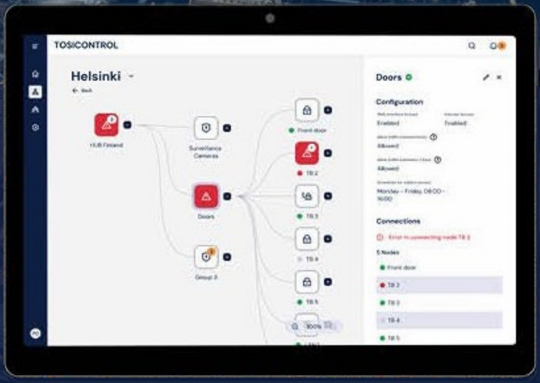
TOSIBOX

Sakari Suhonen

CEO, Tosibox, US

Sakari Suhonen, CEO of Tosibox US, is a proven leader in OT cybersecurity and network automation. With over 20 years leading B2B software companies, he has transformed organizations and driven exceptional growth, including spearheading Finland's first B2B enterprise SaaS company IPO. His business acumen and innovative approach have established him as a respected executive with a consistent track record of delivering results.



Why OT Cybersecurity Should Be Your Top Priority in 2025

EXECUTIVE ALERT

When Industrial Systems Become the Target

Let me share a sobering wake-up call that hit our industry recently. In January 2024, I watched closely as Keytronic Corporation – a major printed circuit board manufacturer – faced every executive's nightmare. Their story particularly resonated with me because it demonstrated how quickly a cybersecurity incident can escalate from an OT problem to a board-level crisis.

The incident began during a routine Tuesday morning when their security team flagged suspicious network activity. Within hours, their leadership had to make an unprecedented decision: shut down manufacturing operations across multiple facilities. This wasn't just a technical glitch – the BlackBasta ransomware group had gained control of their operational technology systems, the very industrial controls managing their precision manufacturing equipment.

The business impact was immediate and severe. A two-week production shutdown followed, triggering a cascade of consequences that would be familiar to any manufacturing executive: missed customer commitments, disrupted supply chains, and ultimately a drop in stock price when the incident became public. Perhaps most troubling for the board was learning that the attackers had lurked in their systems for weeks, methodically studying their industrial control systems before striking.

As you review your own risk assessments and cybersecurity investments, consider this: Is your organization prepared to prevent this type of operational devastation? Have you truly protected the industrial systems that form the backbone of your business?

The Growing Threat to Our Industrial Systems

Today's world runs on connected industrial systems controlled by Operational Technology (OT) - the hardware and software that monitors and controls physical devices and industrial processes. Unfortunately, the frequency and sophistication of attacks targeting operational technology (OT) networks have risen dramatically. Recent Microsoft analysis reveals that 78% of industrial network devices have known vulnerabilities - with 46% running deprecated firmware that can't be patched and 32% operating with unpatched vulnerabilities.

This exposure has led to several devastating attacks in 2024: the Sandworm group targeted a Texas water treatment facility causing overflow, American Water's operations across 24 states faced disruption by suspected state-backed actors, and the China-linked Volt Typhoon campaign persistently targeted critical US infrastructure sectors including water, energy and transportation. These incidents underscore a concerning trend.

Adding to the potential damage are often-lacking security measures, which make OT attacks not only attractive for attackers but also relatively easy to execute. The urgency of this situation is reflected in recent market projections from MarketandMarkets - the OT security market is expected to grow from $20.7 billion in 2024 to $44.9 billion by 2029, representing a compound annual growth rate (CAGR) of 16.8%. With industrial systems becoming increasingly connected and vulnerable, organizations are investing heavily in network security and segmentation to protect their critical infrastructure.

Why OT Security is the New Battleground

When we talk about protecting OT systems, we face unique challenges that traditional IT security approaches can't address:

Safety risks

Unlike typical IT breaches that might expose data, attacks on OT systems can cause physical harm. In 2021, attackers tried to poison a Florida water supply by remotely changing chemical levels, and in 2024, Russian-backed hackers targeted a water treatment facility in Texas, as reported by CNBC.

Legacy infrastructure

Many OT systems were built decades ago when cybersecurity wasn't a consideration. These systems often run outdated software that can't be easily updated, lacking basic features like encryption or access controls, according to recent analysis from SC Media.

Expanded attack surface

The explosion of connected devices creates more entry points for attackers. IoT Analytics projects we'll see 35 billion connected devices by 2028.

Limited visibility

Fortinet's latest State of Cybersecurity Report reveals a critical security gap: only 5% of organizations report 100% visibility of their OT systems, while 67% have visibility of about 75% of their systems. This blind spot creates significant vulnerabilities that attackers can exploit.

Sophisticated adversaries

Both criminal groups and nation-states are developing advanced attacks specifically designed for industrial targets. The Department of Financial Protection and Innovation recently warned that organizations like Volt Typhoon are specifically targeting critical infrastructure with the apparent intent to disrupt services during potential geopolitical conflicts.

Skills deficit

The Ponemon Institute's latest research shows only 44% of organizations believe they have enough staff to manage OT security risks and only 52% have dedicated OT security incident response teams.

Five Strategic Priorities for OT Security

As we look toward the future of OT security, focus on these five priorities:

1

Create internal boundaries

According to Gartner's latest Market Guide for Operational Technology Security, network segmentation is capturing over a quarter of all OT security spending. By establishing secure zones within your networks, you can contain breaches and prevent lateral movement. Their research shows that 84% of OT breaches spread beyond their initial entry point when proper segmentation isn't in place.

2

Make critical systems "cyber invisible"

The NSA and CISA jointly recommend using unidirectional gateways, strategic air-gapping, and connection reduction to ensure that essential control systems simply can't be seen or reached by attackers. What hackers can't see, they can't target.

3

Deploy continuous monitoring solutions

Deploy continuous monitoring solutions: utilize technologies that can detect anomalies in real time. Establishing a robust vulnerability management system can greatly minimize cybersecurity risks.

4

Develop specialized expertise

DNV GL's latest report reveals that while 84% of energy sector employees say they know what to do if they spot a potential cyber threat, over three-quarters worry their training isn't sophisticated enough to handle advanced attacks. Consider partnering with OT security specialists who understand both IT security principles and industrial operations.

5

Navigate complex compliance

Organizations now face expanding regulatory requirements including the NIS2 Directive in Europe, the Cyber Inicident Report for Critical Infrastructure Act (CIRCIA) in the US, and various sector-specific frameworks. Forward-thinking organizations are creating compliance crosswalks that map controls across multiple frameworks.

Executive Action Plan

Immediate Actions

Deloitte's latest research shows that two-thirds of organizations are planning to increase OT security spending this year. Their analysts warn that delaying puts you at risk. We're seeing the emergence of specialized security leaders focused specifically on OT systems. The time for action is now.

Implementation Strategy

McKinsey's latest practical guide emphasizes looking for solutions designed for OT environments that are simple to implement and operate. The ideal security tools should provide robust protection without requiring every team member to become an OT security expert.

Partner to Create Cross-Functional Excellence

Success requires bridging the IT-OT divide. The Ponemon Institute's latest study reveals that organizations that effectively connect these traditionally siloed teams and partner with OT security specialists experience 62% fewer disruptive security incidents. By speaking both languages - IT and OT - your security approach becomes more comprehensive and effective. Bringing in OT network experts can provide an added layer of expertise to help bridge the gap.

IT OT

A Call to Action

OT cybersecurity is no longer optional---it's a critical business imperative. As digital transformation accelerates, organizations must adopt a proactive, comprehensive approach to protecting their operational technologies.

As an executive, you have the opportunity to position your company ahead of this curve. Those who prioritize OT security today will be better positioned to innovate safely in tomorrow's connected world, while those who delay may find themselves managing crises instead of leading transformation.

Sakari Suhonen

CEO, Tosibox, US

Sakari Suhonen, CEO of Tosibox US, is a proven leader in OT cybersecurity and network automation. With over 20 years leading B2B software companies, he has transformed organizations and driven exceptional growth, including spearheading Finland's first B2B enterprise SaaS company IPO. His business acumen and innovative approach have established him as a respected executive with a consistent track record of delivering results.