cabreza

PROCESS & GOVERNANCE • January 2026

The Process Improvement Gap in Industrial Security

Organizations that can see problems but lack the machinery to solve them

EXECUTIVE SUMMARY

> Process improvement ranks 8th in OT security investment at just 31%. Only 17% invest in tabletop exercises. This whitepaper examines why organizations can detect problems but struggle to solve them, and how to build the operational processes that convert visibility into outcomes.

The Problem

Process improvement ranks **8th** in OT security investment priorities at 31%. Only 17% of organizations invest in ICS-specific tabletop exercises. SOAR adoption sits at 12%—the lowest measured category.

Meanwhile, detection tools dominate: logging and monitoring at 72%, asset inventory at 67%.

This imbalance produces a predictable result: organizations that can see problems but lack the organizational machinery to solve them. Sophisticated detection generates alerts that go to teams without the processes, playbooks, or practiced capability to respond effectively.

Process isn't glamorous. Governance structures, escalation paths, and operational procedures don't make for compelling demos. But process is the backbone that determines whether technology investments produce outcomes.

The Evidence: Technology Investment Outpaces Organizational Capability

Investment priorities reveal the imbalance:

AREA	INVESTMENT RATE
Logging, monitoring, detection	72%
Asset inventory	67%
Secure remote access	52%
Process improvements	31%
Tabletop exercises	17%
SOAR	12%

Detection and visibility tools receive majority investment. Process and organizational capability receive minority investment. The gap between seeing problems and solving them widens.

Incident response capability lags:

FINDING	PERCENTAGE
Organizations with dedicated ICS/OT IR plan	56%
Organizations lacking ICS/OT-specific IR	44%
SOC with OT capabilities	31%
"Extensive" OT network monitoring	12%

44% of organizations have no OT-specific incident response plan. They may have generic IT procedures, but applying IT incident response to OT can make situations worse—isolating systems that must remain operational, triggering safety shutdowns, or destroying evidence needed to understand the attack.

Budget ownership fragments:

BUDGET OWNER	PERCENTAGE
CISO/CSO leads decisions	27%
Shared IT/OT budget	37%
IT controls budget	31%
ICS/OT responsible	26%

Only about a quarter of organizations have CISO-led OT security budgets. The rest operate with fragmented ownership and unclear accountability. When multiple parties share responsibility, nobody fully owns outcomes.

Third-Party Access: A Case Study in Process Failure

Third-party access to industrial environments represents one of the clearest examples of process failure enabling technical compromise.

The attack vector is proven:

- 82% experienced at least one attack from third-party access in the past year
- 45% experienced five or more such attacks
- 63% have partial or no understanding of third-party connectivity

Tool sprawl reflects process absence:

FINDING	PERCENTAGE
Organizations with 4+ remote access tools	55%
Organizations with 6+ remote access tools	33%
2+ non-enterprise grade tools on OT	79%
Maximum tools in single enterprise	16

These tools didn't accumulate through coordinated strategy. One project needed VPN access. Another used a remote support tool. A third deployed a vendor's proprietary solution. Without process to govern tool selection and deployment, complexity grows unmanaged.

The technology to secure third-party access exists. What's missing is process to:

- Authorize access appropriately
- Review whether access remains necessary
- Monitor third-party sessions
- Revoke access when relationships end

82% of organizations experienced attacks through this vector. Process failure, not technology failure, enabled most of them.

Why Process Gets Deprioritized

Technology is easier to buy.

Tools have clear purchase paths. Budgets are allocated. Procurement executes. Something tangible exists afterward.

Process investment is harder:

- Who owns process development?
- How do you budget for organizational change?
- What does "done" look like?
- How do you measure success?

The difficulty of executing process investment leads organizations to default to technology, even when process would produce more value.

Process isn't visible.

Detection dashboards provide visible evidence of security investment. Executives can see assets discovered, alerts generated, threats detected.

Process improvement produces less visible results:

- IR plans sit in document repositories
- Governance structures are organizational charts
- Training produces knowledge, not artifacts
- Exercises produce learnings, not dashboards

When security leaders need to demonstrate investment value, technology produces more compelling visuals.

Process requires cross-functional coordination.

Technology deployment can occur within IT or security teams. Process improvement typically requires coordination across IT, OT, operations, engineering, compliance, and leadership.

Cross-functional coordination is harder than single-team execution. Organizations default to what they can accomplish within existing authority—which usually means technology over process.

What the Data Shows Works

Tabletop exercises multiply readiness.

Organizations including field technicians in tabletop exercises report readiness levels **1.7x higher** than those that don't. Same technology, dramatically different capability.

Only 17% invest in ICS-specific tabletops despite this evidence. The investment-to-outcome ratio is exceptionally favorable.

CISO leadership improves outcomes.

CISO-led programs are 82% likely to be mapped to security standards versus 42% for organizations without corporate-wide policies. Executive-level attention to OT security affects not just budget but program maturity.

Regulated sites perform better.

Regulated sites experience 50% fewer financial losses and safety impacts—not because they have fewer incidents, but because compliance forces them to operationalize discipline. Required IR plans get practiced. Required controls get implemented.

The mechanism: regulation makes process investment mandatory rather than optional.

The Path Forward

1. **Budget explicitly for process** — Process should be a line item, not overhead. Categories might include: IR development, exercises, governance implementation, third-party access management, training.
2. **Measure process outcomes** — Detection metrics are straightforward (alerts generated, assets discovered). Process metrics require more thought: incident response time, third-party access accuracy, exercise participation, policy currency.
3. **Start with high-impact gaps:**
    - **OT-specific IR plan** (44% lack one)
    - **Third-party access management** (82% experienced attacks via this vector)
    - **Tabletop exercises** (1.7x readiness improvement)
4. **Clarify ownership** — Fragmented budget authority produces gaps. Someone needs to own OT security outcomes with corresponding authority and accountability.
5. **Make process investment visible** — Report on response time improvements, exercise findings, and capability development alongside technology metrics.

Detection generates alerts. Process determines whether those alerts produce outcomes.

Technology enables security. Process produces it.

Sources

- SANS Institute, State of ICS/OT Cybersecurity 2024: https://www.sans.org/blog/the-2024-state-of-ics-ot-cybersecurity-our-past-and-our-future
- SANS Institute, State of ICS/OT Security 2025: https://www.sans.org/white-papers/state-of-ics-ot-security-2025
- Dragos, OT Cybersecurity Year in Review: https://www.dragos.com/ot-cybersecurity-year-in-review
- Claroty, The Problem with Remote Access Tool Sprawl: https://claroty.com/resources/reports/the-problem-with-remote-access-tool-sprawl
- Claroty, Global State of CPS Security 2024: https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions