



THE INDUSTRIAL HEARTLAND UNDER SIEGE

A Comprehensive Analysis of Cybersecurity Volatility
and Emerging Threats in Wisconsin and
Midwest Manufacturing

prepared by
CENTURION DATA SYSTEMS
2026

INTRODUCTION

The Digital Siege on Midwest Manufacturing

The manufacturing sector across Wisconsin and the broader Midwest stands at a critical inflection point. As Industry 4.0 technologies reshape production floors from Milwaukee to Minneapolis, the convergence of information technology and operational technology systems has created an unprecedented attack surface that threat actors are exploiting with increasing sophistication.

\$52B+

Annual Manufacturing
Output

9,000+

Manufacturing
Establishments

~500K

Manufacturing
Workers

Wisconsin alone contributes over \$52 billion annually to the national manufacturing output, with more than 9,000 manufacturing establishments employing nearly half a million workers. The state's manufacturing ecosystem encompasses everything from heavy machinery and automotive components to food processing and medical devices.

The integration of smart sensors, cloud-based SCADA systems, and AI-driven quality control has dramatically improved efficiency but has simultaneously exposed critical infrastructure to cyber threats that were previously confined to the IT domain. Legacy programmable logic controllers now share network segments with enterprise resource planning systems, creating lateral movement opportunities.

This report examines the cybersecurity landscape through the lens of three converging threat vectors: sophisticated ransomware syndicates, state-sponsored actors targeting industrial control systems, and the emergence of agentic AI-driven attacks that operate at machine speed.

The Geopolitical Frontline: Targeting the Industrial Core

The cybersecurity threat landscape for Midwest manufacturers has been fundamentally altered by the intensification of state-sponsored cyber operations. Nation-state actors, particularly those affiliated with Iran, China, and Russia, have shifted their targeting from traditional espionage objectives to direct operational disruption of industrial systems.

Critical Finding: Iranian-affiliated actors exploited CVE-2021-22681 in Rockwell Automation PLCs, enabling unauthorized access to programmable logic controllers used across Wisconsin manufacturing facilities.

STATE-SPONSORED CYBER INCIDENTS AFFECTING MIDWEST MANUFACTURING

Threat Actor	Target Sector	Mechanism	Impact
CyberAv3ngers (Iran)	Water/Mfg PLCs	CVE-2021-22681 Rockwell Automation	Unauthorized PLC access
Handala (Iran-linked)	Medical Devices	Data wipe attack on Stryker systems	Complete data destruction
Volt Typhoon (China)	Critical Infrastructure	Living-off-the-land techniques	Persistent access for disruption
Sandworm (Russia)	Energy/Mfg Systems	Supply chain compromise	Operational disruption

The **CISA advisory AA23-335A** specifically warned that Iranian actors had developed custom tools capable of scanning for and exploiting vulnerable Rockwell Automation ControlLogix and GuardLogix PLCs. These controllers are ubiquitous in Wisconsin's manufacturing sector, controlling everything from assembly line robotics to chemical processing systems.

CASE STUDY

The Stryker Data Wipe Strike

The attack on Stryker Corporation, headquartered in Kalamazoo, Michigan, represents one of the most significant cyber incidents affecting the Midwest medical device manufacturing sector. The "Handala" group, an Iranian-linked threat actor, claimed responsibility for a devastating data wipe attack that targeted Stryker's operational systems.

IMPACT ASSESSMENT

- Complete destruction of targeted data repositories
- Operational disruption across manufacturing lines
- Supply chain delays affecting hospital equipment delivery
- Estimated recovery timeline: several weeks
- Geopolitical motivation linked to Middle East tensions

Unlike traditional ransomware attacks that encrypt data for extortion, the Stryker incident was a pure destruction operation. The attackers deployed wiper malware designed to permanently destroy data rather than hold it for ransom, indicating a shift in threat actor objectives from financial gain to operational disruption and geopolitical signaling.

Key Takeaway: The Stryker attack demonstrates that Midwest manufacturers face not only financially motivated cybercriminals but also state-sponsored actors pursuing destructive objectives. Traditional backup and recovery strategies are insufficient against wiper attacks.

The incident underscores the need for manufacturers to implement immutable backup solutions, network segmentation between IT and OT environments, and enhanced monitoring for destructive malware signatures. The medical device sector is particularly vulnerable given the life-safety implications of production disruptions.

The Evolution of Ransomware: Extortion and Disruption

The ransomware threat facing Midwest manufacturers has evolved dramatically. What began as opportunistic encryption attacks has transformed into sophisticated, multi-stage extortion campaigns specifically targeting the manufacturing sector's low tolerance for downtime.

SNAP-ON INC.

Kenosha, WI

The 0apt group targeted Snap-on's systems, exfiltrating proprietary tool designs and employee data before deploying encryption.

INOTIV

West Lafayette, IN

Qilin ransomware operators breached Inotiv's research systems, threatening to release sensitive pharmaceutical research data.

THUNDER MTN HARLEY-DAVIDSON

Loveland, CO

Genesis ransomware disrupted dealership operations, compromising customer financial data and service records.

RANSOMWARE STATISTICS: YEAR-OVER-YEAR COMPARISON

Metric	2024	2025	2026 (Proj.)
Mfg. Attacks (Global)	1,424	2,100+	~2,800
Avg. Ransom Demand	\$1.2M	\$2.1M	\$3.5M
Avg. Downtime (Days)	21	18	14
Data Exfiltration Rate	68%	82%	91%
Midwest Share of US	14%	18%	22%

Warning: The Midwest's share of US manufacturing ransomware attacks is growing disproportionately, rising from 14% in 2024 to a projected 22% in 2026. This reflects targeted campaigns against the region's concentrated industrial base.

Manufacturing consistently ranks as the most-attacked sector globally, accounting for over 25% of all ransomware incidents. The sector's reliance on just-in-time production and interconnected supply chains makes downtime extraordinarily costly, creating strong incentives for ransom payment.

SECTION 03

Emerging Threats: The Era of Agentic AI and Machine-Speed Attacks

The most transformative development in the 2025-2026 threat landscape is the emergence of agentic AI systems capable of conducting autonomous cyber operations. These AI-driven attacks represent a paradigm shift from human-directed campaigns to machine-speed operations that can identify, exploit, and pivot through networks faster than human defenders can respond.

"Vibe-Coded" Phishing: AI systems now generate hyper-personalized phishing campaigns by scraping LinkedIn profiles, company websites, and industry publications. These attacks achieve click-through rates 3x higher than traditional phishing, with grammatically perfect, contextually relevant lures.

ATTACK TIMELINE: HUMAN VS. AI-DRIVEN OPERATIONS

Attack Phase	Human-Led	AI-Driven
Initial Reconnaissance	2-4 weeks	15-30 minutes
Credential Harvesting	3-7 days	2-4 hours
Lateral Movement	1-2 weeks	30-90 minutes
Data Exfiltration	2-5 days	1-3 hours
Ransomware Deployment	Hours to days	Minutes
Full Kill Chain	4-8 weeks	< 24 hours

Key Insight: AI-driven attacks compress the traditional kill chain from weeks to hours. This speed advantage means that conventional incident response playbooks, designed for human-speed attacks, are fundamentally inadequate for the emerging threat landscape.

Identity systems have become the primary attack vector for AI-driven campaigns. Agentic AI can systematically test stolen credentials across multiple platforms, generate convincing deepfake audio for vishing attacks, and create synthetic identities that bypass traditional verification processes.

Supply Chain Volatility: The Crisis in Logistics

The convergence of physical cargo theft and digital attack vectors has created a new category of supply chain risk for Midwest manufacturers. In 2025, cyber-enabled cargo theft contributed to an estimated **\$6.6 billion in losses nationally**, with the Midwest's dense logistics networks proving particularly vulnerable.

\$6.6 Billion in cargo theft losses in 2025 – cybersecurity is now a logistics issue. Digital attacks on load boards, carrier systems, and 3PLs are accelerating physical theft.

KEY ATTACKER TECHNIQUES

- **"Signing-as-a-Service"** – Re-signing malicious tools with trusted certificates to bypass endpoint detection
- **RMM Redundancy** – Installing multiple remote monitoring and management tools to maintain persistent access
- **Financial Reconnaissance** – Searching compromised networks for cryptocurrency wallets, fuel cards, and financial access
- **Load Board Compromise** – Infiltrating digital freight platforms to redirect shipments and create fraudulent carrier identities

Key Insight: Major Midwest manufacturers like Oshkosh Corporation and Harley-Davidson face elevated risk through reliance on third-party logistics providers (3PLs) whose cybersecurity postures may not match enterprise standards.

Corporate Innovation and the Dual Edge of AI

While AI presents significant threats, Oshkosh Corporation demonstrates how the same technology can be harnessed for safety, efficiency, and competitive advantage. The company's AI initiatives earned multiple CES 2025 Innovation Awards, showcasing the positive potential of machine learning in manufacturing.

AWARD-WINNING AI INNOVATIONS

COLLISION AVOIDANCE MITIGATION SYSTEM (CAMS)

Integrates radar sensors with AI algorithms for real-time hazard detection on aerial work platforms. Automatically adjusts boom operations to prevent collisions, protecting workers at height.

HARR-E AUTONOMOUS REFUSE ROBOT

An AI-powered autonomous robot that retrieves and returns residential waste carts. Uses machine learning and mobile app integration to reduce physical strain on collection workers.

AI-POWERED CONTAMINATION DETECTION

Camera-based AI systems monitor recycling streams in real time, identifying contaminants and improving sorting accuracy. Enhances sustainability outcomes while reducing manual inspection costs.

Key Takeaway: Oshkosh Corporation's AI investments demonstrate that the same technologies weaponized by threat actors can be redirected toward safety, sustainability, and operational excellence when deployed with proper governance.

These innovations highlight the dual nature of AI in manufacturing: the same capabilities that enable autonomous cyber operations can also drive unprecedented improvements in worker safety and environmental performance.

SECTION 06

Wisconsin's Regulatory Response and Data Breach Landscape

Wisconsin's DATCP has documented a steady rise in identity theft and data breach complaints. The state's breach notification law (Wis. Stat. § 134.98) requires entities to notify affected residents, but proposed legislation SB166 would significantly expand consumer protections.

NOTABLE DATA BREACH INCIDENTS

Company	Date	Residents	Data Accessed
700Credit	Mar 2025	4,028	SSN, financial data, credit reports
TransUnion	Jan 2025	3,812	Credit scores, personal identifiers
5CA (Discord)	Feb 2025	2,100	Email, usernames, IP addresses
Melzer's Fuel	Dec 2024	1,450	Payment cards, driver info
Univ. of Phoenix	Nov 2024	890	Student records, financial aid data
Mercor	Apr 2025	2,340	Employment data, background checks

Senate Bill 166 (SB166) – Proposed Privacy Law

- Applies to entities controlling data of 50,000+ consumers
- Grants consumer rights: access, deletion, correction, portability
- Requires data protection assessments for high-risk processing
- Penalties up to \$7,500 per intentional violation

Key Insight: Wisconsin manufacturers should begin preparing for SB166 compliance now, as the legislation mirrors comprehensive privacy frameworks already enacted in neighboring states and is expected to pass in the current legislative session.

The growing volume of breaches affecting Wisconsin residents underscores the urgency of both stronger regulatory frameworks and proactive corporate data governance strategies.

SECTION 07

The Financial Reality: Insurance, Licensing, and Rising IT Costs

The financial landscape of cybersecurity in Midwest manufacturing is shifting dramatically. Cyber insurance premiums continue to rise while underwriters demand increasingly rigorous security controls as prerequisites for coverage. IT spending is accelerating as manufacturers recognize that legacy infrastructure creates unacceptable risk.

2026 CYBER INSURANCE UNDERWRITER REQUIREMENTS

Control Category	2026 Expectation	Why It Matters
MFA Enforcement	Phishing-resistant MFA on all admin and remote access	Credential theft is #1 initial access vector
EDR Deployment	100% endpoint coverage with 24/7 managed detection	Reduces dwell time from weeks to hours
Backup Restore Tests	Quarterly tested, air-gapped, immutable backups	Validates recovery capability before incidents
Patching Cadence	Critical patches within 72 hours, routine within 30 days	Unpatched vulnerabilities enable 60% of breaches

Warning: Underwriters are increasingly conducting technical audits before issuing policies. Manufacturers that cannot demonstrate compliance with these baseline controls face premium increases of 30-50% or outright coverage denial.

Managed Service Providers (MSPs) are shifting from break-fix models to proactive, managed security agreements. This transition reflects the reality that cybersecurity is no longer an IT cost center but a business continuity imperative requiring continuous investment and expertise.

SECTION 08

Operational Resilience: A Roadmap for Midwest Manufacturers

Building resilience against the evolving threat landscape requires a structured, multi-layered approach. The following four strategic pillars provide a practical framework for Midwest manufacturers to strengthen their cybersecurity posture.

01 HARDENING THE IDENTITY PERIMETER

- Deploy phishing-resistant MFA on all privileged accounts
- Implement Just-in-Time (JIT) access provisioning
- Enforce session hardening and continuous authentication
- Monitor for credential stuffing and token theft

02 OT ISOLATION AND SECURITY

- Disconnect PLCs from corporate networks where possible
- Scan for known ICS vulnerabilities (e.g., CVE-2021-22681)
- Inventory all machine identities and certificates
- Implement network segmentation with monitoring

03 AUTONOMOUS DEFENSE AND CONTAINMENT

- Deploy AI-driven EDR/NDR with automated response
- Implement behavioral email security systems
- Monitor AI model telemetry for adversarial inputs
- Establish machine-speed incident response playbooks

04 SUPPLY CHAIN AND 3RD PARTY RISK

- Conduct cybersecurity audits of all carrier partners
- Require Software Bills of Materials (SBOMs)
- Implement continuous monitoring of 3PL security posture
- Establish contractual security requirements

Key Takeaway: These four pillars work together as an integrated defense strategy. Implementing them in isolation reduces their effectiveness – manufacturers should pursue all four simultaneously, prioritizing based on their current risk exposure.

Organizations that adopt this roadmap position themselves not just to survive the current threat landscape, but to build lasting competitive advantage through superior operational resilience.

CONCLUSION

The Future of Industrial Security in the Midwest

The cybersecurity landscape facing Wisconsin and Midwest manufacturers has fundamentally shifted. The convergence of state-sponsored industrial espionage, AI-accelerated ransomware, and supply chain digitization has created a threat environment that demands equally sophisticated defensive responses.

The era of periodic security assessments and reactive incident response is over. Manufacturers must embrace continuous, automated defense strategies that operate at machine speed to match the capabilities of modern threat actors. Identity-centric security, OT isolation, and AI-driven detection are no longer aspirational goals but operational necessities.

The path forward requires innovation, investment, and collaboration. Organizations that build resilience now will not only survive the current threat landscape but emerge as leaders in the next generation of secure, intelligent manufacturing.

SOURCES

- [1] CISA ICS Advisory ICSA-22-090-05
- [2] Dragos OT Cybersecurity Report 2025
- [3] Rockwell Automation Security Advisory
- [4] FBI Flash Alert: Iranian Cyber Actors
- [5] Mandiant APT Research Report
- [6] Stryker Corporation SEC Filing
- [7] CISA Alert AA24-290A
- [8] Snap-on Inc. Data Breach Notice
- [9] Inotiv Qilin Ransomware Disclosure
- [10] Sophos State of Ransomware 2025
- [11] Verizon DBIR 2025
- [12] IBM Cost of a Data Breach 2025
- [13] Gartner AI Security Forecast
- [14] SentinelOne Agentic AI Report
- [15] CargoNet Annual Report 2025
- [16] FreightWaves Cyber Theft Analysis
- [17] Oshkosh Corp. CES 2025 Awards
- [18] WI DATCP Consumer Protection
- [19] Wis. Stat. § 134.98
- [20] WI Senate Bill 166 (SB166)
- [21] 700Credit Breach Notification
- [22] TransUnion Incident Report
- [23] Marsh Cyber Insurance Report 2025
- [24] Deloitte Manufacturing IT Survey
- [25] NIST Cybersecurity Framework 2.0
- [26] ISA/IEC 62443 Standards
- [27] WI Manufacturers & Commerce