# **The Reshaping of Manufacturing: Cyber Risks, Critical Events, and Strategic Imperatives (June - August 2025)**

## **Executive Summary**

The manufacturing sector is facing an unprecedented wave of cyberattacks, solidifying its position as the most targeted industry globally for the third consecutive year.1 A confluence of factors—accelerated digital transformation, the convergence of information technology (IT) and operational technology (OT) systems, and a brittle, interconnected supply chain—has created a uniquely vulnerable landscape. The past 60 days, from mid-June to mid-August 2025, have been marked by a significant surge in both financially motivated ransomware campaigns and sophisticated, state-sponsored espionage operations.

A key development during this period has been the massive volume of new Industrial Control Systems (ICS) advisories released by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), underscoring the foundational insecurity of the critical infrastructure that powers global production.2 Attackers are capitalizing on these systemic weaknesses through well-established methods like exploiting unpatched vulnerabilities and leveraging social engineering, as well as evolving tactics such as rebranding their operations and using supply chain partners as backdoors to their ultimate targets.1 The distinction between financially motivated cybercriminals and state-aligned actors is becoming increasingly blurred, as both seek to exfiltrate high-value intellectual property (IP) and disrupt critical infrastructure for strategic gain.7

This report presents a deep-dive analysis of the manufacturing sector's cyber threat landscape, providing detailed incident breakdowns and actionable strategic recommendations. The findings underscore the urgent need for a fundamental shift in defense strategy—from a reactive, protection-oriented model to a proactive, resilience-by-default posture. To effectively counter these threats, manufacturing leaders must prioritize urgent vulnerability management, enforce strict supply chain vetting, and bridge the security gap between IT and OT, recognizing that a breach is not a matter of "if," but "when."

## **1. The Industrial Threat Landscape: Manufacturing as a Prime Target (June-August 2025)**

The manufacturing sector remains a top target for cybercriminals, a trend that has held for three consecutive years.1 As of 2024, the industry accounted for over a quarter (25.7%) of all incidents within the top ten most attacked industries, driven by its critical role in the global economy and an accelerating reliance on connected devices and technologies.1 The high-pressure, low-downtime nature of manufacturing operations makes it a particularly attractive target, as operational halts can lead to immediate and substantial financial losses.10

A central and unifying trend driving this heightened risk is the convergence of IT and OT systems.11 Traditionally, OT networks, which control industrial processes and physical equipment like SCADA systems and programmable logic controllers (PLCs), were physically isolated from the internet. This "air-gapped" model was long considered a reliable security measure. However, this assumption is no longer a viable defense. Modern factories are voluntarily or involuntarily connecting these OT environments to IT networks for a variety of business-enabling purposes, such as remote diagnostics, energy optimization, and feeding real-time data to analytics platforms and AI models.11

This creates a vast new attack surface where a compromise on the IT side—often the less-secure business network—can provide a direct entry point for attackers to pivot to the production-critical OT environment. The August 2023 ransomware attack on Clorox serves as a foundational example of this paradigm shift. A breach on the IT network forced the company to shut down critical systems, bringing operations to a halt, causing product shortages, and stretching recovery efforts into the next quarter.12 This incident clearly demonstrated that when IT systems fail, OT operations often follow, revealing that the air-gap is no longer a reliable defense but a legacy concept. Security strategies must now be holistic, not siloed, to protect the entirety of the converged network.

Furthermore, the manufacturing supply chain has become a primary avenue for attack, viewed by many organizations as the single greatest barrier to cyber resilience.13 Modern supply chains are complex and often opaque, with adversaries exploiting the security weaknesses of third-party suppliers and partners to gain downstream access to larger, more valuable targets.6 A single compromised vendor can trigger a cascading global disruption, as evidenced by the 2023 MKS Instruments ransomware breach, which resulted in an estimated $250 million loss for its key customer, Applied Materials.7

The motivations behind these attacks are increasingly complex, driven by both traditional financial gain and state-sponsored espionage.10 While ransomware and data extortion continue to be the most common financially motivated threats, state-aligned advanced persistent threat (APT) groups are also actively targeting the manufacturing sector for intellectual property (IP) theft and economic espionage.7 The semiconductor industry is a prime example of this geopolitical risk, where proprietary chip designs and process data are coveted targets.7 This elevates the supply chain problem from a business risk to a national security imperative, as the "new global trade war" is being waged with cyber espionage rather than just tariffs.7 If state-backed actors can steal key IP, it can fundamentally weaken a nation's technological leadership and defense readiness.

## **2. Detailed Incident Analysis: How Attacks Unfolded (June-August 2025)**

The period from June to August 2025 saw several high-profile incidents that illustrate the manufacturing sector's vulnerability and the attackers' evolving methods.

| Incident | Victim | Date | Known Threat Actor | Method | Primary Impact |
| --- | --- | --- | --- | --- | --- |
| Nucor Corporation Incident | Nucor Corporation (Steel) | June 2025 | Unspecified, Ransomware Suspected | Unauthorized system access, data exfiltration | Temporary production halt, data theft 15 |
| Warlock Attack | Indian Manufacturing Company | July 2025 | Warlock Ransomware Group | Ransomware, Data Exfiltration | Data theft (HR, financial, design files) 17 |
| APT41 Campaign | Taiwanese Semiconductor Companies | July 2025 | China-backed APT41 | Software supply chain compromise (via software update) | IP theft (chip designs, process data) 7 |
| Sensata Technologies Attack | Sensata Technologies (Industrial Tech) | June 2025 | Unspecified, Ransomware | Ransomware, Data Exfiltration | Operational disruption (manufacturing, shipping), data theft 10 |

The Nucor Corporation incident, publicly disclosed in June 2025, involved a cyberattack that led to unauthorized access to the company's IT systems and the exfiltration of "limited" data.15 As a precautionary measure, the North American steel producer proactively halted production operations at multiple facilities, a clear demonstration of the interconnected nature of its IT and OT systems.15 The company’s incident response was swift, taking systems offline, restoring data from backups, and engaging external experts. While Nucor's public statements, including its SEC filing, asserted that the incident caused "no material impact" to its financial conditions 15, this framing overlooks the significant operational disruption and security breach that necessitated a production halt. This pattern of downplaying breach severity in public statements is a common practice that can mask the full extent of a cyberattack's impact on a company's operations and security posture.

A similar trend was observed in the July 2025 Warlock ransomware attack on an India-based manufacturing company. The Warlock group leaked data allegedly stolen from the victim, a review of which suggested the exfiltration of sensitive HR records, financial files, and, critically, internal design software archives and employee data repositories.17 While Warlock is a criminal ransomware group, its focus on stealing valuable IP mirrors the objectives of state-sponsored actors.

This convergence of motives is best exemplified by the China-backed APT41, a group known for conducting both state-sponsored espionage and financially motivated campaigns for its own benefit.18 In July 2025, APT41 infiltrated multiple Taiwanese semiconductor companies via a compromised software update, a classic software supply chain attack.7 The group's method was highly sophisticated, using web shells for persistence and a dropper to load a backdoor, which allowed them to navigate the network and exfiltrate high-value proprietary chip designs and process data.18 The fact that both criminal ransomware groups and state-sponsored actors are focused on the same type of target—a manufacturing company's intellectual property—suggests that the distinction between these groups is becoming increasingly blurred. It is likely that some nation-states are now leveraging criminal groups as proxies to achieve strategic objectives while maintaining plausible deniability, a move that elevates IP theft to a new, geopolitical level.

## **3. Major Threat Actors and Their Evolving Methods**

The manufacturing sector's threat landscape is populated by a dynamic and competitive ecosystem of threat actors, many of whom are professionalizing their operations to maximize profit and evade detection.

| Threat Actor | Type | Associated Aliases | Primary Target Sectors | Noteworthy TTPs | Key Observations |
| --- | --- | --- | --- | --- | --- |
| **Qilin** | RaaS | Agenda ransomware | Professional Services, Construction, Manufacturing, Healthcare 17 | Double extortion, written in Golang and Rust, spear phishing for initial access 17 | Led ransomware activity in July 2025 with 73 victims 17 |
| **INC Ransom** | RaaS | Sinobi (Possible Link) 17 | Critical infrastructure, Manufacturing, Energy, Telecommunications 17 | Double extortion, use of diverse tools (AdFind, PsExec, Rclone), lateral movement 17 | Ranked second in July 2025 with 59 victims 17 |
| **APT41** | State-Sponsored APT (China-backed) | BARIUM, Blackfly, Brass Typhoon, Earth Baku 21 | High-tech manufacturing, healthcare, defense, government 7 | Exploits public-facing vulnerabilities, software supply chain attacks, modular malware, IP theft 7 | Known for dual motivations (espionage & financial gain); TTPs mimic financially motivated gangs 20 |
| **Embargo** | RaaS | Possible rebrand of BlackCat/Alphv 9 | Healthcare, Business Services, Manufacturing 8 | Double extortion, uses Rust programming language, avoids high-visibility tactics 8 | Potential state-linkage due to politically charged messages 8 |
| **Warlock** | RaaS | N/A | Manufacturing | Data exfiltration, HR, financial, and design file theft 17 | Targeted an Indian manufacturing company in July 2025 17 |

The ransomware ecosystem is characterized by a constant flux of new and evolving groups. Qilin led ransomware activity in July 2025 with 73 victims, capitalizing on the decline of rivals like RansomHub.17 Close behind, the INC Ransom group ranked second with 59 victims, with a notable focus on critical infrastructure targets.17 INC Ransom’s operational methods are sophisticated, utilizing a diverse toolkit including off-the-shelf software like PsExec for remote command execution and Rclone for data exfiltration.22 The emergence of new players like D4RK4RMY, which offers a unique RaaS model with a base salary plus a 50% cut of ransom proceeds, further underscores the professionalization and commoditization of cybercrime.17 The constant rebranding of groups, such as the potential link between Sinobi and INC Ransom, makes tracking and attribution a persistent challenge for law enforcement and security teams.17 This evolving business model makes attacks more scalable and difficult to disrupt, as core operators can easily evade accountability by simply changing their name.

The Embargo ransomware group is a prime example of the fluid nature of the threat landscape. Assessed as a potential successor or rebrand of the notorious BlackCat/Alphv group, Embargo has been linked to over $34 million in cryptocurrency transactions since mid-2024, with a primary focus on the manufacturing, healthcare, and business services sectors.9 While technically sophisticated, the group avoids the "overt branding and high-visibility tactics" of groups like LockBit, likely to evade law enforcement scrutiny and media attention.8 This strategic choice reveals a deliberate approach by some actors to operate in the shadows, making them harder to anticipate and gather intelligence on. The fact that some of Embargo’s attacks have featured politically charged messages further blurs the lines, leading some analysts to speculate that the group may be state-aligned despite its clear financial motivations.8

## **4. Attack Vectors and Initial Access Techniques**

Attackers targeting the manufacturing sector use a combination of well-established and increasingly sophisticated methods to gain initial access to a network.

* **Vulnerability Exploitation:** The exploitation of known, but unpatched, software vulnerabilities remains a primary initial access vector.5 The October 2023 Boeing attack was traced to a vulnerability in Citrix software (Citrix Bleed).1 Despite a high severity score (9.4 out of 10) and a CISA-FBI advisory urging immediate patching, thousands of instances remained vulnerable months later.1 This is a systemic problem, particularly in manufacturing, where the difficulty of patching legacy OT systems without disrupting production creates a "patching paradox." The sheer volume of new vulnerabilities, as evidenced by the dozens of advisories released by CISA for major ICS vendors in a single day in August 2025, overwhelms security teams and makes it difficult to keep up.2
* **Credential Theft and Social Engineering:** The human element remains the most common entry point for cyberattacks.5 Phishing emails, which can be highly convincing and appear to come from internal sources or trusted business partners, are a leading cause of network compromise.24 These attacks are often combined with commodity infostealer malware, which harvests credentials that can then be used to access corporate VPNs or OT management interfaces.7 In February 2025, CISA issued an advisory in response to ransomware actors leveraging an unpatched vulnerability in SimpleHelp Remote Monitoring and Management (RMM) software to compromise a utility billing software provider, highlighting the risk of exploiting remote access tools.25
* **Supply Chain Compromise:** Attackers are increasingly targeting the supply chain as a backdoor into a target organization.6 This can take several forms:
  + **Software Supply Chain:** This method involves injecting malicious code or vulnerabilities into legitimate software updates, open-source libraries, or commercial binaries. The July 2025 APT41 attack on Taiwanese semiconductor companies, where a compromised software update served as the initial access vector, is a direct example of this technique.7
  + **Third-Party Vendor Access:** A compromised vendor, such as a managed service provider (MSP) or a logistics partner, can provide a trusted connection into the target's network, allowing attackers to bypass direct defenses. This is a common tactic for ransomware-as-a-service (RaaS) crews.6
  + **Hardware and IoT Devices:** A more advanced, and often state-sponsored, method involves physical tampering with hardware components or exploiting insecure firmware on IoT devices during the manufacturing or distribution process.6

The reliance on legacy systems and the struggle to apply patches without interrupting production create a systemic, widespread vulnerability that cannot be solved with a quick fix. This necessitates a fundamental re-evaluation of security postures to move beyond traditional reactive models.

## **5. Official Advisories and Strategic Guidance**

Federal agencies are actively working to address the escalating cyber risks to critical manufacturing, with a particular focus on the vulnerabilities of ICS.

| Date | # of Advisories | Affected Vendor(s) | Example Products/Vulnerabilities |
| --- | --- | --- | --- |
| August 14, 2025 | 32 | Siemens, Rockwell Automation, Güralp | Siemens: SIMATIC RTLS, SIPROTEC 5; Rockwell: FactoryTalk Viewpoint, ControlLogix Ethernet Modules 2 |
| August 12, 2025 | 7 | Johnson Controls, Schneider Electric, AVEVA | Johnson Controls: iSTAR Ultra (OS Command Injection, Default Credentials); Schneider Electric: EcoStruxure Power Monitoring Expert 3 |

CISA released a staggering volume of Industrial Control Systems (ICS) advisories in August 2025, providing timely information on security issues and exploits affecting ICS environments.2 On August 14, CISA released 32 advisories for products from major vendors like Siemens and Rockwell Automation.2 This was followed by another seven advisories on August 12, which included vulnerabilities in equipment from Johnson Controls and Schneider Electric.3

These advisories highlight the foundational insecurity of the critical infrastructure that powers the manufacturing sector. The vulnerabilities disclosed are often basic, such as the "OS Command Injection" and "Use of Default Credentials" flaws found in Johnson Controls' iSTAR Ultra door controllers.3 These vulnerabilities carry high CVSS scores, with some reaching 8.7, underscoring the severity of the risk.3 The sheer number and nature of these alerts signal that the core infrastructure of the manufacturing sector was not designed with modern security in mind, as many of these systems and protocols lack basic encryption or authentication.11 This systemic problem requires a fundamental shift in design philosophy, moving toward a "Secure-by-Design" approach from the ground up, rather than relying on retroactive patches that can be difficult to implement.

This top-down push is also reflected in the June 6, 2025, Presidential Executive Order charging multiple agencies, including the National Institute of Standards and Technology (NIST), with strengthening the nation's cybersecurity.28 NIST and CISA continue to provide frameworks and guidelines, such as the NIST Cybersecurity Framework and CISA’s Framework for Improving Critical Infrastructure Cybersecurity, to help organizations align their security activities with business requirements and emerging regulatory pressure.28

## **6. Expert Recommendations for Enhanced Cyber Resilience**

Given the sophisticated and persistent threats facing the manufacturing sector, a shift from a traditional, reactive security posture to one focused on cyber resilience is a strategic imperative. This requires a multi-faceted approach that addresses foundational weaknesses, embraces a proactive stance, and leverages advanced technologies.

* **Mitigating Foundational Risks:** The single most critical action for manufacturers is to enforce strict segmentation between IT and OT networks. This architectural separation is essential to prevent attackers from pivoting from a compromised IT network to production-critical OT systems, thereby containing the impact of a breach.7 Simultaneously, organizations must implement a robust vulnerability management program that prioritizes the patching of internet-facing systems, particularly for known, high-severity vulnerabilities.1 Since phishing and social engineering remain a primary initial access vector, regular, mandatory, and effective security awareness training for all employees is non-negotiable.5
* **Adopting a Proactive Stance:** A resilient security posture operates on the principle of "never trust, always verify".31 This zero-trust architecture should be applied to all users, devices, and connections, especially for third-party access, to minimize the damage of a compromised account.6 Organizations should also invest in continuous attack surface monitoring and threat intelligence to identify exposed assets, leaked credentials, and vulnerable vendor ecosystems before attackers can exploit them.7
* **Leveraging Emerging Technologies:** As attackers use AI and machine learning to craft more adaptive attacks, security teams must do the same.30 AI-driven security platforms offer crucial insights and can improve the detection of subtle threat patterns that traditional security systems may miss, particularly in complex OT environments.33 By establishing behavioral baselines and analyzing real-time telemetry, AI can transition a security program from reactive incident response to predictive resilience. This requires organizations to move beyond the question of "how can we prevent an attack?" and instead ask "how fast can we detect and recover from an attack?"
* **Addressing the Cybersecurity ROI Challenge:** A major challenge for security leaders is justifying investments in a landscape where skilled talent is scarce and the cost of securing a massive legacy footprint is high.10 To secure executive buy-in, security leaders should adopt cyber risk quantification models. These tools provide concrete, data-driven metrics that demonstrate the direct financial impact of a cyberattack on operational continuity and the return on investment (ROI) of a security initiative.33 This allows the conversation to shift from abstract technical risk to a concrete business-risk management exercise, which is essential for securing the necessary budget and support for modernizing industrial security.

#### Works cited

1. 20 Recent Cyber Attacks & What They Tell Us About the Future of Cybersecurity, accessed August 14, 2025, <https://secureframe.com/blog/recent-cyber-attacks>
2. CISA Releases Thirty-Two Industrial Control Systems Advisories ..., accessed August 14, 2025, <https://www.cisa.gov/news-events/alerts/2025/08/14/cisa-releases-thirty-two-industrial-control-systems-advisories>
3. CISA Releases Seven Industrial Control Systems Advisories | CISA, accessed August 14, 2025, <https://www.cisa.gov/news-events/alerts/2025/08/12/cisa-releases-seven-industrial-control-systems-advisories>
4. ICS systems face elevated cyber risk as CISA issues advisories covering multiple vendor vulnerabilities, accessed August 14, 2025, <https://industrialcyber.co/cisa/ics-systems-face-elevated-cyber-risk-as-cisa-issues-advisories-covering-multiple-vendor-vulnerabilities/>
5. What are Ransomware Attacks? - Palo Alto Networks, accessed August 14, 2025, <https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods>
6. 2025 Supply Chain Threat Landscape: AI, APIs, and the Weakest Link - SecureWorld, accessed August 14, 2025, <https://www.secureworld.io/industry-news/2025-supply-chain-threats-ai-api>
7. Chip Makers See A 6X Surge in Cyberattacks and $1B in Ransomware Losses, accessed August 14, 2025, <https://www.ien.com/artificial-intelligence/news/22947866/sixfold-surge-in-cyberattacks-and-1b-in-ransomware-losses-are-reshaping-the-global-semiconductor-industry>
8. Unmasking Embargo Ransomware: A Deep Dive Into the Group's TTPs and BlackCat Links, accessed August 14, 2025, <https://www.trmlabs.com/resources/blog/unmasking-embargo-ransomware-a-deep-dive-into-the-groups-ttps-and-blackcat-links>
9. Embargo Ransomware Group Tied to $34M in Ransom Profits - Bank Info Security, accessed August 14, 2025, <https://www.bankinfosecurity.com/embargo-ransomware-group-tied-to-34m-in-ransom-profits-a-29217>
10. Major Cyber Attacks Targeting Manufacturing Industry in 2025 ..., accessed August 14, 2025, <https://socradar.io/major-cyber-attacks-manufacturing-industry-in-2025/>
11. How Cyber Risk Is Reshaping Manufacturing in 2025, accessed August 14, 2025, <https://manufacturing-today.com/news/how-cyber-risk-is-reshaping-manufacturing-in-2025/>
12. Top Cybersecurity Breaches in Manufacturing and What You Can Learn From Them, accessed August 14, 2025, <https://armorpoint.com/2025/07/24/top-cybersecurity-breaches-in-manufacturing-and-what-you-can-learn-from-them/>
13. Supply Chains Are Complex, Opaque and Insecure: Regulators Are Demanding Better, accessed August 14, 2025, <https://www.isms.online/cyber-security/supply-chains-are-complex-opaque-and-insecure-regulators-are-demanding-better/>
14. Industrial espionage - Wikipedia, accessed August 14, 2025, <https://en.wikipedia.org/wiki/Industrial_espionage>
15. Steel Giant Nucor Hacked: Attackers Breach IT Systems - Cyber Press, accessed August 14, 2025, <https://cyberpress.org/steel-giant-nucor-hacked/>
16. Nucor data pilfered in May cyberattack - SC Media, accessed August 14, 2025, <https://www.scworld.com/brief/nucor-data-pilfered-in-may-cyberattack>
17. Cyble reveals US primary target with 223 ransomware victims amid ..., accessed August 14, 2025, <https://industrialcyber.co/critical-infrastructure/cyble-reveals-us-primary-target-with-223-ransomware-victims-amid-rising-attacks-on-critical-infrastructure/>
18. APT41 Has Arisen From the DUST | Google Cloud Blog, accessed August 14, 2025, <https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>
19. Global Data Breaches and Cyber Attacks in June 2025: Over 16 ..., accessed August 14, 2025, <https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-june-2025-over-16-billion-records-exposed>
20. apt41.pdf - HHS.gov, accessed August 14, 2025, <https://www.hhs.gov/sites/default/files/apt41.pdf>
21. APT PROFILE – MISSION2025 - CYFIRMA, accessed August 14, 2025, <https://www.cyfirma.com/research/apt-profile-mission2025/>
22. INC Ransom: A Sophisticated Ransomware & Data Extortion Group - Cyble, accessed August 14, 2025, <https://cyble.com/threat-actor-profiles/inc-ransom/>
23. Embargo ransomware gang has handled at least $34 million in about a year, report says, accessed August 14, 2025, <https://therecord.media/embargo-ransomware-gang-blackcat-alphv-successor>
24. Top 7 Cyber Attacks Threatening Manufacturing Companies - BitLyft, accessed August 14, 2025, <https://www.bitlyft.com/resources/cyber-attacks-threatening-manufacturing-companies>
25. Official Alerts & Statements - CISA, accessed August 14, 2025, <https://www.cisa.gov/stopransomware/official-alerts-statements-cisa>
26. Supply chain attack - Wikipedia, accessed August 14, 2025, <https://en.wikipedia.org/wiki/Supply_chain_attack>
27. Johnson Controls iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, iSTAR Edge G2 | CISA, accessed August 14, 2025, <https://www.cisa.gov/news-events/ics-advisories/icsa-25-224-02>
28. Cybersecurity | NIST, accessed August 14, 2025, <https://www.nist.gov/cybersecurity>
29. Framework for Improving Critical Infrastructure Cybersecurity - CISA, accessed August 14, 2025, <https://www.cisa.gov/resources-tools/resources/framework-improving-critical-infrastructure-cybersecurity>
30. Top Cyber Threats in Manufacturing | MxD, accessed August 14, 2025, <https://www.mxdusa.org/2025/02/13/top-cyber-threats-in-manufacturing/>
31. 5 Best Practices for Operational Technology (OT) Security - Fortinet, accessed August 14, 2025, <https://www.fortinet.com/resources/cyberglossary/ot-security-best-practices>
32. Cost of a Data Breach Report 2025 - IBM, accessed August 14, 2025, <https://www.ibm.com/reports/data-breach>
33. Industrial Cybersecurity Market Outlook 2025: Focus on quantifying risk, embracing AI, building operational resilience, accessed August 14, 2025, <https://industrialcyber.co/features/industrial-cybersecurity-market-outlook-2025-focus-on-quantifying-risk-embracing-ai-building-operational-resilience/>