NETWITNESS

REPORT

Top Threats and Trends in Industrial Network Security

REPORT

Executive Summary

Industrial network security has crossed a threshold. What used to be a niche concern handled by a handful of OT engineers is now boardroom material, government priority, and frontpage news. The attacks are more targeted, the attackers are more patient, and the consequences more physical than anything the cybersecurity world dealt with a decade ago. Here's what's happening and why it matters.

What stands out is how threats have evolved. Ransomware now focuses on halting operations, not just encrypting files. At the same time, nation-state actors are taking a slower, more strategic approach, quietly mapping critical infrastructure for future use. These attacks are harder to detect and often remain unnoticed for long periods.

The risk is amplified by persistent weaknesses inside industrial environments. Legacy systems, flat networks, insecure remote access, and third-party connections continue to create easy entry points. Many of these gaps are known but remain unresolved due to operational constraints.

The takeaway is simple. The challenge is no longer about awareness or technology. It is about execution. Organizations that fail to secure their industrial environments proactively will face increasing operational, financial, and regulatory consequences as the threat landscape continues to intensify.

Table of Contents

Notable Cyber Attacks to Consider

The attacks of early 2026 made one thing clear: industrial and operational environments are no longer collateral damage in cyber incidents. They're the target.

Company	Sector	What Happened	Key Risk Exposed
AkzoNobel	Manufacturing	Ransomware hit a U.S. manufacturing site; large volumes of internal data stolen and leaked online	Plant-level networks treated as low-priority targets
Mazda Motor Corporation	Automotive / Industrial	Attackers exploited a vulnerable warehouse management system to access employee and partner data	Operational systems left unpatched and outside security scope
Michelin	Industrial / Manufacturing	Over 300GB of company files stolen via the Oracle EBS hacking campaign	Third-party platform vulnerabilities cascading into OT-adjacent environments
Stryker Corporation	Medtech / Manufacturing	Wiper malware knocked manufacturing and order processing offline; company forced into manual operations	IT breach with direct operational consequences no malware needed to cause damage
Cognizant TriZetto	Healthcare IT / Operations	3.4 million patient records exfiltrated after unauthorized access to operational systems	Interconnected operational platforms creating wide blast radius from a single breach

Taken together, these incidents aren't outliers. They're the pattern. Attackers don't need to find the most sophisticated path into your environment. They need to find the one system that nobody thought was important enough to protect.

Key Industrial Network Threats

Industrial threats don't show up randomly. They follow patterns, exploit the same gaps, and repeat across environments. Once you step back, the common threads become clear.

Here's where the real risk is coming from:

The Ransomware Problem Has Evolved

Manufacturing has been the top ransomware target for four consecutive years. In 2024 alone, attacks against industrial organizations spiked **87%** year over year. That number alone should stop people in their tracks. But the more alarming development isn't the volume, it's the direction.

Early ransomware is straightforward: encrypt files, demand payment, collect or move on. The new generation of ransomware is OTaware. Attackers aren't just locking down IT systems anymore. They're directly manipulating industrial processes in the systems that move physical things in the real world, from manufacturing lines to water treatment controls. The encryption of data is almost secondary now. The real leverage is operational disruption.

How do they get there? Mostly through two avenues that have existed as vulnerabilities for years: vulnerable remote access points and flat networks. When OT and IT networks aren't properly segmented, a foothold anywhere becomes a pathway everywhere. Ransomware groups know this and move laterally through these environments with increasing confidence. The lesson here isn't complicated, but it's still being ignored at scale flat networks in industrial environments aren't just a configuration problem; they're an existential risk.

State Sponsored Actors Are Playing a Long Game

The ransomware threat is visible and loud. The state sponsored threat is quiet, methodical, and arguably more dangerous.

Threat actors linked to nation-state programs the most prominent example being VOLTZITE, tied to China's Volt Typhoon spent 2025 doing something that doesn't look like an attack at first glance. They were infiltrating critical infrastructure through small office routers at electric utilities. They were pulling GIS data, OT network diagrams, and operational instructions. Not destroying anything. Not tripping alarms. Just learning.

This is a preposition. The goal isn't disruption today, it's capability tomorrow. Security experts who've tracked these campaigns are clear about where these leads: when geopolitical tensions escalate to crisis level, that accumulated knowledge gets weaponized. The infrastructure maps they've stolen become targeting packages. The access they've quietly maintained becomes the onramp for destructive operations.

What makes this so difficult to counter is the patience involved. These campaigns operate on timelines that don't align with typical threat detection cycles. An organization might see nothing suspicious for months, even years, while an adversary is quietly building a map of everything that matters.

ICS Specific Malware Is Getting Smarter

For a long time, ICS specific malware was rare. Stuxnet was the anomaly everyone referenced but assumed it was one off. That assumption is no longer reasonable.

In 2024, attackers expanded the use of specialized malware like Fuxnet and Frosty Goop tools built specifically to interact with industrial control systems in ways that generic malware cannot. These aren't repurposed IT tools with new packaging. They're purpose built for OT environments, designed to understand and manipulate the protocols and hardware that run industrial operations.

Alongside this, the living off the land technique has taken root in industrial environments. Rather than deploying recognizable malware, attackers use the legitimate built-in tools that already exist within the environment. In hybrid IT/OT settings, this makes detection genuinely difficult. The malicious activity looks like normal operations because it's using the same tools normal operations use. Traditional signature-based detection doesn't catch it. You need behavioral analytics and deep environment knowledge to spot the anomalies, and most industrial organizations aren't there yet.

Too Many Industrial Assets Are Still Directly Exposed

Here's something that's hard to explain given how long the security community has been warning about it: **40%** of organizations still have OT devices with known, actively exploited vulnerabilities connected to the internet. Not obscure vulnerabilities. Actively exploited ones.

It gets worse. **65%** OT environments have insecure remote access conditions. **45%** have SSH communicated with publicly routable addresses. These aren't sophisticated attack vectors. They're open doors. The reasons this persists are real, but they no longer justify the risk.

Operational technology environments often run legacy systems that can't be patched without taking production offline. The people managing these systems are engineers, not security professionals. Downtime is expensive, and the business pressure to keep things running frequently wins. But the calculus is shifting. The cost of a successful attack, including regulatory penalties, remediation, and operational disruption, now regularly exceeds the cost of the downtime required to fix these issues. That argument is finally starting to land in budget conversations.
can you recheck this, they do not connect

Supply Chains are a Structural Vulnerability

The third-party problem in industrial security is significant and underappreciated. **46%** of organizations experienced breaches due to third-party access in the past 12 months. More revealing: **54%** discovered security gaps in vendor contracts only after incidents occurred. The risk was always there. They just didn't look until something went wrong.

Vendor access to OT environments is operationally necessary. Maintenance contracts, remote diagnostics, software updates these require access. But every vendor connection is an attack surface extension, and most organizations don't monitor or control that surface with anywhere near the rigor they apply to their own employees.

Geopolitical dynamics are adding another layer. **67%** of organizations are rethinking supply chain geography in response to international tensions. That's the right instinct strategically, but every transition creates a window of vulnerability new vendors, new integrations, new access points that haven't been fully assessed yet. The period of supply chain restructuring is itself a risk period.

Defense priorities for 2026

Complete asset inventory

You cannot defend what you don't know exists. Every untracked device is a potential open door and attackers find them faster than most teams do.

Aggressive network segmentation

Flat networks turn a single breach into a full takeover. Protocol-aware firewalls and micro segmentation keep attackers contained even after they get in.

OT-specific monitoring

IT security tools are blind to industrial protocols. Anomalies in Modbus or DNP3 traffic look like normal noise unless your detection platform actually speaks those languages.

Multi-factor authentication

Remote access especially from vendors is one of the most exploited entry points in industrial environments. A single stolen credential should never be enough.

Offline backups

When ransomware hits, recovery depends on what survives it. Engineering workstation software and controller configurations need offline copies that attackers simply cannot reach.

Build security maturity

Tools without discipline don't hold. Organizations that invest in structured programs governance, processes, trained people consistently outperform those that rely on technology alone.

The Trends Shaping What Comes Next

The threat landscape above describes where things are. The trends below describe where they're heading.

AI powered attacks are compressing the timeline

Threat actors are using AI for automated reconnaissance, polymorphic malware that adapts to evade detection, and deepfake social engineering that's increasingly difficult to distinguish from legitimate communication. The practical effect is that the window between initial compromise and significant damage is shrinking. Defenders who rely on human speed detection and response are going to fall behind. AI on the defensive side isn't optional anymore; it's the only way to match the operational tempo of AI assisted attacks.

Zero trust micro segmentation is becoming the practical standard

The old model of perimeter defense builds a strong wall and trust everything inside has been functionally dead for years in IT. Industrial networks are now catching up. Organizations are moving toward dynamic, software defined boundaries around critical assets. This matters especially for the legacy OT security devices that can't be patched. If you can't fix the vulnerability, you isolate the asset so thoroughly that exploiting it becomes impractical. It's not a perfect solution, but it's a realistic one.

IT/OT convergence is both a risk and an opportunity

As these networks integrate, the attack surface expands. Attackers who gain a foothold in IT now have potential pathways into OT. But the convergence also enables unified security solutions, and organizations that have implemented them effectively are seeing substantial results a **93%** reduction in cyber incidents in some cases. The trend is inevitable. The question is whether organizations manage the integration deliberately or let it happen by default.

Hybrid security architectures are replacing all cloud approaches

Pure cloud-based security monitoring creates a single point of failure for environments that cannot afford operational disruption. The emerging model combines centralized cloud visibility with decentralized onsite protection, so that even during connectivity loss, the local environment maintains integrity. For industrial operations that run 24/7, this isn't an architectural preference; it's a practical requirement.

Hacktivists and cybercriminals are coordinating

Groups like ELECTRUM and GRAPHITE are now sharing intelligence and infrastructure with hacktivist personas. The tactical use of this is clever: hacktivist activity creates noise and draws attention, while the sophisticated actors conduct their actual operations under cover of the distraction. Defenders who take hacktivist incidents at face value as politically motivated nuisances rather than potential cover operations are missing a layer of what's happening.

What This All Adds Up To »

Industrial network security in 2025 and beyond is not a technical problem with a technical solution waiting to be found. The solutions largely exist. The challenge is organizational building the governance structures, budget commitments, and cross functional coordination between IT and OT teams that actually implement them.

The threat actors are disciplined, patient, and increasingly sophisticated. The infrastructure they're targeting is critical in the literal sense, disrupting it has real-world physical consequences. And the window for organizations to get ahead of this, rather than simply responding to it, is narrowing. The time for treating OT security as a secondary concern to IT security is over.

Contact Information

Email for customer Service
support@netwitness.com

Website
www.netwitness.com

Follow us for regular updates