



CYBER REPORT

MANUFACTURING

2025

The manufacturing industry, which is integral to the economy, involves the production of goods using labor, machines, tools, and chemical or biological processing. Manufacturing organizations face significant cybersecurity risks that can lead to data breaches, operational disruptions, and financial losses. They often handle sensitive data such as intellectual property, trade secrets, proprietary production data, and customer information. To mitigate these threats, they must implement comprehensive cybersecurity measures and continuously monitor and update security protocols. Learn about the risks for manufacturing in our report.

MARKET INSIGHTS

634,000

Manufacturing companies
in the United States

2,305

Total number of reported
cyber incidents annually

\$5.56M

Average cost of each
reported cyber incident



TOP CYBER RISKS

- **Industrial Espionage:** theft of sensitive intellectual property and trade secrets
- **Ransomware:** data encryption and ransom demands can halt operations
- **Supply Chain:** exploitation of weak links in the supply chain poses great risk
- **Operational Technology (OT):** targeting unprotected OT systems like SCADA and ICS
- **Phishing/Social Engineering:** unauthorized access to systems by stealing legitimate credentials
- **Insider Threats:** data breaches or sabotage by employees or contractors
- **Legacy Systems:** vulnerabilities in older systems lacking modern security
- **Third-Party Vendors:** vulnerabilities introduced by partners and suppliers
- **Data Privacy/Compliance:** compliance with data protection regulations
- **Intellectual Property Theft:** unauthorized access to sensitive design or customer data.

Manufacturing was the most attacked industry in

**2022, 2023,
& 2024**

Biggest industry financial loss impact:

**Downtime &
Business Interruption**

WHY IS MANUFACTURING TARGETED?

- **Valuable IP:** Manufacturing companies hold valuable intellectual property that attackers can steal for profit or espionage.
- **Operational Disruption:** Cyber attacks can halt manufacturing operations, causing costly downtime and equipment damage.
- **Supply Chain Weaknesses:** Attackers exploit vulnerabilities in interconnected supply chains to access multiple organizations.
- **Outdated Systems:** Many manufacturing facilities use legacy systems with known security flaws, making them easy targets.
- **Low Cyber Awareness:** The sector often lacks cybersecurity training, making employees more susceptible to phishing and other attacks.

In the event of a cyberattack, a manufacturing company is likely to incur total losses of

\$290K - \$50M+

The average likelihood of manufacturing companies suffering a cyber event in the next 12 months.

20%

KEY STATS

- **A Growing Resource and Skills Gap:** 68% of respondents said their IT teams are understaffed or lack the necessary training to manage growing network complexities.
- **Visibility as a Priority:** 64% identified real-time network visibility as crucial to maintaining security and operational efficiency in a global manufacturing context.
- **Secure Global Connectivity:** 54% of manufacturing leaders highlighted the need for secure access for remote teams and global sites, emphasizing the importance of consistent and reliable connectivity.
- **Cost Control and Simplification:** 50% of respondents indicated that simplifying network management and controlling costs are essential, particularly as they expand into cloud and multi-cloud environments.
- **Convergence as a Strategic Advantage:** Manufacturing organizations see value in converged network and security solutions, which offer enhanced security, operational resilience, and reduced IT workloads.

Source: Manufacturing.net, [Report Explores Network Security Trends in Manufacturing](#)



SpearTip Cyber Solutions to Assist Manufacturing



Rapid Incident Response

- Data Breach Investigation
- Decryption Assistance
- Digital Forensics



24/7 Managed SOC

- Endpoint Protection
- Identity Threat Detection



Risk Assessments

- Cybersecurity Health Check
- Cybersecurity Gap Analysis
- Tabletop Exercises



Vulnerability Assessments

- External & Internal
- Web Application
- Wireless, Firewall, and Cloud



Adversary Services

- Penetration Testing



Security Program Development

- Incident Response Planning
- Phishing Campaign Assessment
- Managed Security Awareness Training

OUR ANALYSIS

- Supply chain attacks can stress business resiliency and any event that causes business interruption typically causes the highest losses.
- Many manufacturers lack plans for incident response, disaster recovery, and business continuity. If they do exist, most plans are often out of date and limited.
- Skills gap and resource limitations for cybersecurity often pose challenges to manufacturing entities.

Sources: IBIS Manufacturing in the US, IBM Cost of a Data Breach Report; IBM X-Force Threat Intelligence Report 2024; Security Magazine; Verizon 2024 Data Breach Investigations Report; Reuters Cyber

SpearTip, a Zurich Company
1714 Deer Tracks Trail, St. Louis, MO
800.236.6550 www.speartip.com

For further information, please contact the SpearTip Security Operations Center team at info@speartip.com

This is a general description of certain types of managed security services, and/or other risk engineering or risk management services provided by Zurich Resilience Solutions, which is part of the Commercial Insurance business of Zurich Insurance Group and does not represent or alter any insurance policy or service agreement. Such services are provided to qualified customers by affiliates of Zurich Insurance Company Ltd, including but not limited to SpearTip, LLC, 1714 Deer Tracks Trail Suite 150, Saint Louis, MO 63131, USA; and The Zurich Services Corporation and Zurich American Insurance Company, each at 1299 Zurich Way, Schaumburg, IL 60196, USA. The opinions expressed herein are those of SpearTip, LLC as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (collectively, Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction. In the United States, managed security services are provided by SpearTip, LLC and risk engineering and risk management services are provided by The Zurich Services Corporation.