tosi The fastest way to connect, protect and control OT networks and critical infrastructure.

Thought Leadership

TOP 10 LESSONS LEARNED IN OT SECURITY IN 2025

A Year of Transformation for Industrial Cybersecurity

By Sakari Suhonen, CEO, Tosi US

The year 2025 marked a turning point for operational technology (OT) security. For many organizations, cyber risk moved from abstract concern to operational reality, with direct consequences for safety, uptime, and business continuity.

At Tosi, we have spent over a decade working alongside operators in oil & gas, water and wastewater, building automation, and industrial environments worldwide. In 2025, what we observed across these sectors was consistent and unmistakable: the way organizations think about OT security is changing, often under pressure, and sometimes too late.

If there is one defining takeaway from the year, it is this. **OT security is no longer a future problem, a niche discipline, or an isolated technical function.** It is a core business risk that demands executive ownership, continuous visibility, and defenses that reflect how industrial operations actually work.

Across multiple industry reports published in 2025, ransomware activity targeting industrial organizations rose sharply. More notably, a growing share of these incidents resulted in operational disruption rather than data loss alone. While reporting methodologies vary, the conclusion is consistent: industrial cyber risk escalated meaningfully in 2025.

What follows are ten lessons the OT security community learned this year, often the hard way.

1 ISOLATION IS NOT PROTECTION

I still hear "we're air-gapped" as if that solves the problem. It doesn't. Most of the intrusions we see start in IT and move laterally. If you can't see what's connected and control who's accessing it, isolation is just a story you're telling yourself.

3 NATION-STATE THREATS ARE A BASELINE ASSUMPTION

This used to be a concern for defense contractors and power grids. Not anymore. If you're running critical infrastructure like water, manufacturing, or energy, you have to assume sophisticated adversaries are interested. Plan accordingly.

5 ASSET VISIBILITY IS AN ONGOING OPERATIONAL CAPABILITY

You can't protect what you can't see. But a static inventory from last year isn't visibility. It's a snapshot that's already wrong. The organizations doing this well treat visibility as a living capability, not a one-time project.

2 RANSOMWARE NOW TARGETS OPERATIONAL DISRUPTION

Attackers figured out that shutting down a plant can hurt more than stealing data. We've watched customers lose days of production from ransomware that never touched a single OT device. It just took down the systems operators needed to do their jobs.

4 THE CISO IS INCREASINGLY ACCOUNTABLE FOR OT SECURITY

The question "who owns OT security?" finally has an answer at most organizations: the CISO. That's the right call. You can't manage risk across IT and OT with two separate strategies and hope they align.

6 ZERO TRUST REQUIRES OT-SPECIFIC ADAPTATION

Zero Trust makes sense in principle, but you can't apply IT frameworks directly to OT and expect them to work. Legacy systems, uptime requirements, safety constraints: you have to adapt the approach or you'll create more problems than you solve.

7 INCIDENT RESPONSE MUST BE PRACTICED, NOT JUST DOCUMENTED

A plan in a binder doesn't help when things go sideways. The customers who run tabletop exercises handle real incidents far better than those who assume their documentation is enough. Practice exposes gaps that paper never will.

8 REMOTE ACCESS REMAINS A PRIMARY EXPOSURE POINT

Every customer I talk to relies on remote access for vendors, integrators, and internal teams. That's not going away. But it's also where we see the most risk. If you're not controlling and monitoring every remote session, you're exposed.

9 COMPLIANCE IS CONVERGING, BUT ENFORCEMENT IS NOT

Whether you're operating in the US or EU, regulators want the same things: visibility, accountability, controlled access. The difference is how they enforce it. Either way, treating compliance as a checkbox guarantees you'll be caught off guard.

10 STRATEGY MUST BE INFORMED BY MATURITY, NOT ASSUMPTIONS

The organizations making real progress start by being honest about where they are. Without that baseline, you're guessing at priorities and hoping your investments pay off. Hope isn't a strategy.

LOOKING AHEAD

Looking ahead, successful OT security programs will be defined less by individual technologies and more by discipline: continuous visibility, practiced response, and executive accountability. Organizations that treat OT security as an operational capability rather than a compliance exercise will be best positioned to manage risk in 2026 and beyond.

APPLY THESE LESSONS TO YOUR ENVIRONMENT

Many organizations struggle not because they lack tools, but because strategy is often built on assumptions rather than objective insight. The challenges outlined above rarely exist in isolation, and most organizations face a combination of visibility gaps, remote access risk, and operational constraints.

Explore how these OT security principles are applied in real-world operational environments, based on organizational needs.

→ EXPLORE SOLUTIONS BY NEED

ABOUT TOSI

Tosi (formerly Tosibox) is the global pioneer in Cyber Physical Systems protection platforms for OT networks. Since 2011, the company has deployed its unified platform to connect, protect, and control hundreds of thousands of industrial devices worldwide. With headquarters in Irving, Texas, and Oulu, Finland, Tosi serves hundreds of enterprise customers globally, directly and through a network of 200+ partners. The company's integrated platform enables rapid deployment, comprehensive visibility, and unified control, simplifying compliance while delivering measurable security and operational improvements.

US HQ
1212 Corporate Drive
Suite 170
Irving, Texas 75038

GLOBAL HQ
Elektroniikkatie 2a
7th floor
90590 Oulu, Finland

CONTACT US

in ▶ tosi