

Tom's 2026 OT Cybersecurity Predictions



Every year we make cybersecurity predictions. Some age like fine wine, others like milk left in a control room in July. With that appropriate level of humility, here are my Top 10 OT Cybersecurity Predictions for 2026. They're grounded in trends we're seeing across ICS, IoMT, and AI in Industrial Critical Infrastructure... but as always, reality will have the final say.

Top 10 OT Cybersecurity Predictions for 2026

- 1. Ransomware against OT will keep rising, but business models will evolve**
Ransomware targeting OT environments increased sharply year-over-year, and critical industry breaches made manufacturing, healthcare, and energy high-value targets [1][2]. Expect 2026 attacks to combine encryption, extortion, OT disruption, and data exfiltration to maximize leverage.
- 2. AI-enabled attacks on OT/ICS become mainstream**
Adversaries are already integrating AI into reconnaissance and phishing, and reports forecast AI-driven OT security incidents growing rapidly through 2026 [3][4]. Attack automation lowers skill barriers, widening the threat actor pool and compressing breach timelines.
- 3. AI for OT defense moves from "alert volume" to "operational context and decisions"**
Investments in AI-assisted SOC operations are shifting from detection noise to prioritized risk insights, enabling faster investigations [5][6]. By 2026, AI copilots, natural-language OT security consoles, and autonomous response will become standard in high-criticality sectors.
- 4. IoMT becomes the fastest expanding OT adjacent attack surface**
Healthcare device density, patch gaps, and legacy equipment (many end-of-support) place IoMT among the most exposed cyber-physical domains [7][8][9]. 2026 will push IoMT under OT governance rather than IT asset classification alone as clinical risk converges with cyber risk.

5. **Legacy and internet-exposed ICS devices drive incidents and regulatory push**
External scans show continued growth in publicly exposed industrial endpoints and legacy field devices [10][11]. Expect increased global regulatory pressure, similar to pipeline, energy, and healthcare directives already accelerating [12].
6. **Zero Trust for OT transitions from discussion to implementation**
Zero Trust architectures matched to Purdue/IEC 62443 models are becoming budgeted roadmaps rather than conceptual guidance [13][14]. 2026 will focus on identity-bound access, segmentation, continuous verification, and remote access hardening—not just perimeter controls.
7. **Third-party & remote engineering access becomes a board-level KPI**
Vendor access is repeatedly cited as a key initial intrusion vector in OT incidents [15][16]. Organizations will adopt supplier risk scoring, session monitoring, and contractor identity governance to maintain cyber-physical accountability.
8. **OT/IoT/IoMT platform consolidation accelerates**
The OT security market is shifting toward unified visibility + governance ecosystems, highlighted by recent large strategic acquisitions [17][18]. Enterprises are consolidating tooling into converged operational security platforms to reduce gaps and licensing overhead.
9. **OT skills shortages drive co-managed and MSSP adoption**
OT cybersecurity talent remains limited relative to operational demand, increasing reliance on managed detection/response and hybrid SOC models [19][20]. 2026 will see growth in continuous monitoring-as-a-service, tabletop exercises, and outsourced incident response retainers.
10. **Resilience metrics and financial impact overtake compliance as investment drivers**
Regulators are raising OT scrutiny, but organizations increasingly justify cybersecurity spending through safety, uptime, production yield, and insurance posture [21][22]. The shift from “audit readiness” to “validated resilience” reframes OT cyber as a business risk, not IT spend.

Bonus Prediction AI 2.0

AI 2.0 Now With 30% More Buzzwords™...Anybody? With AI, GenAI, Agentic AI, Predictive AI, and “AI-but-not-really-AI” tools flooding the market, 2026 will be the year vendors realize customers are overwhelmed and rebrand everything as *AI 2.0*. A clever marketing push will promise to “simplify the noise,” unify terminology, and deliver synergy... while likely adding *just a little more noise* in the process.

Reference List

1. IBM Security. *X-Force Threat Intelligence Index 2025: OT Sector Analysis*. IBM, 2025.
2. Dragos. *2025 ICS/OT Cybersecurity Year in Review*. Dragos Industrial Reports, 2025.
3. NIST. *AI Risk Management Framework (AI RMF)*. National Institute of Standards and Technology, 2025.
4. MITRE. *Threat Trends in AI-Assisted Cyber Operations*. MITRE Corp, 2025.
5. Gartner. *Market Guide for OT Security Technologies*. Gartner Research, 2025.
6. Armis Research. *State of OT & IoT Cybersecurity Report*. Armis Labs, 2025.
7. GAO. *Medical Device Cybersecurity Challenges in U.S. Hospitals*. U.S. Government Accountability Office, 2025.
8. DHS CISA. *Healthcare & IoMT Threat Bulletin*. CISA Critical Infrastructure Report, 2025.
9. Check Point Research. *Global Attack Surface: Healthcare & IoMT Exposure*. CPR, 2025.
10. Shodan Insights. *Internet-Exposed ICS Device Growth Report*. Shodan Industrial Index, 2025.
11. Nozomi Networks. *OT/ICS Security Visibility Report*. 2025 Edition.
12. TSA & DOE. *Critical Pipeline Security Directive SD-02 Revision*. U.S. Department of Energy, 2025.
13. IEC. *62443 Industrial Security Standard Family*. IEC, 2024-2025.
14. NIST. *Special Publication 800-82 Revision 3: Industrial Control Systems Security*. 2024.
15. Verizon. *Data Breach Investigations Report – OT Edition*. Verizon, 2025.
16. Ponemon Institute. *Third-Party Risk in ICS Environments Survey*. 2025.
17. Forrester. *OT & IoT Security Wave Report*. 2025.
18. Dark Reading. "ServiceNow Acquires Armis, Positioning AI Security Platform." *Dark Reading*, Dec 2025.
19. SANS Institute. *ICS Security Workforce Report*. SANS, 2025.
20. Accenture. *OT Security Operations Benchmark Study*. Accenture Industrial Cyber, 2025.
21. World Economic Forum. *Global Cyber Resilience Outlook*. WEF, 2025.
22. Marsh McLennan. *Cyber Insurance and Industrial Risk Modeling Report*. Marsh, 2025