cabreza

WORKFORCE & TRAINING • January 2026

The OT Talent Crisis and Knowledge Gap

The paradox of recognizing people as the greatest risk while underinvesting in them

EXECUTIVE SUMMARY

> Over half of the ICS/OT security workforce has less than five years of experience, yet organizations invest twice as much in technology as workforce development. This whitepaper analyzes the talent crisis, the certification gap, and practical strategies for building human capability alongside technical controls.

The Problem

More than half of the ICS/OT security workforce—**52.6%**—has been in the field for five years or less. 51% lack OT-specific certifications. Only 9% dedicate 100% of their time to OT security.

These aren't abstractions. They mean that systems controlling power plants, water treatment facilities, manufacturing operations, and transportation networks are frequently protected by personnel who are still learning the unique characteristics of operational technology environments.

Organizations recognize the problem: 66% identify people as their greatest security risk. Yet they allocate 52% of budget to technology and only 25% to workforce development.

You can buy sophisticated detection tools. You cannot buy experienced operators.

The Evidence: An Inexperienced, Stretched Workforce

The experience gap is significant:

FINDING	STATISTIC
Workforce with ≤5 years experience	52.6%
Lacking ICS/OT-specific certifications	51%
100% dedicated to OT security	Only 9%
View OT as primary responsibility	65%

This isn't a criticism of the workforce—it reflects a rapidly growing field that didn't exist as a distinct discipline until recently. The talent pipeline hasn't had time to mature. But the implications are serious: deep expertise in OT security takes years to develop, and most practitioners are still early in that journey.

Staff are increasingly stretched across both IT and OT:

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

The near-doubling reflects convergence reality—but also expertise dilution. When a single person covers both environments, OT often gets less attention. IT systems generate more alerts, face more frequent attacks, and have more mature tooling. OT security becomes secondary.

The investment paradox persists:

CATEGORY	BUDGET ALLOCATION
Technology	52%
Workforce development	25%
Organizations identifying people as greatest risk	66%

Two-thirds of organizations recognize that people are their greatest risk. They then invest twice as much in technology as in the people who must operate it. This pattern is understandable—technology produces tangible outputs while training is harder to measure—but the downstream effects are significant.

The Consequences: Capability Gaps Where They Matter Most

Incident response suffers most visibly:

FINDING	PERCENTAGE
Organizations with dedicated ICS/OT IR plan	56%
Organizations lacking ICS/OT-specific IR	44%
SOC with OT capabilities	31%
Using range environments for OT training	34%

44% of organizations have no OT-specific incident response plan. They may have generic IT procedures, but applying IT incident response to OT environments can make situations worse—taking systems offline that must remain operational, triggering safety shutdowns that cause more damage than the incident itself, or destroying forensic evidence needed to understand what happened.

Dragos field teams consistently encounter this gap:

> *"Most ICS engineers and OT personnel are not trained in cyber incident response, leaving them ill-equipped to recognize or contain cyber threats."*

Knowledge retention creates compounding risk:

When experienced personnel leave, institutional knowledge leaves with them. This person knows that PLC was configured differently during the 2018 expansion. That engineer remembers why the network was segmented this particular way. Documentation is frequently incomplete or outdated.

New hires spend months rediscovering what predecessors knew intuitively.

> *"Limited forensic data collection in OT environments means that after an incident, organizations don't have the insights they require to know what happened—or if the threat is still present."*

Without experienced personnel who understand both the systems and the security implications, organizations struggle to learn from incidents and prevent recurrence.

What the Data Shows Works

Training produces measurable returns:

Organizations including field technicians in tabletop exercises report readiness levels **1.7x higher** than those that don't. The technology is identical—the training makes the difference.

Strategic employee training correlates with **$260,000 less in breach costs**. This represents tangible ROI that can justify training budgets.

Organizational structure matters:

CISO-led programs are **82% likely** to be mapped to security standards, versus 42% for organizations without corporate-wide policies. When OT security has executive-level attention, programs develop more systematically. Policies get operationalized rather than just documented.

GOVERNANCE MODEL	MAPPED TO SECURITY STANDARDS
CISO-led programs	82%
No corporate-wide policies	42%

Dedicated roles outperform split responsibilities:

The 9% of professionals who are 100% dedicated to OT security represent the organizations most likely to develop deep expertise. The 38% covering both IT and OT are spread too thin to develop mastery in either domain.

The Path Forward

The talent gap won't close through hiring alone—there aren't enough experienced practitioners to hire. Organizations need sustained investment in developing the workforce they have.

1. **Invest proportionally to the risk** — If 66% of organizations identify people as their greatest risk, 25% budget allocation isn't proportionate. Training, certification support, and retention programs deserve budget comparable to technology.
2. **Retain expertise aggressively** — Developing OT security practitioners takes years. Losing them to competitors or burnout wastes that investment. Career pathways, competitive compensation, and manageable workloads matter.
3. **Capture institutional knowledge** — Document system configurations, historical decisions, and operational context before it walks out the door. When the one person who understands a system leaves, the organization shouldn't lose that knowledge entirely.
4. **Dedicate roles where possible** — Split IT/OT responsibility dilutes expertise in both domains. Where organizational scale permits, dedicated OT security roles develop deeper capability.
5. **Practice incident response** — The 1.7x readiness improvement from tabletop exercises represents exceptional ROI. Practiced teams outperform unpracticed teams regardless of tool sophistication.

The tools exist. The frameworks exist. What the industry lacks is a workforce scaled, trained, and retained to use them effectively.

Technology enables security. People produce 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, Guardians of Government - Federal OT Security: https://claroty.com/resources/reports/guardians-of-government-the-state-of-federal-ot-security
- OPSWAT/SANS Workforce Report: https://www.prnewswire.com/news-releases/opswat-sponsored-sans-2024-icsot-cybersecurity-report-uncovers-critical-workforce-gaps-302272455.html