Intelligence (AI) is being leveraged by attackers to automate and enhance their tactics. AI-driven attacks can adapt and evolve, making them harder to defend against. This trend is expected to continue growing.[4]

Moreover, AI can magnify the impact of other cyberattack types mentioned above. For instance, AI can be used to create more sophisticated ransomware, conduct highly convincing phishing and social engineering campaigns, and identify vulnerabilities in supply chains more efficiently. As AI technology advances, the potential for these attacks to become more frequent and severe only increases.

## Cost of being breached

Cyberattacks on manufacturers can be devastating, leading to costly downtime, and the loss of intellectual property and confidential customer data. In fact, NFP reports that, despite security and government experts recommending companies not pay ransoms, manufacturers pay ransoms more than any other industry in order to avoid data loss and potential downtime. The consequences of the attack are simply not worth it, leaving them shelling out an average of $550,000 demanded by cybercriminals.[6] As AI continues to expand within the criminal world, manufacturers may experience even more cyberattacks.

## Artificial intelligence

Artificial intelligence and machine learning (ML) are making major impacts within the manufacturing sector. Manufacturers are turning to AI and ML to improve their operations in many ways, including:

**Robotics and automation**
AI-powered robots perform complex tasks with precision, helping to increase productivity and reduce human error.

**Production planning and scheduling**
AI enhances production efficiency by optimizing resource allocation and streamlining workflows.

**Predictive maintenance**
AI predicts equipment failures and schedules maintenance to help reduce downtime and extend machinery lifespan.

**Quality control**
AI enables real-time quality inspection and defect detection, helping to ensure high product standards and reduce waste.

**Supply chain optimization**
AI optimizes supply chain management by forecasting demand, managing inventory, and improving logistics efficiency.

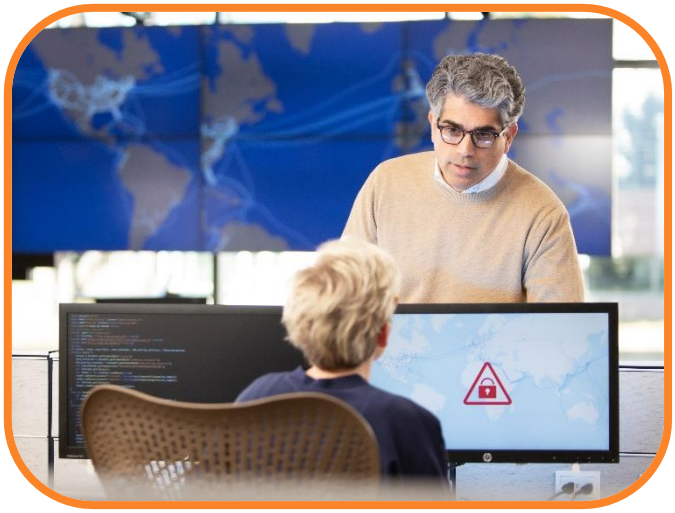
**Enhanced safety**
AI-powered sensors help robots and machines understand and navigate their surroundings, reducing the risk of collisions and ensuring safe interactions with human workers.

While AI and ML are being integrated in many ways to propel manufacturing operations forward, there are also many risks associated with AI.

# AI exploitation in manufacturing: A growing threat

The manufacturing industry is facing an unprecedented wave of cyber threats, driven by the rapid adoption of advanced technologies and the increasing sophistication of cybercriminals utilizing AI. As manufacturers strive to boost efficiency through automation and IIOT expansion, they inadvertently expand their attack surface, making it easier for AI-driven cyber adversaries to find entry points.

## AI-enhanced attack techniques



Cybercriminals are leveraging AI to sharpen their attack methods, including:

- **AI-driven industrial espionage:** Cybercriminals are increasingly using AI to conduct industrial espionage. This technique leverages AI to analyze vast amounts of data to identify valuable intellectual property and trade secrets, making it easier for attackers to target and steal sensitive information. As a result, manufacturers may face significant financial and competitive damage.
- **Deepfakes**: Hackers can utilize AI to create highly convincing audio and video impersonations, making their attacks appear legitimate and increasing their chances of success. According to Gartner, by 2026, nearly a third of enterprises may no longer trust standalone identity verification tools, as deepfakes increasingly undermine biometric and authentication systems.[7]
- **Spear-phishing**: By analyzing personal data and social media profiles, attackers can craft highly targeted phishing campaigns, significantly improving the likelihood of successful breaches. By leveraging AI, attackers can churn out hyper-convincing phishing campaigns tailored to each targeted individual at an astounding rate.[8]
- **Evasive malware**: AI and cloud-enabled malware can infiltrate existing security systems, learn from them, and adapt to avoid detection in future attacks.[9]
- **Automated targeting**: Cybercriminals can use AI to automate the distribution of targeted messages, dramatically increasing the scale and speed of their attacks.[10]

## Impact on manufacturing operations

The rising frequency of cyberattacks is pushing manufacturers to enforce stringent cybersecurity measures across their supply chains. This trend is particularly evident in the automotive industry, where cybersecurity mandates are becoming increasingly common. So the question is: how are manufacturers using AI to protect themselves against this onslaught of cyberattacks coming their way?

Manufacturing was in the top 3 most-targeted industries by every one of the five major ransomware groups Arctic Wolf investigated in the last 12 months.

# AI as a defense tool in manufacturing cybersecurity

In response to the escalating complexity and frequency of cyberattacks, manufacturers are increasingly turning to AI technologies to bolster their cybersecurity defenses. These technologies help automate threat detection and response strategies, enabling manufacturers to protect critical infrastructure.

Here are some of the key strategies manufacturers are actively employing to safeguard against ongoing cyberthreats:

- **Continuous authentication and encryption:** Manufacturers are implementing robust cybersecurity measures that involve continuous authentication and encryption. Continuous authentication ensures that users are verified at regular intervals, rather than just at the initial login, reducing the risk of unauthorized access. Encryption protects data by converting it into a code that can only be deciphered with the correct key, ensuring that sensitive information remains secure even if intercepted.
- **Data de-identification services:** AI is being utilized to deploy data de-identification services, which help protect sensitive information while still enabling data analysis. Data de-identification involves removing or obscuring personal identifiers from datasets, allowing manufacturers to analyze data without compromising privacy. This is particularly important for compliance with data protection regulations and for safeguarding customer information.
- **Integration of AI and machine learning (ML):** By integrating AI and ML into their cybersecurity solutions, manufacturers can enhance threat detection capabilities. These technologies analyze vast amounts of data to identify patterns and anomalies that may indicate potential threats. AI and ML can learn from previous incidents to predict and prevent future attacks, making cybersecurity systems more adaptive and resilient.
- **Unified cyber defense:** Manufacturers are developing a cohesive and integrated cyber defense strategy that secures all relevant infrastructure. This approach ensures that all systems, from production

lines to administrative networks, are continuously monitored and protected against potential threats. Unified cyber defense involves coordinating various security measures and technologies to create a comprehensive defense mechanism.

- **Adoption of zero-trust security models:** Companies are embracing zero-trust security models, which require stringent verification for every individual and device attempting to access network resources. The zero-trust approach operates on the principle that no entity, whether inside or outside the network, should be trusted by default. This model mandates continuous verification of user identities and device integrity, significantly reducing the risk of unauthorized access and breaches.[11]

These strategies highlight a proactive approach to cybersecurity, acknowledging that as digital technologies and interconnectivity expand, so do the associated vulnerabilities and risks of cyberattacks.

## Challenges and risks

Despite the benefits, manufacturers face several challenges and risks associated with the implementation of AI in their security frameworks:

- **Lack of skilled workforce:** There is a shortage of skilled personnel capable of maintaining and running AI applications, which can hinder effective security management. According to the 2024 ISC2 Cybersecurity Workforce Study, the global cybersecurity workforce gap is estimated to be over 3.4 million professionals. This shortage is particularly pronounced in AI and security disciplines.
- **Data silos:** Manufacturers often deal with segmented IT infrastructures, where data resides in silos (e.g., warehouse data, sales data, R&D data). This fragmentation complicates the integration of AI solutions and can lead to security gaps.
- **High operational costs:** Implementing AI in manufacturing can be a costly endeavor. Expenses arise from various areas such as data acquisition, infrastructure, talent, model development, integration, compliance, and ongoing maintenance. These costs are further amplified by issues like data silos and inadequate network capacity, which contribute to inefficiencies and increased overall expenses.[13]
- **Data privacy concerns:** The use of AI in manufacturing raises significant data privacy issues, particularly regarding the handling of personal identifiable information (PII). Manufacturers must ensure compliance with applicable laws and regulations while leveraging AI technologies.
- **Ethical concerns:** The potential for AI to be misused or to inadvertently lead to biased decision-making processes poses ethical challenges that manufacturers must navigate carefully.[14]

# Cybersecurity regulations for AI in the manufacturing industry

In the manufacturing sector, adhering to cybersecurity regulations is crucial, especially when incorporating AI technologies. Here are some key aspects to consider:

**Executive orders and national directives:** In the U.S., the "Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity," issued in January 2025, sets forth comprehensive cybersecurity standards, including those for AI-driven tools. This directive underscores the critical role of AI in detecting and mitigating advanced cyber threats in real-time.[15] However, given that this executive order is so new, the full impact and implications are still uncertain at this point.

**Global regulatory landscape:** For manufacturing companies operating on a global scale, navigating the diverse regulatory requirements related to data sovereignty, supply chain security, and incident reporting is essential. These regulations vary widely across regions, including the US International Traffic in Arms Regulations, EU data transfer laws, and similar regulations in China and India.

**Industry-specific guidelines:** Agencies like the Cybersecurity and Infrastructure Security Agency (CISA) offer detailed frameworks and guidance for implementing cybersecurity measures in critical infrastructure sectors, including manufacturing. These guidelines often encompass best practices for integrating AI into cybersecurity defenses.[15]

Navigating these regulations can be complex, but they are crucial for protecting manufacturing operations from cyber threats. A reliable technology partner can assist manufacturers in understanding and adhering to compliance requirements.

# Recommendations for IT security in manufacturing

## 1. Prepare your network

Design and maintain a robust network architecture that includes segmentation, access controls, and encryption. Regularly test and update network defenses to stay ahead of emerging threats.

## 2. Advanced Threat Detection

Invest in advanced threat detection and response solutions that can identify and mitigate cyberattacks in real-time. These solutions should be capable of monitoring both IT and OT environments.

3. Multi-factor authentication (MFA)

   Enforce the use of MFA across all systems to add an extra layer of security. This can significantly reduce the risk of unauthorized access even if credentials are stolen.

4. Supply Chain Security

   Collaborate with suppliers and partners to ensure they adhere to robust cybersecurity practices. Conduct regular assessments of their security measures to prevent supply chain breaches.

5. Regular Security Audits

   Conduct frequent security audits of both IT and OT systems to identify and mitigate vulnerabilities. Ensure that legacy systems are included in these audits.

6. Enhance regulatory compliance

   Ensure compliance with relevant cybersecurity regulations and standards. Conduct regular audits and assessments to identify and address compliance gaps.

7. Foster a culture of security

   Promote regular, industry-specific cybersecurity awareness training for all employees, from the factory floor to the executive suite. Use real-world scenarios to illustrate the risks and teach employees how to recognize and respond to phishing attempts. Encourage a culture where security is everyone's responsibility.

8. Utilize managed and professional services

   Leverage managed security services and professional cybersecurity expertise to enhance your security posture. These services can provide specialized knowledge and resources to address complex security challenges.

9. Incident Response Plan

   Develop and regularly update an incident response plan tailored to your manufacturing environment. This plan should include specific protocols for responding to phishing and social engineering attacks.

# How Lumen can help

## Networking and security solutions

With the integration of AI into manufacturing, the demand for high-capacity, low-latency networks has never been greater. Lumen's networking solutions are designed to support manufacturing companies as they prepare for this AI-enabled future. Our robust infrastructure, including our extensive fiber network and advanced AI-driven security solutions, helps to ensure that smart factories can leverage AI technologies to improve operational efficiencies and safety on the factory floor, and be proactive when it comes to maintaining critical machines and production lines.

Lumen provides AI-enabled connectivity, AI-optimized data/cloud, and AI-automated security, and includes the following suite networking and security solutions:

- **Network-as-a-Service (NaaS)**: Lumen® NaaS provides real-time, self-service, scalable control over network connectivity, enabling businesses to manage bandwidth, path, and latency dynamically.
- **Distributed Denial of Service (DDoS) Mitigation**: Lumen® DDoS Mitigation services provide comprehensive protection against DDoS attacks by rapidly filtering out malicious traffic and returning clean traffic to customers, leveraging a multi-layered scrubbing architecture and advanced threat intelligence from Black Lotus Labs.
- **Lumen Defender℠ powered by Black Lotus Labs®**: Lumen Defender℠, powered by Black Lotus Labs®, offers proactive network protection by automatically blocking traffic from risky sources before it breaches internal networks, leveraging unmatched threat intelligence.
- **Secure Access Service Edge (SASE)**: Lumen® SASE solutions unify network and security management through a centralized, cloud-based experience, simplifying the design, purchase, deployment, and orchestration of software-defined network infrastructure and information security.
- **SD-WAN**: Lumen® SD-WAN solutions support secure, scalable, and cost-efficient deployment and management of hybrid networks, providing complete visibility, control, and security across various connectivity types.
- **Rapid Threat Defense**: Rapid Threat Defense integrates Black Lotus Labs intelligence to proactively block known malicious traffic, enhancing operational efficiency and reducing the burden on IT staff.
- **SOCaaS**: Lumen® Security Operations Center as a Service (SOCaaS) offers fully managed cybersecurity threat detection, incident management, and response support, providing visibility across an agency into cyber activity.
- **Incident reporting**: Lumen Incident Reporting system provides prompt reporting and management of risk-related incidents involving company employees, vehicles, and facilities, facilitating rapid response and resolution.
- **Managed and professional services**: Lumen® Managed and Professional Security solutions provide comprehensive protection through proactive threat monitoring, incident response, penetration testing and tailored advisory services, help ensure robust security and compliance for businesses.

BLACK LOTUS LABS® by Lumen

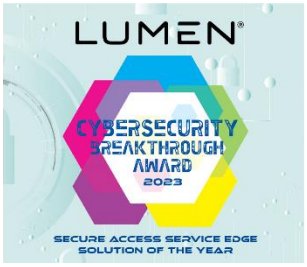
Black Lotus Labs® is the award-winning, in-house threat research arm of Lumen. The team of data scientists, reverse engineers, security engineers, and threat analysts leverages their unmatched visibility into the Lumen network to protect businesses and help keep the internet clean.

Black Lotus Labs use advanced threat technology to identify and eliminate threats quickly, employing machine learning algorithms to automate protection and neutralize threats. The team has been involved in the identification and takedown of some of the most high-profile malware of the past decade.

LUMEN®

By providing secure, high-speed connectivity and real-time data processing capabilities, Lumen helps to enable manufacturers to implement AI applications such as predictive analytics, digital twins, and automated repetitive tasks on the production floor. This helps to accelerate production lines, minimize security and compliance risks, reduce costs and increase revenue.

Lumen has won three consecutive Cybersecurity Breakthrough Awards including the 2022 Network Security Provider of the Year award, the 2023 SASE Solution of the Year award, and the 2024 Threat Intelligence Company of the Year award.



## The bottom line

The integration of AI into manufacturing operations presents both opportunities and challenges in the realm of cybersecurity. By understanding current security trends, vulnerabilities, regulatory changes and the impact of AI, manufacturers can better prepare for and mitigate cyber threats. Implementing robust security measures, staying updated with regulations, and fostering a culture of security are essential steps in safeguarding confidential IP and factory data while helping to ensure the continued advancement of manufacturing technology.

**Your network infrastructure is the cornerstone of your AI efforts**

The Lumen network supports the dynamic demands of AI-powered technologies and enhances smart manufacturing by providing high-capacity connections, deep IP peering and AIOps to leverage AI/ML apps without the constraints of a traditional network.

**VIEW SECURE SOLUTIONS**

# Footnotes

[1] Top Cyber Threats in Manufacturing | MxD | February 2025
[2] 2025 Trustwave Manufacturing Risk Radar Report | Trustwave | April 2025
[3] Recent Cyber Attacks in Manufacturing | IronEdge Group | 2025
[4] The Biggest Cybersecurity Issues Heading into 2025 | InformationWeek | January 2025
[5] Why Manufacturers Are Top Targets for Cyber Criminals | NFP | May 2024
[6] The Biggest Cyber Threats Manufacturers Face in 2025 | Industry Today | April 2025
[7] Gartner Predicts 30% of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to Deepfakes by 2026 | Gartner | February 2024
[8] AI-Supported Spear Phishing Fools More Than 50% of Targets | Malwarebytes | January 2025
[9] AI-Driven Malware: Detecting and Preventing Next-Gen Cyberattacks | Virtual Guardian | March 2025
[10] Cybercriminals Are Targeting AI Agents and Conversational Platforms | Cybersecurity Ventures | December 2024
[11] Top Digital Trends for 2024 | Frost & Sullivan | April 2024
[12] ISC2 2024 Cybersecurity Workforce Study | ISC2 | October 2024
[13] Top Pitfalls to Avoid When Implementing AI in the Enterprise | Lumen | 2024
[14] Cybersecurity Considerations for the Industrial Manufacturing Sector | KPMG | 2024
[15] Cybersecurity Executive Order – Key Implications for the Manufacturing Industry | Foley & Lardner LLP | January 2025



## Why Lumen?

Lumen is your single provider to enable digital transformation. With a comprehensive portfolio and experienced talent, we can help safeguard your customer experience, protect your confidential data, and manage threats. Backed by the extensive and deeply peered Lumen global network, Black Lotus Labs® threat intelligence, and our skilled and experienced team of security experts, Lumen is a trusted partner to help improve your security posture.

866-352-0291 | lumen.com | info@lumen.com



LUMEN®