# Manufacturing Under Attack:

## The Software Supply Chain Risk Report

Ransomware, open-source vulnerabilities, and unvetted AI models are exploiting gaps that physical security can't close. Here's what the data says, and what DevOps and AppSec teams are up against.

### Key Trends & Statistics

**27.7%**
of cyberattacks in 2025 targeted manufacturing

**$260K**
average unplanned downtime cost per hour

**61%**
YoY ransomware surge, 520 → 838 incidents in 2025

**30%**
of all breaches involve third-party software providers

# Top 5 R!sks

### DevOps & AppSec in Manufacturing

The convergence of IT and OT has fundamentally changed the manufacturing attack surface. PLCs, SCADA systems, and industrial controllers now run software built with the same open-source pipelines as any enterprise application, and inherit all the same vulnerabilities. Here are the five challenges creating the most exposure.

**01 CHALLENGE**

### Your Last Release Could Have a Backdoor in It

Growth through acquisition means fragmented artifact stores, no shared security baseline, and SBOMs that take days to assemble manually, if they're assembled at all.

⚠ The real risk: Build drift between dev and production means what you scanned is often not what shipped to the factory floor.

21% of manufacturers have reached OT security maturity level 4; more than 70% are stuck in the middle levels. (Fortinet)

**Regulated by:**

[ SBOM compliance ]: Required for federal contracts
[ IEC 62443 ]: OT/ICS cybersecurity standard
[ EO 14028 ]: US federal software supply chain mandate
[ EU CRA ]: SBOM & vulnerability handling mandate for EU digital products

**02 CHALLENGE**

### Alert Fatigue Is a Vulnerability

A single embedded firmware build can surface thousands of CVE findings. Without context on reachability, teams either chase false alarms or stop triaging entirely.

⚠ The real risk: A vulnerability that misses a firmware release window may not be remediated until the next major cycle, already deployed to thousands of connected OT devices.

90% of manufacturing financial losses from cyber incidents are driven by ransomware, yet ransomware represents only 12% of claims. Alert fatigue delays the response. (Resilience)

**Frameworks & Controls:**

[ NIST SP 800-82 ]: OT/ICS security controls, often unmet in legacy environments
[ CVE Triage ]: Unpatched vulnerabilities drove 13% of manufacturing cyber losses

**03 CHALLENGE**

### Your Codebase Trusts Strangers

Engineering teams consume Maven, npm, PyPI, Docker Hub, and Conan packages at scale. Typosquatting, dependency confusion, and malicious install scripts are active and increasing.

⚠ The real risk: A compromised package in a PLC firmware build isn't a data breach, it's a backdoor with direct access to operational technology systems.

2x the supply chain attacks against manufacturing in 2025, from 154 to 297 incidents. (Check Point Research)

**Exposure Areas:**

[ ICS/SCADA risk ]: A poisoned package can reach the factory floor
[ OSS governance ]: Most manufacturers don't vet open source at ingest

**04 CHALLENGE**

### Signed at Build. Unverified at the Edge

Pushing firmware updates to remote facilities and air-gapped OT networks without cryptographic verification leaves no way to confirm that what arrived matches what was sent.

⚠ The real risk: A sensor deployed in 2019 may still operate in 2031, accumulating unpatched CVEs, while teams fear the operational disruption of pushing an update.

76% of organizations needed more than 100 days to fully recover from a cyber attack. (IBM Cost of a Data Breach Report)

**Verification Gaps:**

[ OT networks ]: Signed builds, unsigned deployment paths
[ Air-gapped environments ]: No return channel to confirm delivery

**05 CHALLENGE**

### Unvetted AI Is Running Your Production Line

Manufacturers adopted AI early, computer vision, predictive maintenance, autonomous material handling, but ML models reach production through informal channels: no SBOM, no scan, no approval record.

⚠ The real risk: An unvetted model on a production line is a privileged, trusted process with direct access to manufacturing data and OT-adjacent networks. It's the open-source governance gap from a decade ago, repeating on a shorter runway.

100 malicious ML models were found on Hugging Face, some with reverse shells and remote backdoors. (JFrog Security Research)

**Governance Gaps:**

[ AI/ML governance ]: No approval process for production models
[ AI-BOM ]: No visibility into training data, weights, dependencies
[ Model provenance ]: No chain of custody from repo to floor

> "Manufacturing now accounts for more than one in four cyberattacks globally, and ransomware alone drives 90% of financial losses in the sector. The gap between physical and software security has become the industry's most expensive blind spot."

### Leading Manufacturers Have Closed the Gap

The challenges above are not theoretical. Organizations have faced them, made a strategic decision to address them systematically, and documented measurable results. If you're ready to close the governance gap and secure your software supply chain, learn more here.