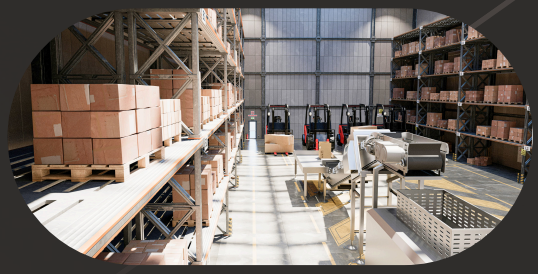
→ CyberResilience.com



The state of cybersecurity in manufacturing

A historical and current landscape analysis

resilience

The state of cybersecurity in manufacturing

A HISTORICAL AND CURRENT LANDSCAPE ANALYSIS

Executive summary

The manufacturing sector now holds the title of the world's most targeted industry, yet its cybersecurity posture remains dangerously out of step with its exposure. For many manufacturers, a fundamental tension persists: the perceived risk of taking production offline to implement security controls often feels greater than the risk of operating without them. Tracing the transformation from isolated industrial control systems to the hyper-connected, AI-augmented threat landscape of 2026, this report grounds its findings in proprietary Resilience claims data from nearly five years of the manufacturing portfolio.

Several converging forces have driven this shift. The rapid adoption of Industry 4.0 technologies has dissolved the boundaries between information technology (IT) and operational technology (OT), creating vast new attack surfaces. Ransomware groups have industrialized their operations, viewing manufacturers as ideal targets due to their low tolerance for downtime and their historically underfunded security programs. Meanwhile, nation-state actors increasingly target manufacturers across subsectors for intellectual property theft, supply chain disruption, and strategic advantage.

The data is stark. Between January and September 2025, global ransomware incidents rose by roughly 46% over the same period in 2024, with manufacturing experiencing a 61% year-over-year surge — the sharpest growth of any sector.[2] According to the IBM X-Force Threat Intelligence Index, manufacturing accounted for more than one in four of all cyberattacks in 2025.[1]

Resilience's own claims data reinforces the external picture. Across nearly five years of the manufacturing portfolio, ransomware accounts for 90% of total incurred losses, dwarfing all other causes of loss combined.[4] Yet the data also reveals that the most expensive losses stem from specific, identifiable control failures. MFA misconfiguration is the single most expensive point of failure in the portfolio, accounting for approximately 26% of all losses — more than the 8% attributable to having no MFA at all. The single most expensive ransomware event in the portfolio, a BlackCat-attributed incident, was directly enabled by misconfigured MFA. These are fixable problems with outsized financial consequences.

Key statistics at a glance

External threat landscape

1 IN 4
cyberattacks targeted manufacturing in 2025

61%
YoY surge in ransomware attacks on manufacturing

71%
surge in threat actor activity targeting the sector

$10B+
estimated global damages from NotPetya (2017)

73%
of orgs experienced an OT breach in 2024

5TH YEAR
as the most targeted industry globally

Resilience claims data

March 2021–February 2026

90%
of incurred losses attributable to ransomware

~26%
of losses from MFA misconfiguration — the #1 point of failure

~13%
of losses from software vulnerability exploits

~8%
of losses from no MFA — less than from misconfigured MFA

~30%
of claims from transfer fraud and email compromise, both driven by phishing

12%
of claim volume is ransomware — but drives 90% of losses

A brief history of manufacturing cybersecurity

NEAR-TERM (2025–2028)

The pre-digital era and air-gapped assumptions

For most of the twentieth century, manufacturing facilities operated in effective isolation. Industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs) were designed to automate physical processes with minimal human intervention. These systems were built for reliability and longevity, not connectivity. Many had lifespans exceeding 20 years, and because they were disconnected from corporate networks and the internet, cybersecurity was simply not a design consideration.[21]

This air-gapped architecture created a false sense of security. The assumption that physical separation from the internet equaled safety would persist for decades and proved to be one of the most consequential blind spots in industrial security.

2010

Stuxnet rewrites the rules

The discovery of Stuxnet in 2010 marked a turning point not just for manufacturing cybersecurity, but for cyberwarfare itself. Stuxnet was a highly sophisticated computer worm, widely attributed to a joint U.S.-Israeli operation, that targeted Siemens SCADA systems controlling centrifuges at Iran's Natanz uranium enrichment facility.[7]

What made Stuxnet unprecedented was its ability to cause physical destruction through digital means. The worm manipulated the speed of centrifuge motors while feeding falsified data back to monitoring systems. It reportedly destroyed nearly 1,000 centrifuges and set Iran's nuclear program back by months or years.[6]

Stuxnet demonstrated several realities that continue to define manufacturing cybersecurity today. It proved that air-gapped systems could be breached. It showed that cyberattacks could cause physical damage to industrial infrastructure. And it established a blueprint that threat actors have studied and adapted ever since.[5]

2017

WannaCry, NotPetya, and the dawn of industrial ransomware

Two attacks in 2017 brought manufacturing cybersecurity to the attention of boardrooms worldwide.

WannaCry erupted in May 2017, exploiting a Windows vulnerability called EternalBlue to spread across networks without human interaction. It affected more than 200,000 devices in over 150 countries. Manufacturers including Honda and Nissan were forced to halt production at multiple facilities.[8]

NotPetya arrived just weeks later and proved to be far more destructive. Although it masqueraded as ransomware, it was actually a wiper designed to destroy data irreversibly. The total damage was estimated at over $10 billion globally.[9] Merck lost approximately $870 million.[10] Maersk lost $250–300 million.[11] Mondelēz incurred $188 million in damages, and FedEx's TNT Express subsidiary lost roughly $400 million.[12]

NotPetya also became a landmark case in cyber insurance when Zurich denied Mondelēz's claim under a war exclusion clause.[13]

RESILINCE CLAIMS DATA

Ransomware dominates manufacturing losses

Resilience claims data confirms what the external landscape suggests: ransomware is the overwhelming driver of financial loss in the manufacturing sector. While ransomware accounts for only about 12% of total claim volume, it is responsible for 90% of incurred losses — a sharply concentrated loss pattern in which a small number of high-severity events drive the total.

2020–2021

COVID-19 accelerates the threat

The pandemic dramatically expanded the manufacturing sector's attack surface at precisely the moment it was least prepared to defend it. Lockdowns pulled workers off factory floors, forcing manufacturers to stand up remote access to operational technology systems that had never been designed for it. Engineers who had previously walked the production line now needed VPN connections and remote desktop access to the same SCADA dashboards. In many cases, these pathways were deployed under emergency timelines with minimal security review — no multi-factor authentication, default credentials left in place, and broad network access granted where narrow permissions were needed. At the same time, severe supply chain disruptions drove rapid adoption of IoT sensors, cloud monitoring, and connected analytics tools, dissolving boundaries in what had been relatively isolated OT environments.

The pressure to maintain production compounded the risk. Manufacturers of medical devices, pharmaceuticals, food and beverage, and other essential goods could not afford to shut down, making them especially vulnerable to ransomware operators who understood that downtime tolerance was effectively zero. A manufacturer running at full capacity during a global supply crunch was more likely to pay a ransom quickly. Meanwhile, IT security teams were stretched thin managing the broader corporate shift to remote work, leaving fewer resources to monitor and secure newly connected OT systems.

The results were dramatic. According to the 2021 Global Threat Intelligence Report, manufacturing jumped from the eighth most targeted industry to second in a single year, representing a 300% increase in attack volume.[14] The Colonial Pipeline attack in 2021, though targeting an energy company, sent shockwaves through the manufacturing sector by demonstrating the real-world consequences of ransomware on critical infrastructure operations.

The current threat landscape

Manufacturing as the top target

By 2025, manufacturing has become the most targeted sector globally across multiple threat intelligence reports. The IBM X-Force Threat Intelligence Index found that the sector accounted for more than one in four of all cyberattacks, making it the most attacked industry for the fifth consecutive year.[1] KELA's research found that ransomware incidents globally rose by roughly 46% year-over-year through the first three quarters of 2025, with manufacturing experiencing the sharpest growth at 61%.[2] Bitsight reported a 71% surge in threat actor activity targeting the sector.[3]

Dominant attack vectors

- **Ransomware**

  Ransomware remains the primary threat to manufacturers. Dragos reported that more than half of all observed ransomware victims in 2024 were in the manufacturing sector.[15] A Sophos survey found that roughly two in three manufacturing companies had been hit by ransomware.[16]

  High-profile incidents in 2025 included a global shutdown at Jaguar Land Rover and production disruptions at Bridgestone.[2] Medical device manufacturer Masimo discovered unauthorized network access that forced facilities to operate below capacity for weeks.[17]

- **Compromised credentials and identity-based attacks**

  Compromised credentials have become the preferred entry point for cybercriminals, accounting for roughly three in ten incidents according to IBM.[1] Attackers obtain these credentials primarily through infostealer malware delivered via phishing emails — which surged 84% year-over-year in 2024[1] — and through credential phishing sites that mimic legitimate login pages. Once obtained, valid credentials allow attackers to log into enterprise systems as if they were authorized users, blending into normal network activity and evading detection. Adversary-in-the-middle phishing kits, now sold as turnkey services on the dark web, can intercept MFA codes in real time, meaning even accounts with multi-factor authentication enabled are not immune.

  RESILINCE CLAIMS DATA

  MFA misconfiguration is the #1 point of failure

  Resilience claims data identifies MFA misconfiguration as the single most expensive point of failure in the manufacturing portfolio, more costly than the absence of MFA itself. The most expensive ransomware event in the portfolio — a BlackCat-attributed incident — was enabled by misconfigured MFA. Implementation quality matters as much as implementation itself.

- **Supply chain attacks**

  Manufacturing's dependence on complex global supply chains creates inherent vulnerability, sending a ripple effect shared by manufacturing, distribution, and wholesale/retail. The World Economic Forum's Global Cybersecurity Outlook 2025 highlighted supply chain attacks as a notably increasing risk.[18]

Intellectual property theft and nation-state espionage

China-linked threat actors continued to target emerging technology, semiconductor companies, defense contractors, and other high-tech manufacturers throughout 2024 and 2025 looking to disrupt operations or garner precious IP to kickstart efforts to eclipse US technological capabilities in an arms race for superiority.[3]

What Resilience claims data tells us about manufacturing risk

The analysis that follows is drawn from Resilience's manufacturing claims portfolio, spanning March 2021 through February 2026. Claims associated with a specific external vendor incident (CDK) in June 2024 have been excluded to provide a baseline view of industry risk.4

The ransomware dominance

Financial volatility across the manufacturing portfolio is driven almost entirely by the presence or absence of a material ransomware event in any given quarter. A small number of high-severity events drive the total, with a single BlackCat-attributed incident representing the most expensive loss in the dataset. The strategic implication is that quarter-over-quarter loss variation in the sector is less a function of threat volume than of whether the quarter happened to include a catastrophic ransomware event.

The frequency versus severity gap

The claims data reveals a sharp divide between the incidents that happen most often and the incidents that cost the most.

High frequency, lower severity: Transfer fraud (15% of claims) and email compromise (14%) are the most common incident types. Transfer fraud claims average approximately ten times the payout of email compromise claims.

Lower frequency, high severity: Ransomware occurs far less often but dictates the total financial risk to the portfolio. The strategic implication is that reducing claim frequency alone does not meaningfully reduce total financial exposure — severity reduction requires targeting the specific controls that prevent or contain ransomware events.

Top losses by cause

The following table summarizes the share of total incurred losses by cause:

Cause of loss	Share of losses
Ransomware	90%
Transfer fraud	4.2%
Ransomware (vendor)	2.2%
Email compromise	<1%

Critical points of failure

The claims data identifies the specific technical or procedural gaps that enabled the most expensive losses in the portfolio.

- **MFA misconfiguration**

  MFA misconfiguration is the single most expensive point of failure in the portfolio, accounting for approximately 26% of all incurred losses. Misconfigured MFA — where the control exists but is improperly deployed, not enforced on all accounts, or subject to bypass conditions — accounts for significantly more losses than the absence of MFA.

  The absence of MFA also appears as a point of failure, accounting for approximately 8% of total portfolio losses. Both findings underscore that identity and access controls are central to manufacturing cyber risk, and that implementation quality matters as much as implementation itself.

  RESILINCE CLAIMS DATA

  The most expensive event was enabled by a control that was in place

  The most expensive ransomware event in the Resilience manufacturing portfolio — a BlackCat-attributed incident — was not caused by the absence of a security control. It was caused by a control that was deployed but misconfigured. MFA misconfiguration accounts for approximately 26% of all portfolio losses, making it the single largest point of failure. Resilience efforts should focus on auditing and validating existing MFA deployments, not just implementing them.

- **Software vulnerabilities**

  Exploits of software vulnerabilities account for approximately 13% of total portfolio losses, concentrated in a small number of high-severity ransomware events. These include incidents attributed to Black Basta and Cactus, which together represent the majority of vulnerability-driven losses. The consistent link between software vulnerability exploitation and ransomware outcomes underscores that patch management failures and ransomware exposure are directly connected in the manufacturing sector — a connection that is particularly relevant given that legacy OT systems often cannot be patched without production downtime.

- **Phishing**

  Phishing is the primary human-centric failure point in the portfolio, identified as the point of failure in virtually all transfer fraud claims. Transfer fraud and email compromise — both driven by phishing — together account for nearly 30% of all claim activity, making phishing the most consistent initial access vector by volume.

A note on wrongful data collection

Wrongful data collection also appears in the claims data, driven primarily by website tracking and pixel-related litigation rather than operational data collection from connected manufacturing systems. The vast majority of these claims result in zero payout, though the category does include one material privacy-related settlement. Because these claims are not unique to the manufacturing sector and their drivers are still being analyzed, they are noted here for completeness but are not featured as a headline finding of this report.

Quarterly stability of non-material risks

The quarterly claims data reveals a highly consistent baseline of non-material claims which typically result in minimal incurred losses. This pattern indicates that manufacturing firms in the Resilience portfolio are generally resilient against minor threats but struggle to contain the material events — primarily ransomware — that bypass primary controls. The financial risk to the portfolio is not driven by an accumulation of small losses but by the periodic occurrence of material ransomware events.

Structural vulnerabilities in manufacturing

The IT/OT convergence challenge

The central structural vulnerability in manufacturing cybersecurity is the convergence of information technology and operational technology. A Fortinet 2024 report revealed that nearly three in four organizations experienced an OT-impacting breach, up from roughly half the year before.[20] The number of internet-exposed ICS devices rose 40% between 2024 and 2025.[19]

Legacy systems and technical debt

OT environments are defined by legacy technology. NIST guidance notes that the lifespan of an OT system can exceed 20 years.[21] Many of these systems run on outdated operating systems that no longer receive security patches — a structural reality that connects directly to the ~13% of portfolio losses attributable to software vulnerability exploits. When legacy OT systems cannot be patched without production downtime, the financial cost of that technical debt shows up in ransomware claims attributed to actors like Black Basta and Cactus.

The cybersecurity maturity gap

Despite being the most targeted sector, manufacturing has historically underinvested in cybersecurity. Manufacturing and retail allocate the lowest percentage of IT budgets to security.[22]

The skills gap compounds the problem. Over half of cybersecurity professionals report their budgets are underfunded.[23]

The evolving regulatory and insurance landscape

Government and regulatory responses

In the United States, the Cybersecurity Maturity Model Certification (CMMC) program establishes minimum cybersecurity requirements for companies in the defense supply chain.[24] The Biden administration proposed a multibillion-dollar federal cybersecurity budget for fiscal year 2025.[25]

Internationally, the European Union's NIS2 directive has expanded cybersecurity obligations to include manufacturing entities.[26] Nearly half of manufacturing organizations now align their ICS security programs with the NIST Cybersecurity Framework.[27]

The cyber insurance dimension

The insurance industry has played a pivotal role in shaping how manufacturers approach cyber risk. Underwriting has tightened as losses mount, with insurers increasingly requiring evidence of specific security controls as conditions for coverage.

The NotPetya war exclusion litigation set a precedent that continues to influence policy language around state-sponsored attacks.[13]

RESILINCE CLAIMS DATA

Claims data as a feedback loop for underwriting

Resilience's claims data provides a direct feedback loop between loss experience and underwriting. The finding that MFA misconfiguration is the single most expensive point of failure in the portfolio — accounting for approximately 26% of all losses, more than the 8% attributable to the absence of MFA — informs not just which controls to require, but how to evaluate whether those controls are working as intended. This shifts the underwriting conversation from "do you have MFA?" to "is your MFA properly configured and enforced across all access points?"

Emerging threats and the road ahead

AI-amplified attacks

AI enables more sophisticated phishing campaigns, deepfake-based social engineering, and automated vulnerability scanning.[28] Organizations using AI extensively in cybersecurity prevention report significantly lower breach costs than those that do not.[29]

Post-quantum cryptography

Of internet-accessible SSH servers globally, fewer than one in fifteen have adopted quantum-resistant encryption.[30]

Expanding attack surface through IoT and IIoT

Connected IoT devices are projected to more than double between 2025 and 2030, with each additional sensor, actuator, and monitoring device on a factory floor representing a potential entry point.[31]

Strategic priorities for manufacturing security leaders

Combining external threat intelligence with Resilience's claims data, the following priorities represent the highest-leverage investments for CISOs and security leaders in the manufacturing sector. They are ordered by demonstrated financial impact in the Resilience portfolio.

1 Audit and validate MFA deployment

MFA misconfiguration is the single most expensive point of failure in the manufacturing claims portfolio. The priority is not just deploying MFA but auditing existing deployments to ensure enforcement across all accounts, elimination of bypass conditions, and proper configuration of conditional access policies. Organizations should treat MFA validation as a continuous process, not a one-time implementation.

RESILINCE CLAIMS IMPACT

MFA misconfiguration accounts for ~26% of total portfolio losses and enabled the single most expensive ransomware event in the dataset

2 Strengthen vulnerability management for external-facing systems

Software vulnerability exploits are directly linked to the most expensive ransomware outcomes in the portfolio. Where patching is not feasible due to OT constraints, organizations should implement compensating controls including network isolation, virtual patching, and enhanced monitoring of vulnerable systems.

RESILINCE CLAIMS IMPACT

Software vulnerability exploits account for ~13% of total portfolio losses, concentrated in high-severity ransomware events attributed to Black Basta and Cactus

3 Implement procedural controls for financial transfers

Transfer fraud and email compromise represent the most frequent claim activity in the portfolio. Manufacturers should implement verification procedures for financial transfers, including out-of-band confirmation for payment changes, dual authorization for large transactions, and targeted training for finance and accounting teams.

RESILINCE CLAIMS IMPACT

Transfer fraud and email compromise together account for ~30% of all claims; phishing is the point of failure in virtually all transfer fraud claims

4 Invest in ransomware containment and response

Because ransomware drives the overwhelming majority of financial loss, the ability to detect and contain a ransomware event before it becomes material is the highest-leverage capability a manufacturer can build. This includes network segmentation between IT and OT environments, endpoint detection and response with ransomware-specific policies, tested backup and recovery procedures, and incident response plans tailored to production environments.

RESILINCE CLAIMS IMPACT

Ransomware accounts for 90% of total incurred losses, concentrated in a small number of high-severity events

5 Extend security requirements to vendors and supply chain partners

Vendor security gaps appear as a distinct cause of loss in the claims data. Manufacturers should extend their security requirements to critical vendors, including contractual MFA and patching requirements, continuous monitoring of vendor risk posture, and contingency plans for disruptions to critical suppliers.

RESILINCE CLAIMS IMPACT

Vendor-related ransomware accounts for 2.2% of total portfolio losses

6 Cyber risk quantification and transfer

Translating cybersecurity risk into financial language that resonates with CFOs and boards is essential for securing adequate investment. The claims data provides a concrete basis for this conversation: ransomware dominates loss, a single point of failure (MFA misconfiguration) drives the largest share of exposure, and unpatched software is a direct line to the most expensive outcomes. These findings map directly to specific control investments and insurance coverage decisions.

References

1 IBM, X-Force Threat Intelligence Index 2025.

2 KELA, “Escalating Ransomware Threats to National Security,” October 2025.

3 Bitsight, “State of the Underground Report,” 2025.

4 Resilience proprietary claims data. Analysis spans March 2021 through February 2026, with claims associated with the CDK vendor incident in June 2024 excluded to provide a baseline view of industry risk.

5 Kaspersky, “What Is Stuxnet?” October 2025; Britannica, “Stuxnet,” 2011.

6 Symantec, “W32.Stuxnet Dossier,” 2011.

7 Kim Zetter, Countdown to Zero Day (Crown, 2014); Stanford CISAC, “Stuxnet: The World’s First Cyber Weapon,” 2015.

8 Forescout, “Since Stuxnet: A Brief History of Critical Infrastructure Attacks,” February 2025.

9 White House assessment, as cited in Columbia University SIPA case study, “NotPetya,” 2021.

10 Merck SEC filings, Q3 2017; New York Federal Reserve Staff Report No. 937, “Pirates Without Borders,” 2020.

11 A.P. Moller-Maersk, Q2 2017 interim financial report.

12 Columbia University SIPA case study, “NotPetya,” 2021.

13 The Council of Insurance Agents & Brokers, “NotPetya: A War-Like Exclusion?” May 2019.

14 NTT Security, Global Threat Intelligence Report (GTIR), 2021.

15 Dragos, “OT/ICS Cybersecurity Report: Year in Review,” 2025.

16 Sophos, “The State of Ransomware in Manufacturing and Production,” 2024.

17 SOCRadar, “Major Cyber Attacks Targeting Manufacturing Industry in 2025,” June 2025; Masimo SEC filing, April 2025.

18 World Economic Forum, Global Cybersecurity Outlook 2025.

19 SOCRadar, “CISA Industrial Control Systems (ICS) Advisories Recap for 2025,” December 2025.

20 Fortinet, “State of Operational Technology and Cybersecurity Report,” 2024.

21 NIST, “Guide to Operational Technology (OT) Security,” SP 800-82 Rev. 3

22 Nordlayer, “Optimize Your 2026 Cybersecurity Budget Allocation,” 2025.

23 ISACA, “State of Cybersecurity 2024 and Beyond.”

24 Alston & Bird, “5 Things Manufacturing GCs Should Know About Cyber Risk,” Law360, July 2025.

25 Federal News Network, “Biden Budget Request Includes $13B for Cybersecurity,” March 2024.

26 European Union, Directive (EU) 2022/2555 (NIS2)

27 Elisity, “Industrial Cybersecurity Budget Alignment: A Manufacturing Framework Guide for 2025,” January 2025.

28 World Economic Forum, Global Cybersecurity Outlook 2025; Cobalt, “Top Cybersecurity Statistics for 2025,” November 2025.

29 Elisity, “Cybersecurity Budget Benchmarks for 2025,” October 2024

30 Forescout, post-quantum cryptography analysis, 2025.

31 Asimily, “5 Operational Technology Challenges in 2024,” August 2025.

Methodology and sources

External sources

This report synthesizes publicly available data from the following industry and government sources. All external claims are cited with numbered endnotes throughout the document.

- IBM, X-Force Threat Intelligence Index 2025
- KELA, "Escalating Ransomware Threats to National Security," October 2025
- Bitsight, "State of the Underground Report," 2025
- Dragos, "OT/ICS Cybersecurity Report: Year in Review," 2025
- Sophos, "The State of Ransomware in Manufacturing and Production," 2024
- Fortinet, "State of Operational Technology and Cybersecurity Report," 2024
- World Economic Forum, "Global Cybersecurity Outlook 2025"
- CISA, Industrial Control Systems Advisories, 2024–2025
- Forescout, "Since Stuxnet: A Brief History of Critical Infrastructure Attacks," 2025
- NIST, "Guide to Operational Technology (OT) Security," SP 800-82 Rev. 3
- ISACA, "State of Cybersecurity 2024 and Beyond"

Resilience data

Resilience's proprietary data is drawn from the manufacturing cyber insurance claims portfolio. The dataset spans March 2021 through February 2026. Claims associated with the CDK vendor incident in June 2024 have been excluded to provide a view of baseline industry risk independent of a single, widely-reported supply chain event. Analysis includes cause-of-loss classification, point-of-failure identification, material claim designation, threat actor attribution, and quarterly trend analysis. All figures reflect incurred losses as of the most recent available analysis period. Findings represent the Resilience manufacturing portfolio and should not be interpreted as representative of the broader manufacturing sector.