cabreza

CONVERGENCE & NETWORK SECURITY · January 2026

IT/OT Convergence: Security Implications

The attack path adversaries exploit most frequently

EXECUTIVE SUMMARY

> The air gap is dead. 70% of OT incidents originate from IT networks, and when ransomware reaches OT, 75% cause partial shutdown. This whitepaper analyzes the convergence reality, the attack patterns that exploit it, and the segmentation strategies that actually reduce risk.

The Reality

The air gap is dead. **70% of OT systems** will connect to corporate IT networks within the next year. 66% of manufacturing plants already use IP networks with real-time data. The convergence of IT and OT isn't a future concern—it's operational reality.

The business drivers are real. Production data flowing to ERP systems. Predictive maintenance requiring cloud analytics. Remote operations enabling efficiency gains. Supply chain integration demanding real-time visibility.

But connectivity creates the attack path adversaries exploit most frequently. When OT connects to IT, it inherits IT's threat exposure.

The Evidence: IT Is the Entry Point

Attack origin data is consistent across sources:

FINDING	SOURCE
70% of OT incidents originated from IT	Dragos
75% of manufacturing incidents began in IT	IBM/ARC
#1 attack vector: Pivot from enterprise IT	Dragos (unchanged since 2019)
58% of ICS/OT incidents used IT as entry	Dragos

The pattern is clear: adversaries compromise IT first, then pivot to OT. This isn't because OT security is stronger—often it's weaker. It's because IT systems are internet-exposed while OT traditionally wasn't. Attackers take the path of least resistance.

Ransomware on OT has surged:

YEAR	RANSOMWARE IMPACT ON OT
2023	32% of incidents
2024	56% of incidents

A 24-percentage-point increase in one year. The encryption of IT systems connected to OT—historians, engineering workstations, management servers—can halt operations even when PLCs remain unaffected.

When attacks reach OT, physical consequences follow:

- 75% of ransomware attacks on industrial organizations caused partial OT shutdown
- 25% caused full OT shutdown
- 74% of OT attacks could cause physical harm to employees or public (Nozomi)

IT incidents cause data loss and operational disruption. OT incidents can cause those plus physical harm. When IT threats reach OT through converged networks, they gain access to consequences pure IT attacks can't achieve.

The Segmentation Illusion

Dragos's field experience reveals a consistent gap between perceived and actual network segmentation:

> *"Many organizations believe they have proper IT/OT network segmentation, but routine penetration tests reveal hidden connections bridging IT and OT."*

The belief in segmentation provides false comfort. Organizations that think they're isolated may not monitor for threats crossing a boundary they believe exists.

How hidden connections develop:

- Vendor support tools require "temporary" connectivity that becomes permanent
- Engineers create connections for convenience that persist indefinitely
- Acquisitions bring undocumented legacy connections
- Shadow IT bridges environments without security review
- System updates and changes create new paths nobody tracks

Historical improvement—with caveats:

YEAR	SEGMENTATION ISSUES
2019	77%
2022	50%
2024	"Flat networks remain common"

More organizations have implemented some segmentation. But partial segmentation may be worse than none—it creates false confidence while still providing attack paths.

The Organizational Gap

Convergence creates security challenges that neither IT nor OT teams can address alone. But organizational structures often don't reflect this reality.

Teams work independently:

- 41% of firms report IT and OT teams operate separately
- When teams work independently on a shared problem, gaps develop at the boundary
- IT implements controls that break OT operations
- OT creates connections that bypass IT security
- Incidents crossing boundaries have unclear ownership

Staff are stretched:

YEAR	% RESPONSIBLE FOR BOTH IT AND OT
2022	20%
2023	38%

The near-doubling of dual-responsibility staff reflects convergence reality but also expertise dilution. IT security skills don't automatically translate to OT understanding. Staff with primary expertise in one domain struggle to cover the other effectively.

Maturity lags: Only 19% of firms are considered "advanced" in securing IT/OT systems per NIST CSF assessment. 81% have converging environments without mature security programs to protect them.

The 90% Finding

Perhaps the most striking statistic:

> *"Approximately 90% of organizations with connected OT infrastructures experienced a security breach in SCADA/ICS systems."*

If breach is nearly certain for connected environments, prevention alone cannot be the strategy. The security model must include detection, response, and recovery—the full spectrum of capabilities needed when prevention fails.

This doesn't mean prevention is worthless. It means prevention is insufficient. Organizations operating connected environments should plan for compromise, not just against it.

The Path Forward

1. **Audit actual connectivity** — Not documented connectivity; actual network traffic. Many organizations discover connections they didn't know existed. You can't secure what you don't know about.
2. **Enforce segmentation technically** — Firewalls and network controls, not just policies. Test segmentation through penetration testing. Assumptions about isolation are frequently wrong.
3. **Monitor the boundary** — The IT/OT boundary is where attacks transition from IT threat to OT impact. Standard IT security tools may not understand OT protocols. Purpose-built monitoring at crossing points provides visibility that generic tools miss.
4. **Coordinate teams** — Independent IT and OT response fails when incidents cross boundaries. Establish communication channels, shared understanding of each environment's constraints, and joint planning for cross-boundary scenarios.
5. **Plan for compromise** — 90% breach rates mean resilience, not just prevention. Detection capabilities that identify attackers in the environment. Response capabilities that contain damage. Recovery capabilities that restore operations.
6. **Accept the reality** — IT and OT are converging. This isn't a future state to prevent; it's current reality to address. Security strategies based on air gaps no longer apply for most industrial organizations.

When IT and OT connect, IT threats become OT threats. Organizations that treat these as separate problems will find that attackers have already unified them.

Sources

- Dragos, OT Cybersecurity Year in Review: https://www.dragos.com/ot-cybersecurity-year-in-review
- Cisco, State of Industrial Networking Report: https://www.cisco.com/c/en/us/solutions/internet-of-things/state-of-industrial-networking-report.html
- Claroty, Global State of CPS Security 2024: https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions
- Nozomi Networks, OT/IoT Security Report: https://www.nozominetworks.com/resources/ot-iot-security-report
- SANS Institute, State of ICS/OT Security 2025: https://www.sans.org/white-papers/state-of-ics-ot-security-2025