SANS | Research Program

SURVEY

SANS 2026 State of ICS/OT Security Survey Insights

Industrial Cybersecurity at a Crossroads



Written by Jason Christopher
Foreword by Tim Conway

November 2026

OPSWAT.

©2026 SANS™ Institute

Table of Contents

Foreword 1

2026 SANS ICS/OT Survey Key Findings 2

Introduction 3

Past: Retrospectives on Industrial Cyber Incidents . . 4

Present: Understanding Current Threats and Detection Capabilities 8

Future: Preparing for Cyber Resilience, Response, and Recovery 15

Conclusions and Next Steps for Industry 22

Demographics 24

Appendix: The SANS ICS 2026 Cyber Resilience Scorecard 25

Appendix: An Industrial Cyber Leader's Guide to ICS/OT Insights 26

Sponsor 28

About the Author



Jason Christopher

Principal Instructor

Senior Vice President, AI, Cybersecurity and Resilience at Energy Impact Partners

Jason teaches **SANS ICS456: Essentials for NERC Critical Infrastructure Protection** and co-authors **SANS ICS418: ICS Security Essentials for Leaders**. Jason's strength in the classroom comes from two decades bridging engineering, policy, and utility operations, turning regulatory complexity and real-world constraints into practical guidance.

READ MORE ABOUT JASON

Foreword



Tim Conway

SANS Fellow

SANS ICS Curriculum Lead at SANS Institute

In reviewing this year's survey, I need to lead with a huge thank you to the community members who showed up in force, during what I know is a relentless schedule, to spend some of their valuable time in contributing to an industry resource. I also want to recognize the unbelievable heart and care that goes into these surveys from the SANS team and, specifically, from Jason Christopher for making certain the survey is delivering with precision and highlighting the actionable trends necessary to inform and drive outcomes that matter. Many organizations and leaders are seeking consensus, benchmarking information, and peer information sharing to assist in programmatic guidance on what realities others are seeing and where they need to be heading. Additionally, we have a practitioner community who takes the time to carefully contribute here to ensure that others have a clear understanding of the challenges being faced and where resources are being allocated. The enormous amount of data being produced, which is analyzed, summarized, and compared to identify trends, then shared across the industry to help drive outcomes, is truly impressive. The fact that it is driven by the community for the community with a leader like Jason helping to navigate is reassuring every year. This year is no different, with Jason once again delivering a true masterclass for the industry, capturing historical trends, identifying the current state of the field, and forecasting where it's heading. I continue to be excited to see how leaders across the industry put these insights into action. And I look forward to watching this survey continue to evolve as a measure and early warning of trends of concern to the defense of critical infrastructure worldwide.

2026 SANS ICS/OT Survey Key Findings

SANS | Research Program

The 2026 State of ICS/OT Security Survey gathered responses from nearly 700 industrial security professionals across every major critical infrastructure sector. This year's theme was cyber resilience: keeping operations safe and running when an incident happens anyway. Six findings from the data demonstrate both how far we've come, and how much more we have left to do.

SUFFERED AN ICS/OT INCIDENT

34%

34% of respondents suffered an ICS/OT cyber incident this year, the largest single-year jump in the survey's history, and detection times slowed for the first time since SANS began tracking them.

DETECTED BY ICS/OT-NATIVE PLATFORMS

38%

38% of incidents were caught by dedicated ICS/OT detection platforms, which is now the No. 1 way industrial incidents are discovered, although the method was unheard of a decade ago when purpose-built OT detection was in its infancy. IT perimeter tools (31%) and trained operators (20%) round out a genuinely layered defense.

DON'T KNOW IF MANUAL OPERATIONS WOULD HOLD

40%

40% of respondents cannot say whether they could sustain manual operations past 48 hours, and only **15%** are confident they can. The disciplined few are rewarded: Those who fully integrate ICS/OT resilience into BC/DR (**just 16%**) and test annually recover the same day at nearly double the rate.

INCIDENTS HALTED OPERATIONS

72%

72% of incidents brought facility or system downtime, while safety impacts nearly doubled and theft of intellectual property rose more than fivefold.

FULL IT/OT VISIBILITY

13%

13% of organizations have full IT/OT visibility across the cyber kill chain, and it demonstrably changes what gets through: They saw far less perimeter exploitation and unauthorized access. For everyone else, budget remains the No. 1 barrier to increasing visibility.

COULD SURVIVE LOSING THEIR AUTOMATION VENDOR

1 in 10

1-in-10 respondents could operate indefinitely if their primary automation vendor disappeared; a majority would be down within a year. The dependency runs through people too: **68%** face operational risk if one or two veterans leave, and only **20%** run a fully functional supply chain cyber risk program.

Each of these findings is unpacked in the sections that follow. To see where your organization stands, take the self-assessment in the appendix: 11 questions, each scored against this year's benchmarks and organized by the SANS Five ICS Cybersecurity Critical Controls.

©2026 SANS™ Institute

Introduction

Beginning in 2017, the *State of ICS/OT Security Survey* has provided industry practitioners with annual benchmarks to help build cybersecurity programs, inform budget priorities, and track critical trends for protecting critical infrastructure. Since its inception, SANS has been able to provide analytics on where industry has matured and where there are still gaps across technology deployments, workforce skills, and internal processes.

This year is no different; however, the focus is squarely on one key topic: resilience. In previous years, we have asked questions around nearly every type of technology that asset owners/operators can deploy in industrial environments. However, given the heightened geopolitical climate, increased threat activity, and a notable pivot in global regulatory requirements, this year our focus is on how organizations are moving toward addressing resilience in cyber operations.

There is a popular motto across cybersecurity practitioners, from the late Dr. Eric Cole:

"Prevention is ideal, detection is a must."

Resilience, however, is a concept that goes beyond detection. How do we recover vital systems? Can we "keep the lights on" despite having a cyber incident? What does it look like to maintain reliable and safe operations during a sophisticated ICS-targeted cyberattack?

Our pivot this year is intended to highlight that, despite our maturity and growth over the last decade, there is still plenty of work to do. Recent events, including the attacks on power systems in Poland and water systems in the United States, demonstrate that the targeting of ICS/OT systems is increasing. Based on the findings from the *2025 State of ICS/OT Security Survey*, we know that industry can (and should) do more to deepen their understanding of their industrial environments.[1] Building on this discussion, we wanted to specifically ask "What do we do if/when things go wrong?"

This year's survey is based on responses from nearly 700 professionals across diverse industrial sectors—one of the highest participation rates in the history of this report.[2] The key findings at the front of this report sketch the arc the data tells: Incidents are up, their impacts are heavier, and detection has matured into a layered discipline led by ICS/OT-native platforms. Visibility, however, is only one aspect of cyber resilience. As attackers increasingly focus on industrial operations, securing our supply chain and understanding the impacts of safety and manual operations will be the deciding factors for mitigating cyber risk. The sections that follow walk that arc from past to present to future. New this year, readers can now self-assess to the benchmarks using the SANS ICS 2026 Cyber Resilience Scorecard in the appendix.

One note on reading the data: Our respondents come from the SANS community, which skews toward organizations already investing in ICS/OT security. The benchmarks in this report are therefore best read as a floor. If, for example, the most security-invested slice of industry reports a one-in-three incident rate and widespread resilience gaps, the industrywide reality is likely worse.

[1] The Appendix of the 2025 survey included a breakdown, by Purdue Model levels, of where industry is performing a variety of activities, from detection to vulnerability management.
[2] Survey demographics are located at the end of this report.

Past: Retrospectives on Industrial Cyber Incidents

In past reports, we've examined incident response from the perspective of failed controls and external pressures. While this year we maintained that focus, we also dove deeper into the impacts.

The 2026 survey highlights the largest jump in reported incidents since SANS began recording ICS/OT incident response statistics. One in three respondents (34%) suffered a cyber incident that impacted their control systems. Similar to previous years, a third of those (31%) were from ransomware. Ransomware no longer stands alone at the top, however: Shared IT/OT credential and identity compromise tied it at 31% of reported incidents, and supply chain compromise appeared in one in five responses (21%). A full breakdown of the incident type can be found in Figure 1.

Q: Did your organization experience any security incidents in your ICS/OT environment in the past 12 months?

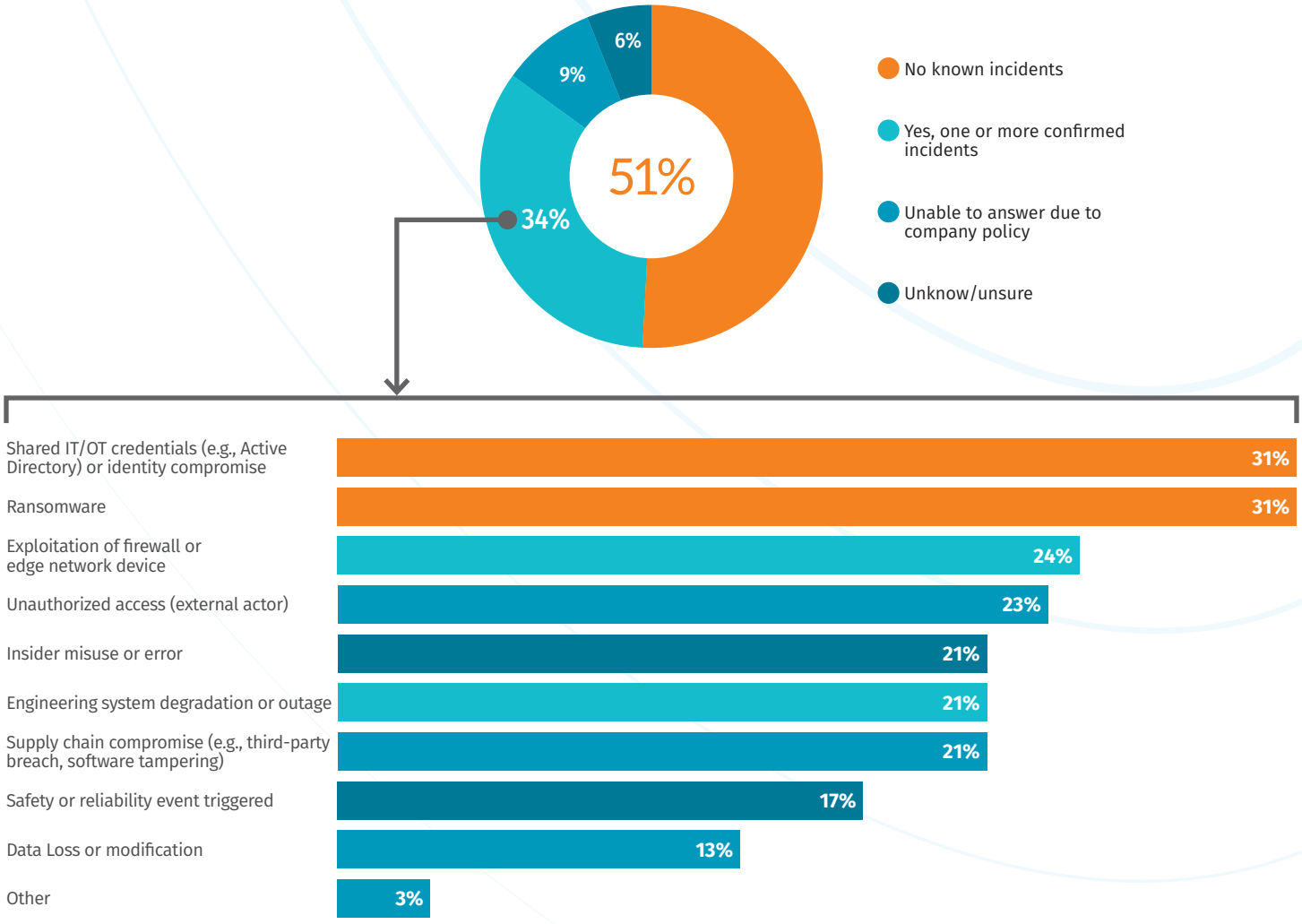


Figure 1. 2026 ICS/OT Cyber Incidents

Not only did the rate of reported incidents increase by a factor of 1.7 from 2025, but the impacts were more severe. Impacts to safety nearly doubled (7% of respondents in 2025 compared to 13% in 2026) and theft of intellectual property reported from these incidents skyrocketed fivefold (from 6% in 2025 to 31% this year). Financial loss, from direct revenue impacts to ransom payments, was close behind: 34% of respondents with incidents reported it, the second most common business impact this year behind facility downtime (35%).

Cyber resilience, as we introduced in the beginning of this report, can best be defined as the ability to maintain reliable and safe operations during an incident. Here, we see our first alarming trend: 72% of reported ICS/OT cyber incidents were accompanied by facility or system downtime. A full breakdown of average downtimes can be found in Figure 2. Ransomware events were significantly slower to respond to, with 31% of those incidents taking eight to 30 days to bring the facility or system back to operations. Similarly, if a safety or reliability event was triggered, the average system or facility downtime spiked compared to other types of ICS/OT cyber incidents.

Q: What type of incident(s) occurred?
Select all that apply.

	<6 hours	6–24 hours	2–7 days	8–30 days	1–3 months	4–6 months	7–12 months	1 year	Over a year	No impact	Unknown/ unsure
Data loss or modification	10%	14%	10%	14%	17%	0%	0%	0%	0%	31%	3%
Safety or reliability event triggered	5%	18%	31%	31%	8%	0%	0%	3%	0%	5%	0%
Supply chain compromise (e.g., third-party breach, software tampering)	4%	17%	21%	23%	11%	0%	0%	0%	0%	21%	2%
Insider misuse or error	0%	15%	31%	15%	4%	0%	2%	2%	0%	21%	2%
Engineering system degradation or outage	2%	23%	25%	23%	10%	0%	0%	0%	0%	10%	0%
Unauthorized access (external actor)	8%	15%	13%	17%	4%	2%	0%	2%	0%	31%	2%
Exploitation of firewall or edge network device	7%	17%	24%	19%	9%	0%	0%	0%	0%	21%	2%
Shared IT/OT credentials (e.g., Active Directory) or identity compromise	10%	7%	26%	17%	9%	0%	0%	0%	0%	21%	1%
Ransomware	4%	19%	20%	31%	11%	1%	0%	0%	0%	10%	4%
Other	17%	0%	17%	17%	0%	0%	0%	0%	0%	50%	0%

Figure 2. Facility or System Downtime During ICS/OT Cyber Incidents

As we teach across the SANS ICS curriculum, incident timelines can be broken into three distinct stages, as seen in Figure 3:

1. Compromise-to-detect
2. Detection-to-containment
3. Containment-to-remediation

The distributions for these timelines across the 2026 participants who suffered an ICS/OT cyber incident can be found in Figure 4.

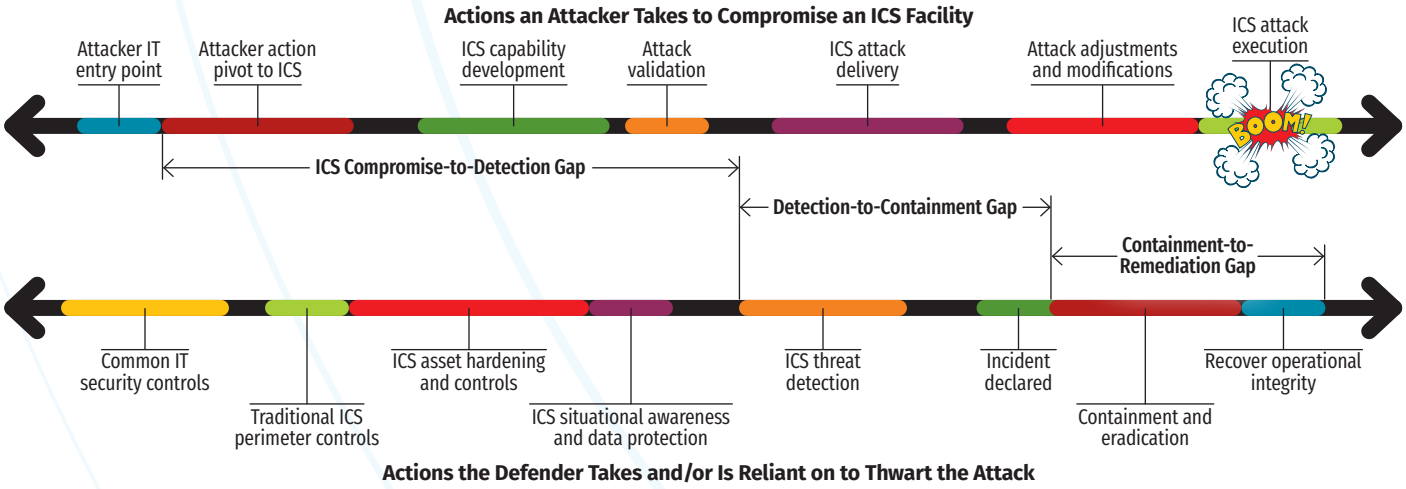


Figure 3. ICS Cyber Incident Timeline

Q: What is the average timeline your organization experiences across the incident life cycle?

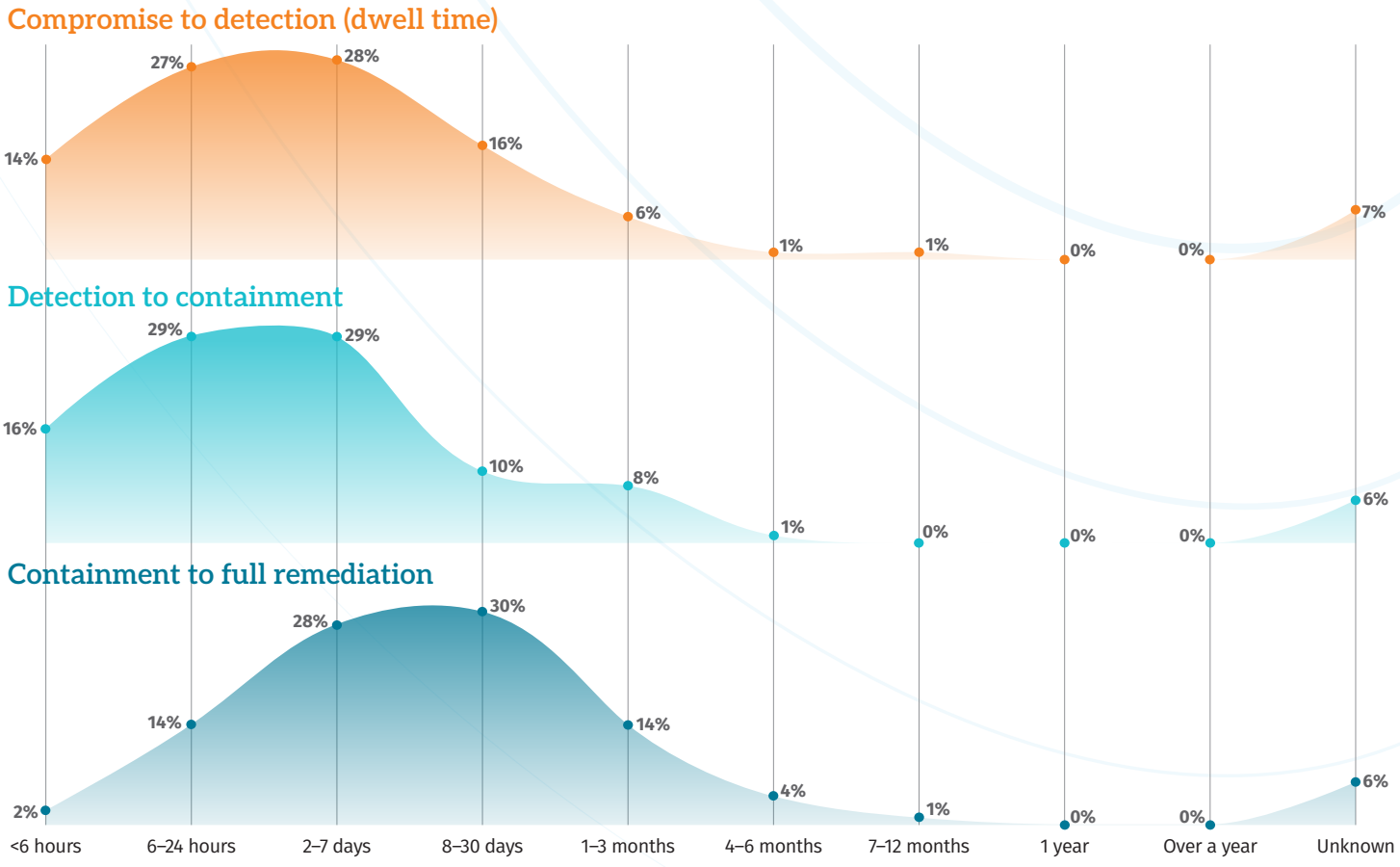


Figure 4. ICS Cyber Incident Timeline Distributions for 2026

Alarmingly, this is the first year where detection times for ICS/OT incidents *were slower*. Since 2024, more than 50% of respondents had detected these incidents in less than 24 hours (compared to 41% this year). In 2019, by comparison, 50% of incidents were detected within the first week. While 2026 is still a marked improvement from that 2019 data point, industry's advantage in this space has slipped from the previous two years.

This is the first year since we've been recording the data that ICS/OT detection times were slower. Combined with an alarming one in three respondents reporting an industrial cyber incident, the data suggests that ICS/OT environments are being targeted more often with more severe impacts.

How these 2026 incidents were detected may shine some light on why those times are slower. Dedicated ICS/OT visibility and threat detection platforms now lead all detection methods, finding 38% of reported incidents, a milestone for a capability that barely existed 10 years ago. IT-centric perimeter tools, such as firewalls, IDS, IPS, and UTM alarms, caught another 31% of incidents, the second-largest share. Detection was also a blended activity, with respondents stating that these incidents were found through human operator-observed errors (20%), periodic log or change management review (22%), and third-party external notification (22%). In other words, detection is not a single platform or single workflow, but needs to be thoroughly embedded into your incident response practices in order to be impactful.

Present: Understanding Current Threats and Detection Capabilities

For the past few years, our survey tracked an increase in ICS/OT-specific threat intelligence being used across critical infrastructure. This year, 74% of respondents reported leveraging threat intelligence—an increase from 67% last year and an all-time high across the State of ICS/OT Security surveys. And, similar to last year, almost every respondent who uses threat intelligence adjusts their defensive priorities based on the new information, as seen in Figure 5.

Q: Has your organization adjusted any defensive priorities in response to threat intel in the past year?

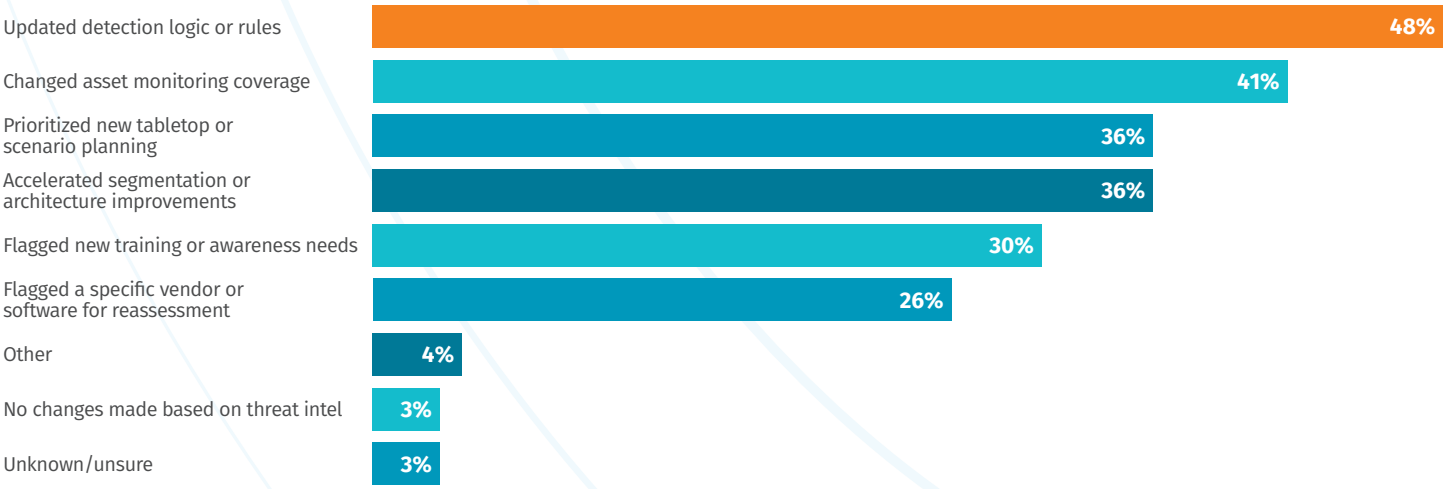


Figure 5. Breakdown of How Organizations Use ICS/OT Threat Intelligence to Improve Their Security Programs

Unfortunately, despite the use of threat intelligence to improve their programs, respondents are still unable to achieve full visibility across IT and OT systems, as outlined in the ICS Cyber Kill Chain white paper[3] (see in Figure 6). Similar to our observations last year, only 13% of respondents reported having full visibility alignment to track threat activity leaving a clear gap in coverage, while 46% reported partial visibility alignment. Ten percent of respondents reported that threat detection and visibility are siloed between IT and OT with no alignment whatsoever.



Figure 6. ICS Cyber Kill Chain Stages by Michael Assante and Rob Lee

[3] "The Industrial Control System Cyber Kill Chain," October 2015, www.sans.org/white-papers/36297

For those who had an industrial cyber incident in the past 12 months, the visibility data tells a more complicated story. Those with full alignment and visibility across IT and OT still had cyber incidents, but demonstrated the steepest drop in incidents from exploited firewalls and edge network devices—which should make sense: If you have IT-OT visibility, those edge devices and perimeters are closely monitored. The same could be said for unauthorized access, which also saw a steep drop in incidents from mature organizations to those with less IT-OT visibility as seen in Figure 7.

Q: What type of incident(s) occurred?

Select all that apply.

	Full visibility alignment	Partial visibility alignment	Minimal alignment	No alignment	Unknown/ unsure
Data loss or modification	12%	16%	7%	19%	11%
Safety or reliability event triggered	31%	17%	15%	10%	0%
Supply chain compromise (e.g., third-party breach, software tampering)	31%	22%	13%	19%	11%
Insider misuse or error	22%	26%	13%	19%	11%
Engineering system degradation or outage	38%	21%	15%	10%	22%
Unauthorized access (external actor)	12%	23%	28%	24%	33%
Exploitation of firewall or edge network device	19%	26%	27%	24%	11%
Shared IT/OT credentials (e.g., Active Directory) or identity compromise	38%	30%	23%	43%	22%
Ransomware	41%	24%	37%	29%	33%
Other	0%	3%	3%	5%	0%

Figure 7. Comparison of Types of Incidents from the Past 12 Months to IT-OT Visibility Across the ICS Cyber Kill Chain

When asked about the barriers to expanding ICS/OT visibility, which has clear benefits to decreasing incidents and related impacts, most respondents cited budget constraints as seen in Figure 8. This unfortunately may point to a disconnect between the technology, its benefits, and therefore the "return on investment." After all, a full 38% of incidents reported were detected using ICS/OT visibility and/or threat detection platforms, and organizations with full IT-OT visibility saw a different mix of incidents, with far less perimeter exploitation and unauthorized access.

Organizations with full IT-OT visibility saw a different, tamer incident mix: Perimeter exploitation fell to 19% of their incidents (compared to ~25% for everyone else) and unauthorized access fell to 13%. Meanwhile, the ICS-specific tooling behind that visibility caught more incidents than any other method this year (38%). Ironically, the tool that finds the most incidents is the one budgets still will not fund: 43% of respondents name budget as the No. 1 barrier to expanding ICS/OT detection and threat platforms.

Q: What is the primary barrier to expanding ICS/OT-specific cyber detection technologies and capabilities outlined in the previous question?[4]

Select all that apply.

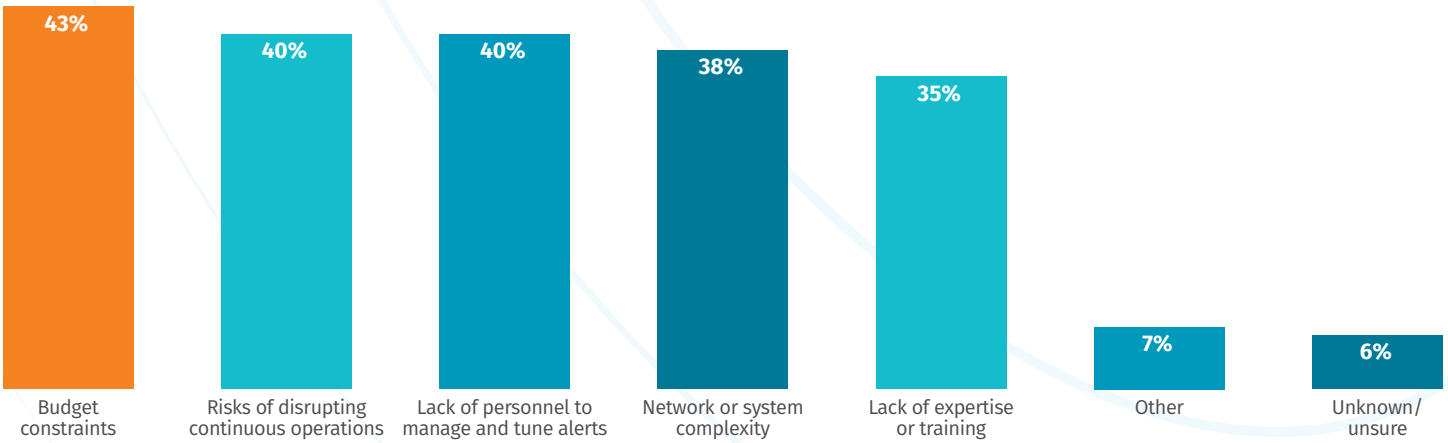


Figure 8. Reported Barriers to Expanding ICS/OT Specific Detections

[4] Previous question was: In your ICS/OT environment, how are cyber anomalies or potential security incidents most frequently detected today?

These threat and detection themes go hand in hand. As mentioned, a majority of respondents use ICS/OT-specific threat intelligence but how they act on it varies from "updating detection logic" to "providing new training and awareness." So, what about overall coverage to identify tactics, techniques, and procedures (TTPs) used by threats? Or the ability to collect data for forensics—including transient data? To further understand the limitations on ICS/OT detection, this year we asked specifically where the coverage gaps are as seen in Figure 9.

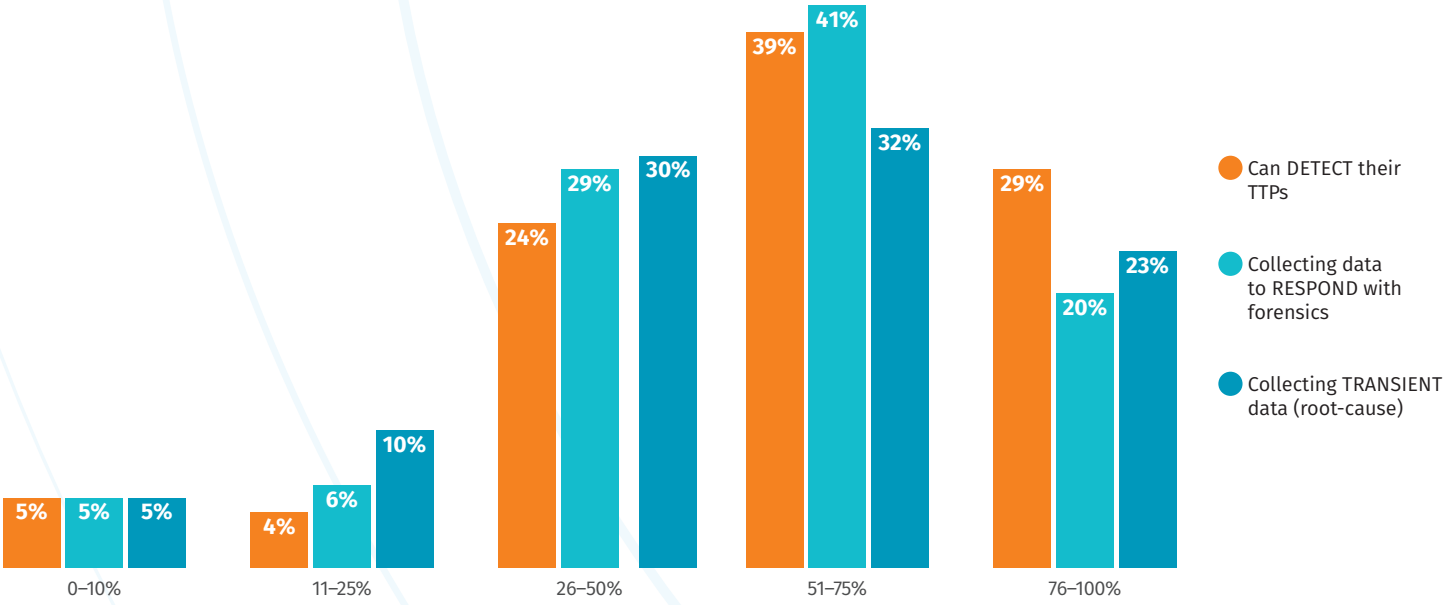


Figure 9. ICS/OT Visibility by Coverage Across Systems/Assets and the Ability to Perform Forensics and Pull from Transient Data Sources[5]

This unpacks a further view into the IT-OT visibility problem. Even respondents who have full alignment across the ICS Cyber Kill Chain have large gaps in the ability to collect and leverage detection. Not all sites are covered and, even where they are, the ability to perform forensics may be limited.

"If a tree falls in the forest and no one is there to hear it, does it make a sound?" The same could be asked of ICS/OT cyber incidents. Even as reported incidents jumped, 56% of respondents are unsure how anomalies in their environment would be detected today, and the average organization has detection coverage at only 61% of its sites. How many incidents went unreported this year because no data existed to see them?

---

[5] Note that the data for this figure is a combination of the following three questions: For the threats that have historically targeted your industry (e.g., PIPEDREAM, Crashoverride, Trisis, etc.) what percentage of your sites could you detect the majority of their Tactics, Techniques, and Procedure (TTPs) in the ICS/OT networks?; For the threats that have historically targeted your industry (e.g., PIPEDREAM, Crashoverride, Trisis, etc.) what percentage of your sites are you collecting the data required to respond and perform appropriate forensics prior to the attack in the OT networks?; At what percentage of your sites are you collecting transient data (e.g., network data such as what commands were sent from an HMI to controller or changes from EWS to logic) to performing root cause analysis in the event of an incident whether it is cyber or not?).

Expanding Detection: Industrial 'Human Sensors' for ICS/OT Networks

Our industry often thinks of ICS/OT visibility in terms of technology, but as reported in the 2025 SANS State of ICS/OT Security survey the most mature organizations involve operators in their annual exercises to help detect, respond, and recover from industrial cyber incidents.

This year, one in five respondents (20%) who suffered from an ICS/OT cyber incident said it was detected, at least in part, by human operators. Among organizations where operators play a role in detecting anomalies, 58% have formally trained them with an additional 30% saying they plan to provide such training in the next 12 to 24 months. Noting the limitations previously outlined with technology deployments and barriers, perhaps the "human sensor" can help augment traditional detection as asset owners and operators expand their IT-OT visibility.

These human sensor networks, however, also need a class of ICS/OT-specific knowledge workers. Recognizing the skill shortage across ICS/OT cybersecurity, this year we asked what organizations were doing to help build, manage, and retain their teams (see Figure 10).

Q: How is your organization primarily addressing the shortage of specialized ICS/OT cybersecurity personnel?
Select your top 3.

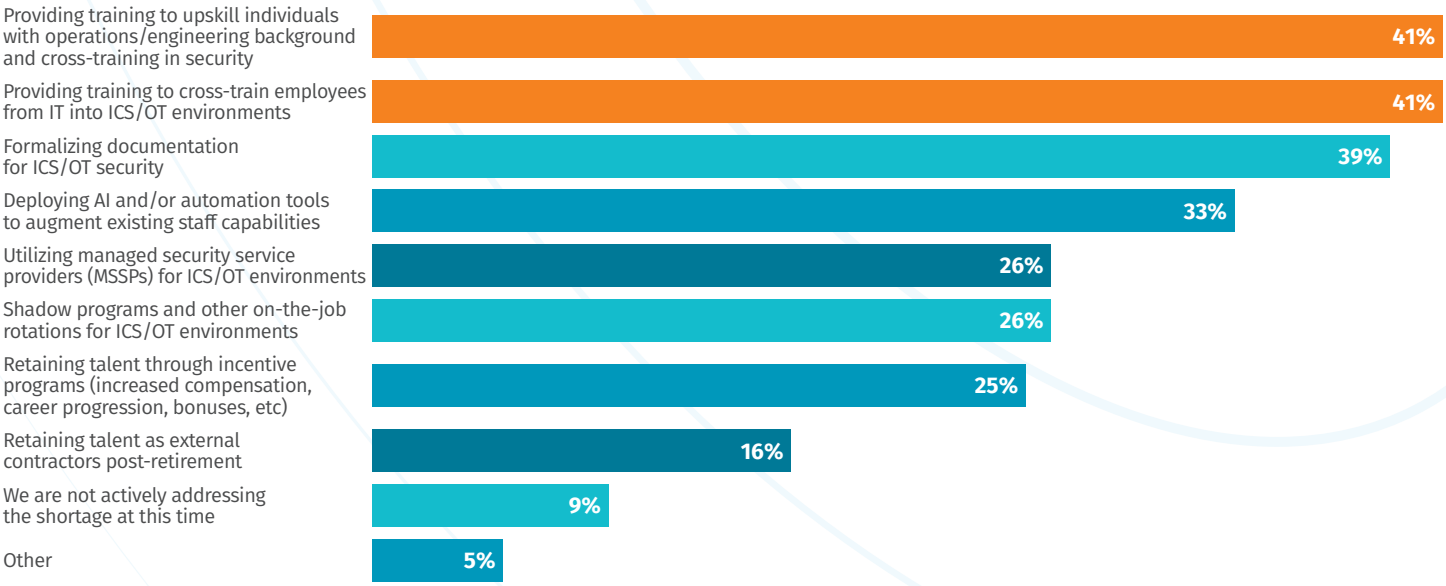


Figure 10. How Organizations Are Building, Managing, and Retaining ICS/OT Cyber Talent

The top three categories tell a compelling story on how organizations plan to upskill and cross-train across the IT-OT divide and formalize documentation for the ICS/OT security program. For many asset owners and operators, it may not be possible to hire an industrial security professional, so building those skills in-house may be the only option. That said, only a third of respondents (33%) said that ICS/OT-specific security certifications were important, outlining a potential gap between training and demonstrated skills for industrial security professionals.

Drilling further into the third of respondents (33%) who are deploying AI and/or automation tools to augment their staff, those specific use cases can be found in Figure 11. The most popular solutions look to alleviate defender pain points, like alarm fatigue to compliance reporting. None of these suggest AI would wholesale replace a human, but these tools can be used to further supplement an already tapped workforce as our industry continues to build ICS/OT skill sets, teams, and programs.

Q: In what capacity are you testing or deploying AI-based tools for ICS/OT security?

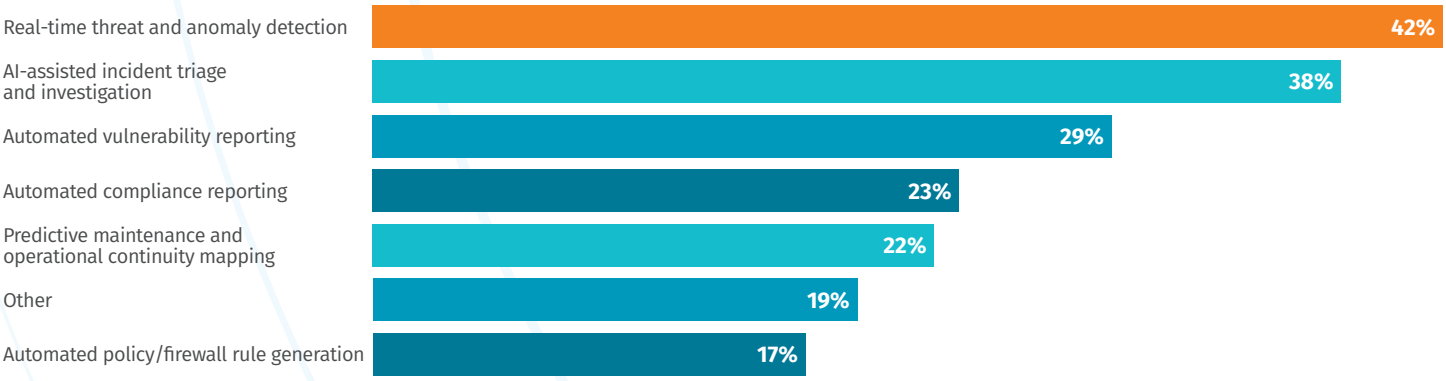


Figure 11. Respondents Who Are Using AI and/or Automation Tools to Augment Against the ICS/OT Cyber Skills Gap

---

Are we missing incentives for industrial security? As we cover in ICS418: ICS Security Essentials for Leaders, there are only so many ways to motivate teams. This year's data shows the imbalance: The top three workforce strategies are all training—upskilling (41%), cross-training (41%), and formalizing documentation (39%)—yet only one in four organizations (25%) use incentive programs such as compensation, bonuses, or career progression to keep the people they train, and only a third consider ICS/OT certifications important. Industry is building skills it has not committed to retaining.

Future: Preparing for Cyber Resilience, Response, and Recovery

After Volt Typhoon and similar threats, the industrial security community has been exploring more conversations on "presumed compromise." To support cyber-resilience initiatives, this year's survey examines the capabilities required to operate safely and reliably despite a compromise or event occurring. This section looks at the people, processes, and technologies to maintain operations during an ICS/OT cyber incident.

Manual Operations as a Fail-Safe: Cyber Resilience and Business Continuity

"Prevention is ideal, detection is a must." But detection without response is of little value. Over the years, we have explored response capabilities. What happens, however, when an incident prolongs recovery in ICS/OT networks? As explored previously, industrial incidents can stretch for months. The longest impact of reported incidents in this year's data took seven to 12 months to detect the incident, another seven to 12 months to contain and yet another seven to 12 months to remediate. The facility/system shutdown lasted for a year.

When all else fails, we may need to rely on manual operations to continue a physical process in the industrial environment. Unfortunately, only 15% of respondents were fully capable of sustaining critical operational processes and safe production in a "manual mode" (without centralized digital SCADA/DCS control) for more than 48 hours. While 34% of respondents believed they were partially capable, an alarming 40% did not know if they were or were not, highlighting a potentially dangerous gap in exercising capabilities and knowledge of facility, technology, and staffing capabilities.

Sustaining manual operations without centralized SCADA or DCS capabilities would be, for many industrial organizations, the equivalent of "limping along" during an incident. Keep the systems running, maintain a new normal. Yet only 15% of respondents believe they could do so for more than 48 hours, and 40% cannot say either way. An untested assumption is not a capability.

If a majority of respondents cannot fully sustain safe, critical operational processes, what happens next? Many organizations would need to think through recovery times and possibly examine full bare-metal restores of ICS/OT assets, networks, and system capabilities. The outlined recovery timeframes can be found in Figure 12. Nearly 27% believe they can bring their most critical facility/system back online within the first day. Another quarter (25%) believe they can do that in the first week.

Q: If you were to suffer from a cyber attack that required either reliance on "manual mode" or a complete full bare-metal restore of ICS/OT assets, network, and system capabilities, what is the quickest your most critical facility/system can be brought back online?

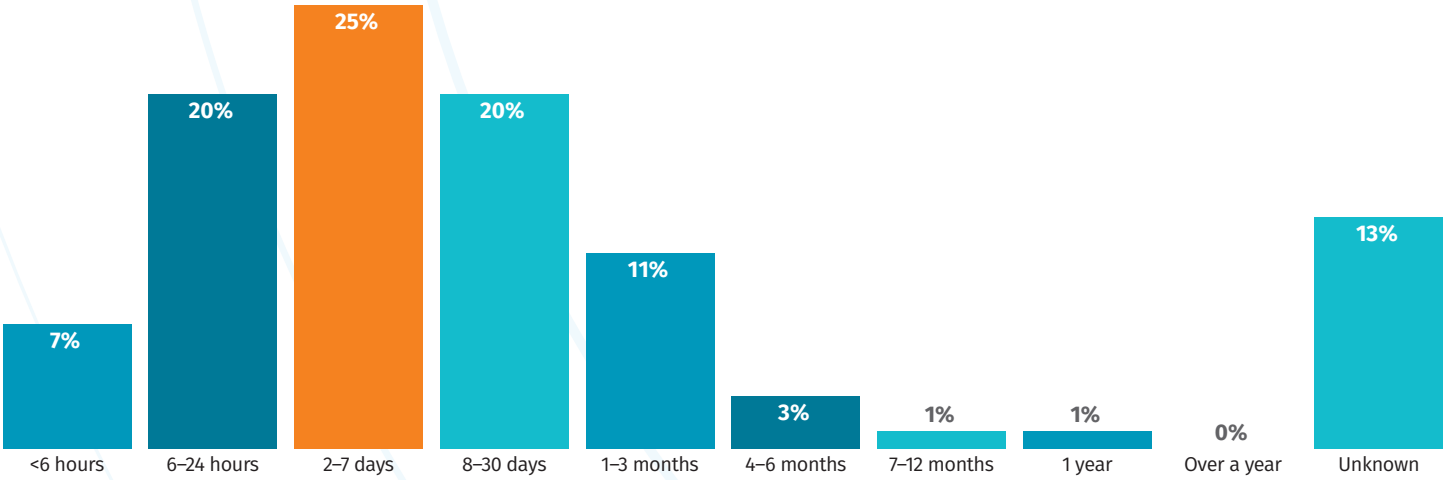


Figure 12. Recovery Timeframes for Manual Model or Bare-Metal Restoration

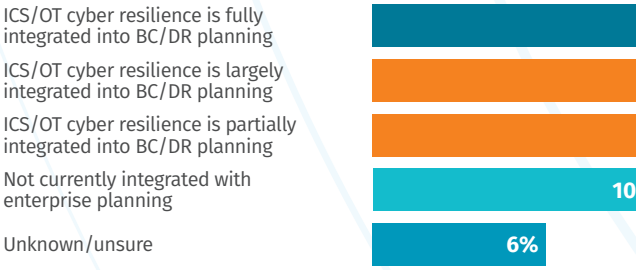
These times significantly improve under two conditions:

1. They test their plans at least annually
2. ICS/OT cyber resilience is embedded into business continuity and disaster recovery (BC/DR) programs

Organizations that did both of these things were recovery all-stars. An impressive 46% reported being able to bring their critical facilities/systems back online in the first day.

Unfortunately, these two skills are rare according to respondents. Only 16% of respondents have fully integrated their cyber activities into business continuity and disaster recovery operations and less than a third (29%) tested their resilience plans (including recovery, failovers, and engineering rebuilds) annually, as seen in Figure 13.

Q: Is your organization actively incorporating ICS/OT cyber resilience strategies into broader enterprise disaster recovery and business continuity planning?



Q: How often are ICS/OT-specific cyber resilience plans (e.g., recovery, failover, engineering rebuilds) tested or validated?

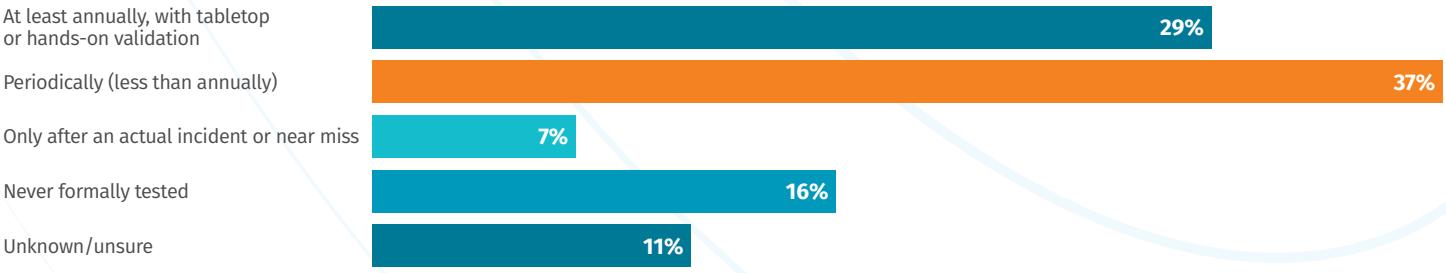


Figure 13. Comparison of How Cyber Resilience Is Tied Into Business Continuity and Disaster Recovery, as Well as Testing Cadence

BC/DR programs are extremely disciplined, and many industrial organizations have battle-tested capabilities. Think about how industries respond and recover from natural disasters (e.g., storms, earthquakes, wildfires)—that's business continuity and disaster recovery. It's something many critical infrastructure sectors prepare for and test. Integrating cyber resilience into BC/DR, as outlined previously, can drastically improve how we manage cyber incidents. For this year's theme, we drilled deeper into specific capabilities that should be integrated, as explored in Figure 14.

Q: Which of the following cyber resilience activities are integrated into your organization's BC/DR planning for ICS/OT environments?

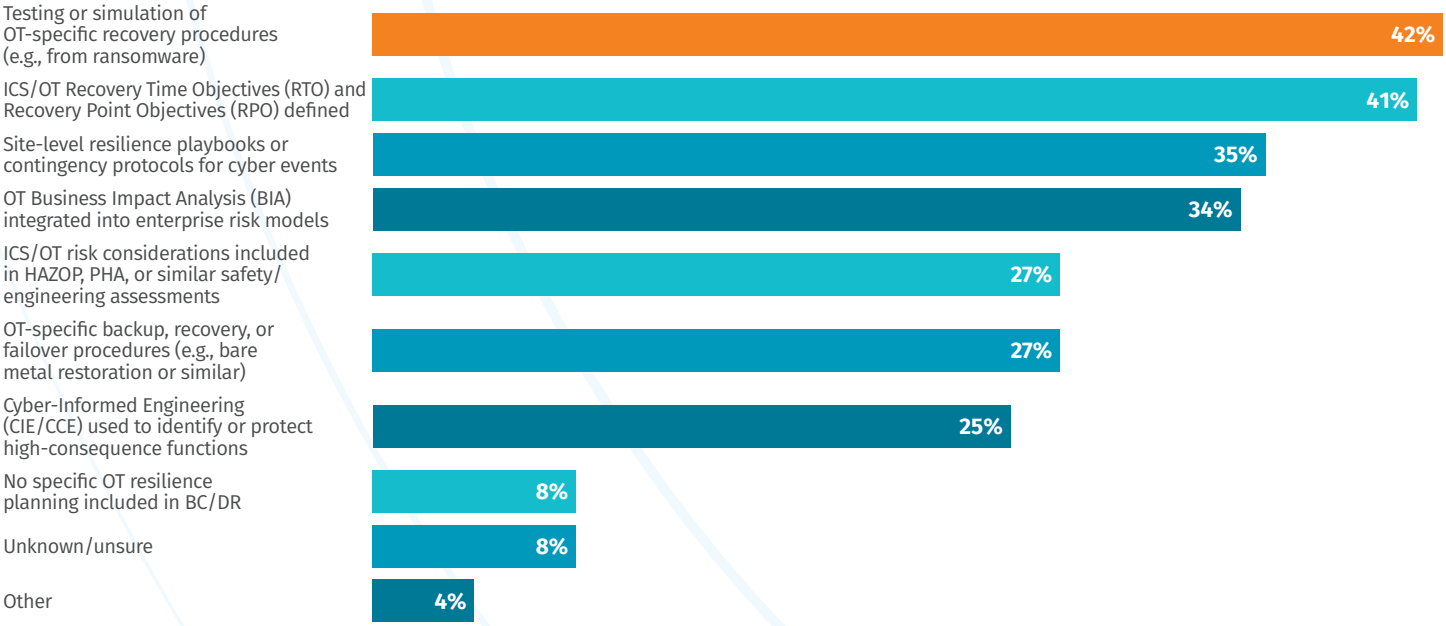


Figure 14. Cyber Resilience Activities Integrated into Organizational BC/DR Planning for ICS/OT Environments

There are some solid foundations being built within cyber-resilience practices and BC/DR programs, including testing recovery procedures, recovery objectives, and site-level resilience playbooks.

And this cross training could be critical during an incident and recovery. When asked to what extent their OT security or operational response capability relies on undocumented "key person" expertise (i.e., institutional knowledge held by a small number of veteran employees) 25% of respondents believe that the loss of one or two key individuals would cause severe operational risk. Another 43% said a similar loss would cause delays, but some documentation exists. Only 5% of respondents felt comfortable that there was no such reliance in their ICS/OT security or response program.

A majority of respondents (68%) report that the loss of one or two key individuals would delay or cause severe operational risk for ICS/OT security and incident response and recovery. Only 5% reported no such reliance. The institutional knowledge in a subject matter expert's head is single-point-of-failure infrastructure. Succession planning is incident response planning.

Global Regulations and Geopolitical Threats: Impacts to the Supply Chain

In the 2025 State of ICS/OT Security survey, we discovered that there were two major drivers for ICS/OT security programs: regulations and threats. Over the past year, both categories seemed to focus on one specific topic: the supply chain. Regulatory efforts like the EU Cyber Resilience Act (CRA), the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards, and the US Securities & Exchange Commission (SEC) have all incorporated elements of supply chain management. Meanwhile, geopolitical conflicts have led to increased threat activities focusing on supply chain compromise. These two forces may collide in the next 12 to 24 months to demand ICS/OT security teams evaluate and manage risks associated with how goods and services are procured, tested, and operated. When asked about supply chain program management, only 20% of respondents had a fully functional supply chain cyber risk management program as seen in Figure 15.

Q: Over the next 24 months, a combination of global regulations (e.g., EU's NIS2 and CRA, updates to NERC CIP, SEC guidelines, etc.), geopolitical conflicts, and cyber supply chain incidents may require additional scrutiny and maturity around supply chain cyber risk. Do you have a supply chain cyber risk management program that can evaluate and mitigate these risks?

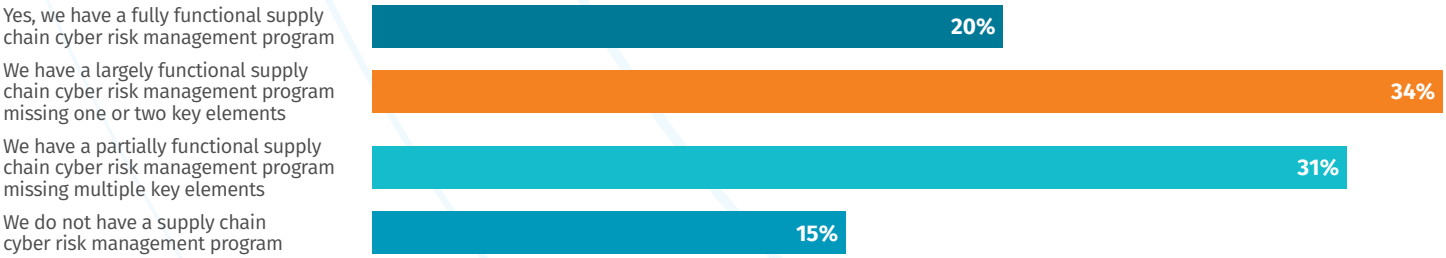


Figure 15. Capability Maturity for Supply Chain Risk Management

For the majority of respondents without a fully functional program, the most common missing elements include:

- Prioritization of the vendor by criticality of reliable operations (34%)
- Notifications for vendor cyber incidents (33%)
- Notifications for vendor vulnerabilities for products/software in ICS/OT environments (33%)
- Evaluation for bills of materials of key asset elements (hardware and/or software) (33%)
- Safeguards against counterfeit or compromised software, hardware, and services (30%)

These gaps can lead to some serious consequences. Let's play out the worst-case systemic risk scenarios for industrial organizations. These could include escalations from geopolitical tensions, war, or sanctions and bans on specific companies—or a catastrophic vendor cyber incident that impacts their ability to supply or support goods and services. Pulling this thread, we asked respondents if their primary ICS/OT automation vendor "completely disappeared tomorrow," how long could their facilities safely sustain continuous production. As seen in Figure 16, only 10% said they could operate indefinitely. A majority of respondents (58%) would shut down or be unable to operate within the first year.

Q: In a "worst-case" systemic risk scenario (e.g., severe geopolitical sanctions, bankruptcy, or a catastrophic vendor breach), if your primary OT automation vendor completely disappeared tomorrow, how long could your facility safely sustain continuous production?

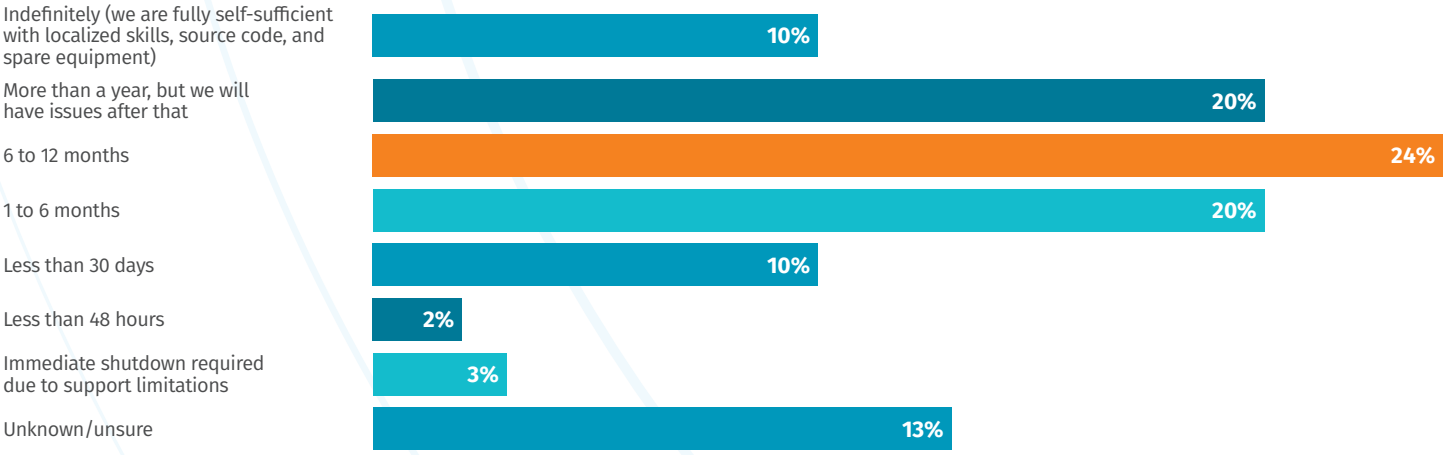


Figure 16. Estimated Time to Safely Sustain Continuous Production in the Event of a Systemic Risk Scenario

The underlying data here is extremely interesting. When compared to capabilities asked about in this year's survey (e.g., IT-OT visibility, BC/DR integration, and supply chain management), roughly half, regardless of capability level, will always be unable to operate continuously after the first year. That said, what *does* change as we increase these capabilities is the ability to operate indefinitely. For example:

- 18% of participants with a fully functional supply chain cyber risk program could operate indefinitely in this worst-case scenario, a near two-fold increase.
- That jumps to 20% for respondents that have a fully integrated BC/DR and cyber-resilience program.
- Meanwhile, those with fully aligned IT-OT visibility take the prize: 25% could operate in this worst-case scenario indefinitely.

All of this represents one consistent pattern: The more you know your systems, the more likely you are to handle bad days.

Finally, in this worst-case scenario, we wanted to ask the respondents that could not operate indefinitely: *How long would it take to transition their critical processes to an alternative automation vendor's ecosystem?* Unsurprisingly, this is not an overnight activity (as seen in Figure 17) with 42% saying it would take one to three years for a transition, 28% reporting three to five years, and 13% replying that it would take more than five years. For 6% of respondents, it would be impossible without a new facility rebuild or massive capital expenditure. Half of that group also reported they could not operate within six months of losing their primary vendor.

Q: How quickly could you realistically transition your critical processes to an alternative automation vendor's ecosystem?

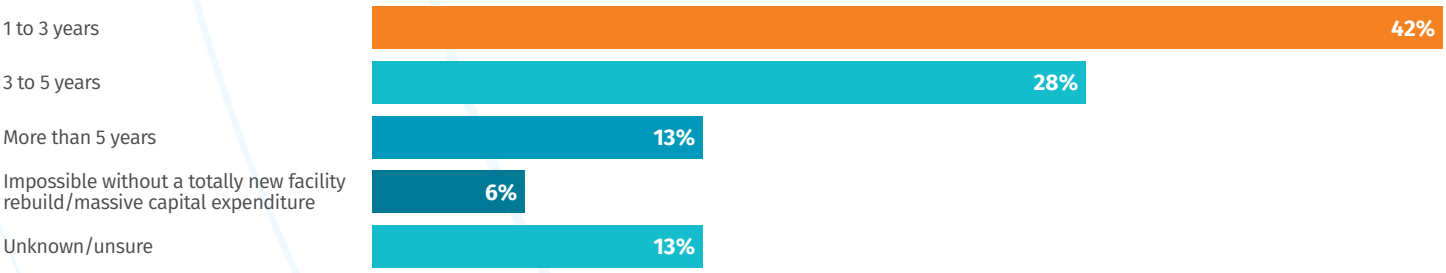


Figure 17. Automation Vendor Transition Timeframes

As before, the numbers here improve if more capabilities are present across their ICS/OT security program. The respondents that can transition the quickest have both full IT-OT visibility alignment *and* BC/DR integration with cyber-resilience practices, jumping to 56% that can migrate within one to three years compared to their peers.

The survey posed a worst-case systemic risk scenario: Severe geopolitical sanctions, a catastrophic vendor breach, or outright bankruptcy takes your primary OT automation vendor off the board tomorrow. Only 10% of organizations could sustain production indefinitely, and 58% would be down within a year. A fully functional supply chain cyber risk program nearly doubles the odds of surviving it. Governments already treat supply chain sovereignty as national security, and sanctions or conflict could trigger this scenario without warning. Nine out of 10 industrial operators have no indefinite answer for it.

Conclusions and Next Steps for Industry

“Prevention is ideal, detection is a must.” That motto has guided our community for two decades, and this year, 696 of your peers told us it is no longer sufficient. One in three respondents suffered an ICS/OT cyber incident. Detection times slowed for the first time since we began recording them. And when incidents arrived, they brought longer downtime, higher safety impacts, and detection led by ICS/OT-native platforms (38%), with the IT perimeter (31%) and trained operators (20%) close behind.

Detection without response and recovery is of limited value. Cyber resilience is the discipline that fills the gap: maintaining safe, reliable operations while the incident is still happening. Measured that way, the industry has work to do. Only 15% of respondents could sustain manual operations beyond 48 hours. Only 16% have fully woven ICS/OT cyber resilience into business continuity and disaster recovery. And 40% could not say whether their most critical processes would survive without their control systems, which may be the most alarming number in this report.

The data also shows us what works. Organizations that test their resilience plans annually and embed them in BC/DR
recovered same-day at nearly twice the rate of their peers. Those with full IT-OT visibility were two and a half times more likely to keep operating indefinitely in a worst-case supply chain scenario. The capabilities behind those numbers are ordinary ones: testing cadences, documentation, cross training, and integration with disciplines industrial operators already trust. Storms, earthquakes, and wildfires taught this industry business continuity. Cyber incidents deserve the same muscle memory.

So where do we go from here? Three moves stand out from this year's data:

1. Test your resilience plans at least annually, with the operators who would actually run manual mode.
2. Integrate ICS/OT cyber resilience into the BC/DR programs your organization already exercises.
3. Map your dependencies, on key people and key vendors alike, before a worst-case scenario does the mapping for you.

Ultimately, this year's theme was a question: What do we do when things go wrong? The honest answer from this year's data is "less than we should, and now we can prove it." If you want to measure yourself and compare to our data, check out our SANS ICS 2026 Cyber Resilience Scorecard in the appendix. None of this requires a new framework. Leveraging the SANS Five ICS Critical Controls (working within an existing or growing industrial security program), security leaders and practitioners can turn this year's data into actionable guidance. The organizations that thrive in the next decade of industrial cyber threats will be the ones that know their systems, test their plans, and treat resilience as an operational skill rather than a paperwork exercise. The benchmarks in this report are the starting line. We look forward to measuring the progress in 2027!

Expert Corner

"The 2026 survey found shared IT/OT credential or identity compromise in 31% of reported ICS/OT incidents and firewall or edge-device exploitation in 24%. IT network intrusions continue to reach into OT, where attackers inside control systems commonly misuse legitimate ICS/OT network protocols and control system functionality for impact without the need for traditional malware, vulnerabilities or exploits. ICS/OT defense controls are different than in IT, and they have different missions.

This reinforces SANS Control 3 (ICS Network Visibility and Monitoring) and Control 1 (ICS-Specific Incident Response): Detect ICS/OT threats and practice engineer-led responses and recoveries through realistic OT specific tabletop exercises.

A rapid and effective action for any ICS/OT sector from the 2026 ICS/OT cybersecurity survey is to conduct ICS/OT-specific tabletop exercises at least annually, quarterly for higher-risk and mature operations. Test industrial incident response, and engineering recovery of critical engineering assets (PLCs, RTUs, HMIs, etc.), and apply those lessons learned collaboratively between IT and OT teams.



Dean Parsons

Principal SANS Instructor and
CEO and Principal Consultant at ICS Defense Force, Inc.

COURSES TAUGHT

ICS515:
ICS Visibility, Detection, and Response

ICS418:
ICS Security Essentials for Leaders

VIEW PROFILE

Demographics

The 2026 SANS ICS/OT Security survey received close to 700 qualified responses from IT and security professionals actively working in security roles. Figure 18 provides the demographic details.



Figure 18. Demographics of Survey Respondents

Appendix: The SANS ICS 2026 Cyber Resilience Scorecard

Score your organization against your peers. Answer each question below as your program stands today, then compare against the 2026 benchmark, drawn from this survey's validated data. In a year when one in three respondents reported an ICS/OT incident and detection times slowed for the first time on record, the questions are organized by the Five ICS Cybersecurity Critical Controls,[6] the framework most industrial security programs already use to structure priorities and budgets. A 12th question covers the 2026 supply chain scenario beyond the controls.

THE SANS ICS 2026 CYBER RESILIENCE SCORECARD

CRITICAL CONTROL	SELF-ASSESSMENT QUESTION	2026 BENCHMARK
01 ICS-specific incident response	**Q1. How often are your ICS/OT-specific resilience and response plans tested or validated?** ☐ At least annually ☐ Less than annually ☐ Only after an incident ☐ Never ☐ Unknown	29% test at least annually. Those who test and integrate with BC/DR recover same-day at 46%, vs. 27% overall.
	Q2. Once an ICS/OT incident is detected, how quickly can your organization contain it? ☐ Under 24 hours ☐ Days ☐ Weeks ☐ Months ☐ Unknown	45% of 2026 incidents were contained within 24 hours of detection.
	Q3. To what extent does your OT security and response capability rely on undocumented expertise held by one or two individuals? ☐ Heavily ☐ Moderately ☐ Minimally ☐ Not reliant ☐ Unknown	68% report the loss of one or two key people would cause delays or severe operational risk; 5% report no reliance.
02 Defensible architecture	**Q4. Are your critical processes capable of sustaining safe production in manual mode, without SCADA/DCS control, for more than 48 hours?** ☐ Fully ☐ Partially ☐ Not capable ☐ Unknown	15% are fully capable; 40% do not know.
	Q5. Is cyber-informed engineering (CIE/CCE) used to identify or protect your high-consequence functions? ☐ Yes ☐ No ☐ Unknown	One in four organizations apply CIE today.
03 ICS network visibility and monitoring	**Q6. What level of visibility alignment exists between your IT and ICS/OT environments across the ICS Cyber Kill Chain?** ☐ Full ☐ Partial ☐ Minimal ☐ None ☐ Unknown	13% report full alignment. Those organizations saw far less perimeter exploitation and unauthorized access.
	Q7. How are cyber anomalies or potential incidents most frequently detected in your ICS/OT environment today? ☐ ICS/OT-native platform ☐ IT perimeter tools ☐ Operators ☐ Log review ☐ Unknown	Actual 2026 incidents were detected by: ICS/OT-native platforms 38% (the No. 1 method), IT perimeter tools (31%), trained operators (20%).
	Q8. What is your expected compromise-to-detection time for an intrusion in your ICS/OT networks? ☐ Under 24 hours ☐ Days ☐ Weeks ☐ Months ☐ Unknown	41% of 2026 incidents were detected within 24 hours, slower than prior years.
04 Secure remote access	**Q9. Are remote access paths into your ICS environment inventoried, and what proportion use brokered connections and unique credentials?** ☐ All ☐ Most ☐ Some ☐ None ☐ Unknown	The 2026 survey measured the consequence: shared IT/OT credential compromise tied ransomware as the No. 1 incident type (31%), and unauthorized external access reached 23%.
05 Risk-based vulnerability management	**Q10. Do you receive vulnerability notifications from vendors for the products and software in your ICS/OT environment?** ☐ Yes ☐ Partially ☐ No ☐ Unknown	33% lack vendor vulnerability notifications.
	Q11. Can your supply chain cyber risk management program evaluate and mitigate vendor-driven risk today? ☐ Fully ☐ Largely ☐ Partially ☐ No program	20% report a fully functional program. Threat-intel users act on intel inside the fence (under 3% made no change), yet only 26% have used it to reassess a vendor.
BONUS 2026 supply chain scenario	**Q12. If your primary OT automation vendor disappeared tomorrow, how long could your facilities sustain production?** ☐ Indefinitely ☐ More than a year ☐ Months ☐ Weeks ☐ Unknown	10% could operate indefinitely; 58% would be down within a year. A fully functional supply chain program nearly doubles the odds of operating indefinitely (18% vs. 9.5%).

[6] "The Five ICS Cybersecurity Critical Controls," SANS Institute Whitepaper, November 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls. Answer scales are condensed from the survey's response options. The 2026 survey measured outcomes and capabilities, not the controls themselves; question 9 is scored against incident evidence rather than a capability distribution.

Appendix: An Industrial Cyber Leader's Guide to ICS/OT Insights

For the first time ever, a separate leadership edition of the SANS State of ICS/OT Security Survey was sent to senior industrial executives, primarily CISOs, CSOs, and security VPs. Their answers provided a unique view of how industrial cyber resilience is being governed, as well as some blind spots when compared to the broader survey. Overall, security leaders highlighted realistic concerns for our industry, but on the question that mattered most—Could operations survive a compromise?—they were directionally more optimistic than the practitioners they lead in the field.

Where Leaders and the Field Agree, and Where They Don't

On the fundamentals, leaders and the field largely agree, which is what makes the divergence credible rather than noisy. Leaders report fully integrated BC/DR at 21%, statistically in line with the field's 16%, and their candor on visibility runs ahead of the aggregate. This is a leadership cohort that knows where its programs are immature and says so.

The divergence concentrates on operational continuity. Leaders universally expect operations to ride out a compromise, while the field—the population that would execute that expectation—is split between partial capability and honest uncertainty. Forty percent of practitioners in the field just did not know if they could.

Pair that with the validation gap (14% routine technical validation on capabilities) and the exercise roster (frontline operators required in 58% of incident response programs), and a pattern emerges: The continuity assumption is held most strongly by the people furthest from the equipment, tested least by the programs they fund, and staffed thinnest at the layer that would deliver it. Combined with an alarming key-person risk from the broader survey, where (68%) report that the loss of one or two key individuals would cause moderate to severe operational risk for incident response and recovery, and that pattern becomes even more alarming. We're depending on a workforce that needs more tools, training, and succession planning.

Key Findings

Not one leader expects a production halt.

Asked how operations would fare if enterprise IT were fully compromised, every leader who answered expects production to continue: **38%** indefinitely on islanded ICS/OT, **62%** temporarily on manual controls and workarounds. Zero foresee degradation or a halt. The field tells a different story: Only **15%** of practitioners call their processes fully capable of sustained manual operations, **40%** cannot say either way, and of those with an opinion, roughly one in five say not capable. Either the broader survey demonstrates a more pessimistic view, or leaders should battle-test their assumptions.

The confidence is not coming from testing.

Albeit a smaller sample size, only **14%** report routine technical validation, such as ICS-specific threat hunting or safe red/purple teaming, across their environments; **43%** describe activity that is ad hoc or missing major elements. Confidence in manual-mode continuity paired with limited technical validation means the continuity plan is, for most, an untested assumption.

The response bench is IT-heavy, by the leaders' own account.

When leaders list who is explicitly required in ICS/OT tabletop exercises, enterprise IT security leads at **83%** and the ICS/OT security team follows at **71%**. Plant managers and frontline engineers and operators, the people who would actually run the manual operations, are required in only **58%** of programs. The plan depends on people who are not consistently in the drill.

Where leaders are more candid than the field: visibility.

Only **7%** of leaders claim fully implemented visibility across the ICS Cyber Kill Chain, **46%** describe partial coverage, and **25%** concede minimal or IT-only visibility. The broader survey population claims full visibility at **13%**. The instruments differ, so read the comparison directionally, but the leadership answers suggest the corner office may hold a more sober view of the visibility gap than the aggregate self-assessment does.

Building Resilience: What Industrial Cyber Leaders Should Do Next

Three priorities from this year's leadership questions and the broader survey point to actionable next steps for any industrial cyber program:

1. Test the continuity assumption before it becomes critical.

Zero leaders expect an operational halt from a cyber event, while only 14% run routine technical validation on ICS/OT capabilities. Leaders should commission a technically validated manual-operations exercise, not a tabletop. This is the same discipline the full report's data rewards: Organizations that test resilience plans annually and integrate them with BC/DR recovered same day from cyber incidents at nearly double the rate of their peers.

2. Put the plant (or field) techs on the response roster.

If manual operations are the fallback, the people who run them belong in every exercise. Make plant/field managers and frontline engineers required participants, not invitees, and measure the drill by whether the plant could maintain operations for a prolonged period of time. The survey data adds urgency: Human operators observed system errors in 20% of this year's real incidents. These are our "human sensors" for ICS/OT security and they should be trained appropriately.

3. Fund visibility where incidents actually get caught.

Leaders' own answers concede the visibility gap (7% full Cyber Kill Chain coverage). The survey data shows what closing it buys: ICS/OT-native platforms caught more of this year's incidents than any other method (38%), while budget remains the No. 1 barrier practitioners name (43%). Visibility investment is the leader-controlled lever in this dataset, and it maps directly to ICS network visibility and monitoring among the Five ICS Cybersecurity Critical Controls.

Conclusion

As attackers continue to target industrial operations, cyber resilience has become even more relevant and needed than ever. This year's survey tackles some heavy hitting questions about our preparedness and capabilities to continue operations despite a cyber incident occurring. "Riding through" and "manual operations" are capabilities that need to involve both security leaders and field practitioners. Diving deep into the data has shown there are misconceptions across both audiences that need to be addressed. The full report includes a SANS 2026 Cyber Resilience Scorecard that can help break down these silos and provide meaningful benchmarks across 12 questions. It's a great place to start for organizations that want to make a difference in how they measure and improve their industrial cybersecurity program.

Sponsor

SANS would like to thank this survey's sponsor:



SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership, and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles, and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about sponsorship opportunities for research, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.

© 2026 SANS™ Institute. All Rights Reserved.