SANS

Analyst Program

Survey

A SANS 2021 Survey: OT/ICS Cybersecurity

Written by **Mark Bristow**

August 2021

tenable

Executive Summary

The operational technology (OT)/industrial control system (ICS) security world continually adapts to meet new challenges and threats. This 2021 SANS OT/ICS Cybersecurity Survey explores how OT defenders across all industries meet these challenges and looks to areas where we can place more emphasis to help defend our critical infrastructure moving forward. This year's survey focuses on actual and perceived risks, threats, information sources, and operational implementation challenges, as well as levels of investment in this important topic. This year, the results clearly show the rise of ransomware impacting critical infrastructure as a significant threat and an area of concern among respondents.

OT cybersecurity practitioners and boardrooms keep threats and perceived risks front of mind. Recent incidents such as the Colonial Pipeline ransomware attack and the JBS Foods ransomware highlight the complex threat environment these systems face. The results confirm this, with ransomware and financially motivated cybercrimes topping the list of threat vectors that cause respondents most concern, followed by the risk from nation-state cyberattacks (43.1%). Most interestingly, the elevation of non-intentional threat vectors made for a combined 34.5% of the total choices for top three threat vectors.

The threat and risk landscape remains somewhat opaque, and incidents often go unreported and insufficiently investigated. When asked to identify the most at-risk sector, most sectors did not choose their own. When asked about vulnerabilities in their sector, however, they reported significant challenges. Incident self-awareness in the form of monitoring and detection also rank relatively low, with only 12.5% of respondents confident they had not experienced a compromise in the past year and 48% of survey participants not knowing whether they suffered an incident. Connectivity to external systems continues as the overwhelming root cause of the incidents, an indication that organizations still fail to follow network segmentation best practices. Additionally, 18.4% of initial infection vectors report leveraging the engineering workstation, a highly concerning fact because few correlate cyber and process data to analyze system breaches. Publicly available channels grossly underreport incidents; for example, almost all respondents indicated having at least one incident, with 90% having some level of impact on the process, yet only high-profile incidents such as Colonial make headlines.

The OT cybersecurity landscape has changed significantly in the past two years. We have seen significant attention and overall growth of investment in securing our critical ICS/OT systems, but we still need some progress in key areas. Key industry-wide insights from this survey include:

- Steady growth in ICS-focused cybersecurity positions
- Overall increase in budget allocation for ICS cybersecurity efforts
- Steady increase in the influence of regulatory regimes to drive cybersecurity investments
- Increase in cloud adoption (and use primary for operational outcomes)
- Significant adoption of MITRE ATT&CK® framework for ICS (given its relatively recent release)

- Continued adoption of ICS monitoring technologies and threat-hunting methodologies
- Continued support for patch management (by most) and vulnerability assessment processes if not evenly applied
- Asset inventories continuing to challenge most organizations, with only 58.2% having a formal process (progress, but not enough progress)

Overall, significant progress has occurred in the areas of professionalizing the workforce, OT monitoring, analysis, assessment, remediation, and response. However, although we still need improvement in inventory and asset management and OT segmentation/system interconnectivity, the past two years have demonstrated great progress (with more to come).

Introduction

The 2021 SANS ICS/OT survey received 480 responses, an increase of 42% over the 2019 survey. Respondents represent a wide range of industry verticals,[1] with additional respondents sub-classifying into 62 unique groups, from gaming to aviation to space systems and payment systems.

The survey represents a balanced view across the industry, capturing responses from those whose primary responsibilities emphasize ICS operations or IT/business enterprise. Most survey respondents spend most of their time focused on ICS cybersecurity. Half of those (50%) report that they spend 50% or more of their time on ICS cybersecurity, as opposed to the 2019 survey where 45% of respondents reported that they spend at least 50% of their time in OT/ICS cybersecurity. In 2021, more than 50% have roles that emphasize ICS operations, either solely or in conjunction with IT/business enterprise. See Figure 1.

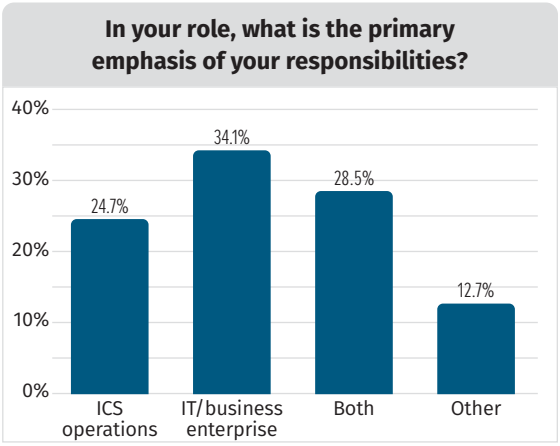


Figure 1. IT/OT Role Focus

This represents a significant increase in the number of ICS cybersecurity professionals in a relatively short period of time. While some have focused on ICS cybersecurity for 15+ years, we now see increasing dedicated resourcing and attention from operators in this space who recognize the importance of these OT-focused roles. This trend might directly result from the number of respondents holding ICS-specific cybersecurity certifications; 54% respondents hold a certification in the 2021 survey versus just 38% in 2019. This investment in certification indicates that the industry recognizes and highly values certifications, particularly SANS certifications. See Figure 2.

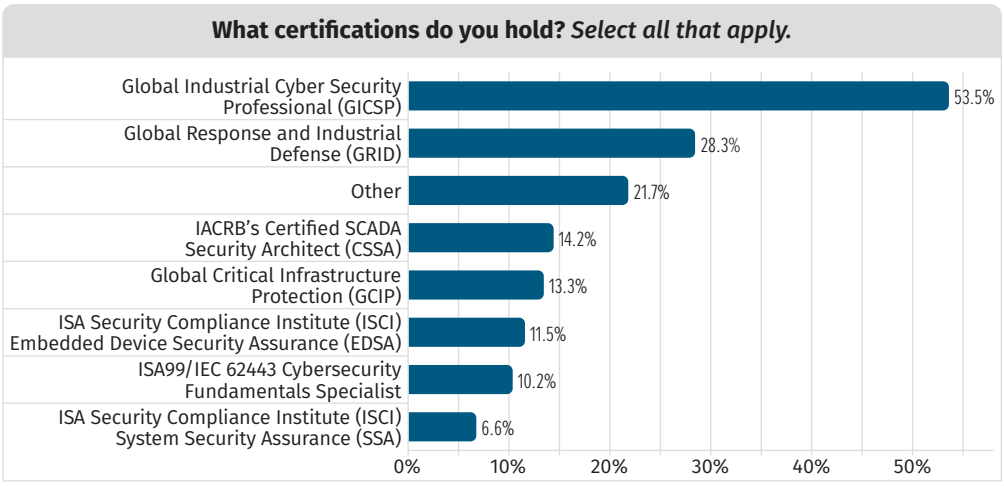
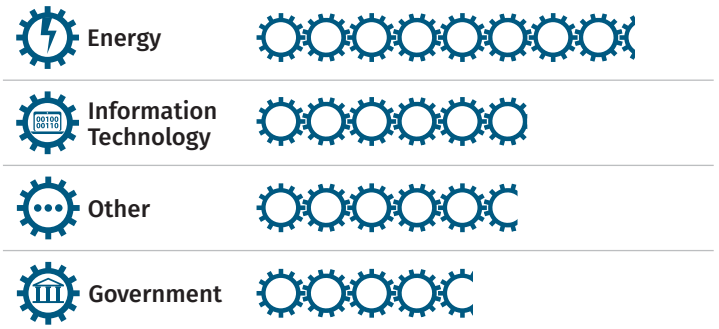


Figure 2. Respondents' Certifications

[1] Survey options based on CISA's critical infrastructure sector definitions, with some modifiers for ICS-specific elements, www.cisa.gov/critical-infrastructure-sectors

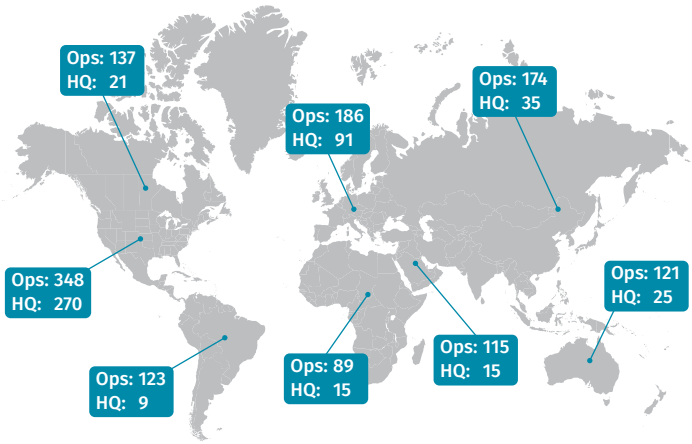
Figure 3 provides a snapshot of survey respondents' demographics.

Top 4 Industries Represented



Each gear represents 10 respondents.

Operations and Headquarters



Organizational Size

Each building represents 10 respondents.

Figure 3. Survey Demographics

The Business of ICS Security

Organizations now recognize the security of their ICS assets as fundamental to their business, and they expressed as their number one concern ensuring the reliability and availability of control systems. See Table 1.

Somewhat surprisingly for industries with a historical focus on safety, ensuring the health and safety of employees and off-site personnel fell in importance from second to fifth place. Preventing financial loss also dropped in importance, another surprising fact since many utilities are investor owned and responsible to shareholders. The global COVID-19 pandemic may have impacted these perspectives, with staffing greatly reduced over the past two years and a financially constrained marketplace resulting from a shift to minimize long-term business risk so as to weather the COVID-spurred slowdown.

Table 1. Top Business Concerns

	2021		2019		Change in Rank
	%	Rank	%	Rank	
Ensuring reliability and availability of control systems	50.3%	1	52.3%	1	—
Lowering risk/Improving security	45.5%	2	34.8%	3	+1
Preventing damage to systems	27.2%	3	27.7%	4	+1
Securing connections to external systems	23.3%	4	11.7%	10	+6
Meeting regulatory compliance	19.8%	5	22.3%	5	—
Preventing information leakage	18.1%	6	14.8%	9	+3
Ensuring health and safety of employees	17.7%	7	42.2%	2	-5
Protecting external people and property	15.2%	8	20.7%	6	-2
Creating, documenting and managing security policies and procedures	13.1%	9	8.2%	13	+4
Protecting company reputation and brand	11.6%	10	17.6%	8	-2
Providing or coordinating employee cybersecurity education and awareness programs	11.2%	11	10.5%	11	—
Preventing company financial loss	7.9%	12	18.8%	7	-5
Protecting trade secrets and intellectual property	6.0%	13	7.8%	14	+1
Minimizing impact on shareholders	3.3%	14	9.8%	12	-2

The greatest challenges facing OT security relate, as always, to people, process, and technology. Respondents' answers relatively balance across these three areas with regard to what they consider the biggest challenges their organizations face. See Figure 4.

Figure 4. OT Challenges

- **Technology—**Technical integration represents a challenge. Organizations need to ensure that technical implementations more effectively integrate legacy OT environments with modern security technologies. Innovation from solution providers can support in this area.
- **People—**We face a significant OT security labor shortage. Although this survey shows that we currently have more OT security professionals than ever, we still need to do more to bring additional professionals into the industry to perform this critical work. We need investments in formal and informal training and professional development to train and re-skill the workforce to meet this surging demand.
- **Processes—**Security leaders need to develop a culture of mutual understanding and shared vision and execution through leadership and process integration. By having IT and OT experts working more closely together, each can better understand the other's perspective and ultimately drive favorable outcomes for the business. Without this shared understanding, all our other efforts may come to nothing.

Without resources, we can secure nothing. Forty-seven percent of respondents report that their ICS security budgets have increased over the past two years, with 16% decreasing the budget and 32% showing no change. When viewed as a comparison to overall budget from 2021 to 2019, significant growth occurred in most of the categories, with an increase in the no-budget response (perhaps because of the elimination of the unknown choice in 2021). See Table 2.

Table 2. 2021 vs. 2019 Budget Comparison

Budget	2021	2019	% Change
We don't have one	23.7%	9.9%	13.8% ▲
Less than $100,000 USD	19.1%	11.5%	7.6% ▲
$100,000–$499,999 USD	24.2%	8.9%	15.3% ▲
$500,000–$999,999 USD	10.8%	8.3%	2.5% ▲
$1 million–$2.49 million USD	10.8%	6.3%	4.5% ▲
$2.5 million–$9.99 million USD	5.2%	3.7%	1.5% ▲
Greater than $10 million USD	6.2%	7.3%	-1.1% ▼

Asset owners continue to invest in the security of their ICS environment, and that investment needs to achieve the security outcomes discussed throughout this survey.

Risks to Our ICS Environments

Risk, the force that drives most effort around ICS safety and security, directly correlates with the threat vector that introduces the risk. In 2021, financially motivated crimes—including ransomware and extortion—rose to the top in overall ranking of vectors that concern respondents, followed by nation-state cyberattacks and devices and "things" (that cannot protect themselves) being added to the network. See Figure 5.

Interestingly, however, when asked to identify the most important threat vector on this list, the order of those with the higher concern differed a bit, indicating that respondents believe that non-intentional threat vectors also play an important role in ICS security:

Select the top three threat vectors with which you are most concerned.
Note: Survey logic requires that you select exactly three choices from the list below.

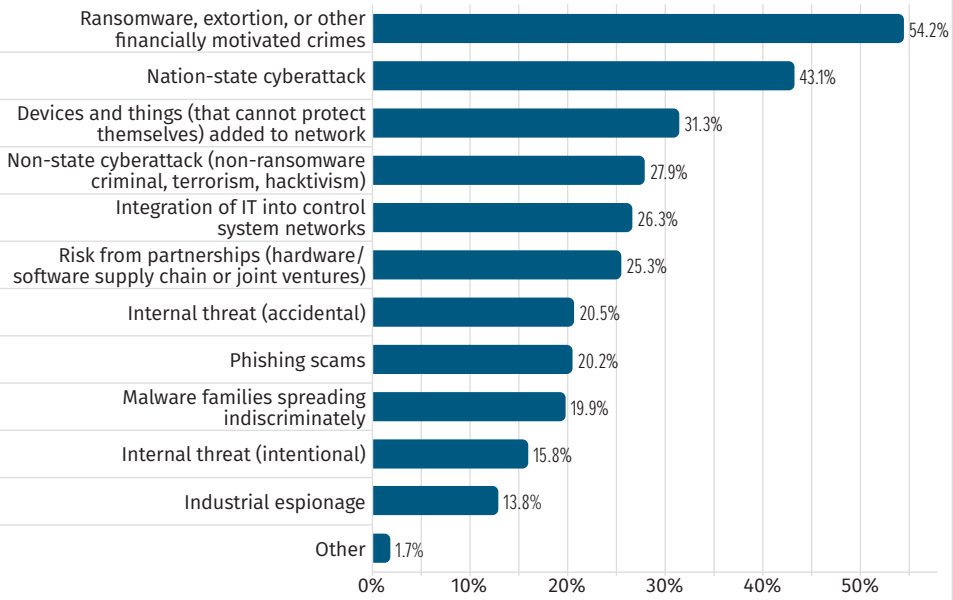


Figure 5. Top Threat Vectors

1. Ransomware, extortion, or other financially motivated crimes
2. Nation-state cyberattack
3. Devices and things (that cannot protect themselves) added to network
4. Non-state cyberattack (non-ransomware criminal, terrorism, hacktivism)

To test the hypothesis that risk perception varies by industrial sector, we posed this question: "Based on your understanding of the ICS threat landscape, which [three] sectors are most likely to have a successful ICS compromise with impact on the safe and reliable operation of the process?" We intended to drive toward perceived industry risk both for the sectors in which respondents participate but other sectors as well.

Figure 6 on the next page shows the results. The energy sector led, followed by healthcare and public health, both traditionally a target of multiple threat actors. The water/wastewater sector followed, not surprisingly, as its low margins often create a lag in security fundamentals. Note that although these results may show some survey bias related to the demographics, the Analyst team wants to note that these results are consistent with both sector and non-sector participant risk perception.

Pay attention to non-intentional threat vectors (i.e., a threat vector that is not malicious in nature but still presents risks). These threat vectors—including accidental insider, unauthorized devices on the network, and risk from partner networks and IT/OT integration—accounted for 35% of the overall top threat vectors.

Some interesting observations indicate that we need more data to better inform the overall risk picture, especially because it remains unclear whether the motivations for these answers result from confidence or overconfidence in one's own security postures:

- Most industries appeared confident in their industry's OT security posture. Of the 18 industry choices available, only five assessed that their own industry as most likely to have a consequential cyberattack: business services, communications, defense industrial base (DIB), energy, and water/wastewater.
- For respondents not choosing their own sector, energy and healthcare/public health were the leading choices.
- Inconsistencies related to sectors respondents considered relatively risk free. For example, sophisticated adversaries often target DIB systems for compromise and to hold at risk. Aside from DIB respondents themselves, however, almost no others selected DIB as a likely target.

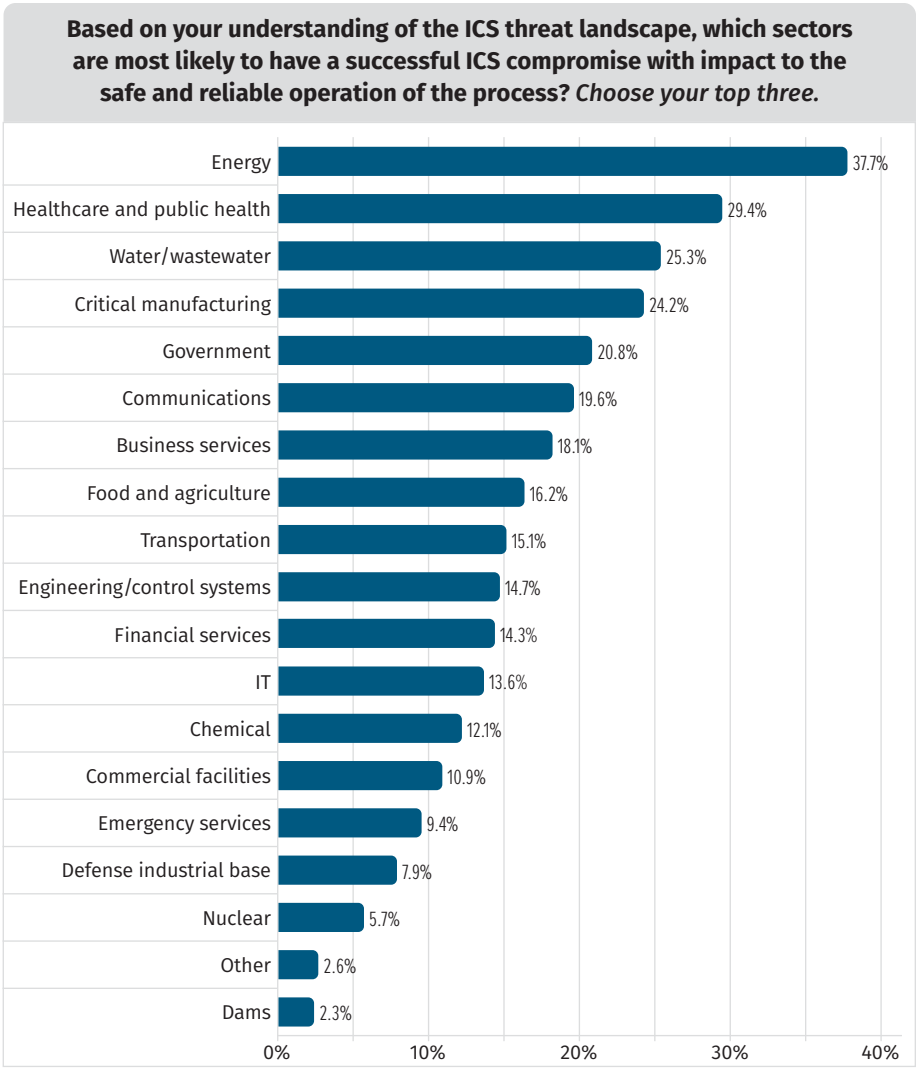


Figure 6. Perception of Sector Most at Risk

Security of ICS has really entered public consciousness over the past few years, and the perception of high and severe/critical threats has increased dramatically from 2019 to 2021 (see Figure 7). Events of 2020 and 2021 may have influenced this perception. Whereas ransomware ranked as the sixth highest concern in 2019, ransomware, extortion, and financially motivated cybercrimes now top the list of threat vectors that concern respondents.

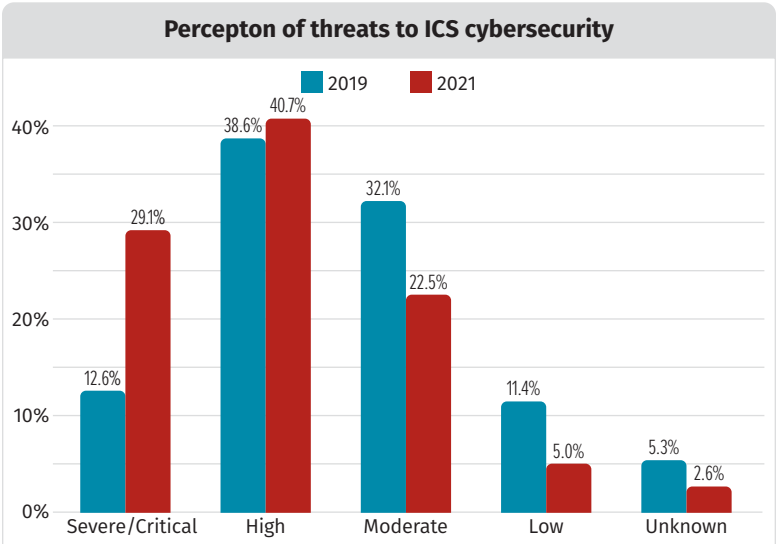


Figure 7. 2019 vs. 2021 Risk Perception

ICS Incidents: Impacts and Gaps

As in 2019, hackers remain the most prevelant source of ICS network intrusion (as expected, because in many cases additional levels of attribution are either impossible or of limited organizational utility). Organized crime rose three postions to the number two source in the 2021 survey, likely attributable to the rise of ransomware incidents, while foreign nation-state sources dropped three positions, from number four in 2019 to number seven in 2021. See Table 3.

A focus over the past few years on employee training, insider threat programs, and business partner validation for cybersecurity may have contributed to the reduction of these concepts between surveys. Interestingly, domestic intelligence services rose three postions, to the number eight concern in 2021.

As in 2019, 15% of respondents report that they have had a cybersecurity incident in their OT environment over the past 12 months. However, we may be losing some ground in the area of incident detection and response. Compared with 42% in 2019 saying that they were uncertain, 48% of survey participants did not know whether they'd had an incident, indicating a clear need to improve our detection and response capabilities as a community. See Figure 8.

Table 3. Threat Actor Risk Over Time

Answer Choices	2021 Rank	2019 Rank	Change
Hackers	1	1	—
Organized crime	2	5	+3 ▲
Current service providers, consultants, contractors	3	3	—
Current employees	4	2	-2 ▼
Activists, activist organizations, hacktivists	5	6	+1 ▲
Unknown (sources were unidentified)	6	7	+1 ▲
Foreign nation-states or state-sponsored parties	7	4	-3 ▼
Domestic intelligence services	8	11	+3 ▲
Former equipment providers	9	12	+3 ▲
Former employees	10	10	—
Current equipment providers	11	8	-3 ▼
Competitors	12	9	-3 ▼
Suppliers or partners	13	13	—
Former service providers, consultants, contractors	14	14	—
Other	15	15	—

Always remember to root risk perception in reality. For instance, the decrease in foreign nation-state attacks (dropping from number four in 2019 to number seven in 2021) is inconsistent with the ranking of nation-state cyberattacks as the second-highest threat vector that concerns respondents.

Have you experienced one or more security incidents (e.g., unauthorized access; security breach; loss of OT relevant data; operational disruption, damage, destruction of product, process, or property) involving your OT/control systems during the past 12 months?

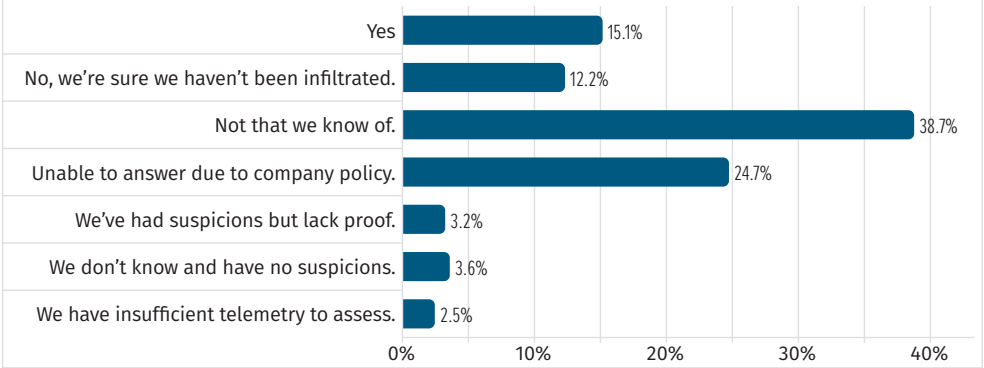


Figure 8. Incidents in the Past 12 Months

Of the 15% reporting an incident, the majority had experienced fewer than 10 incidents. Even with this relatively low number, however, incidents could still prove disruptive: 26% reported that at least 10% of incidents impacted operations. This data indicates that we should question the perception that most incidents do not have an operational impact. See Figure 9.

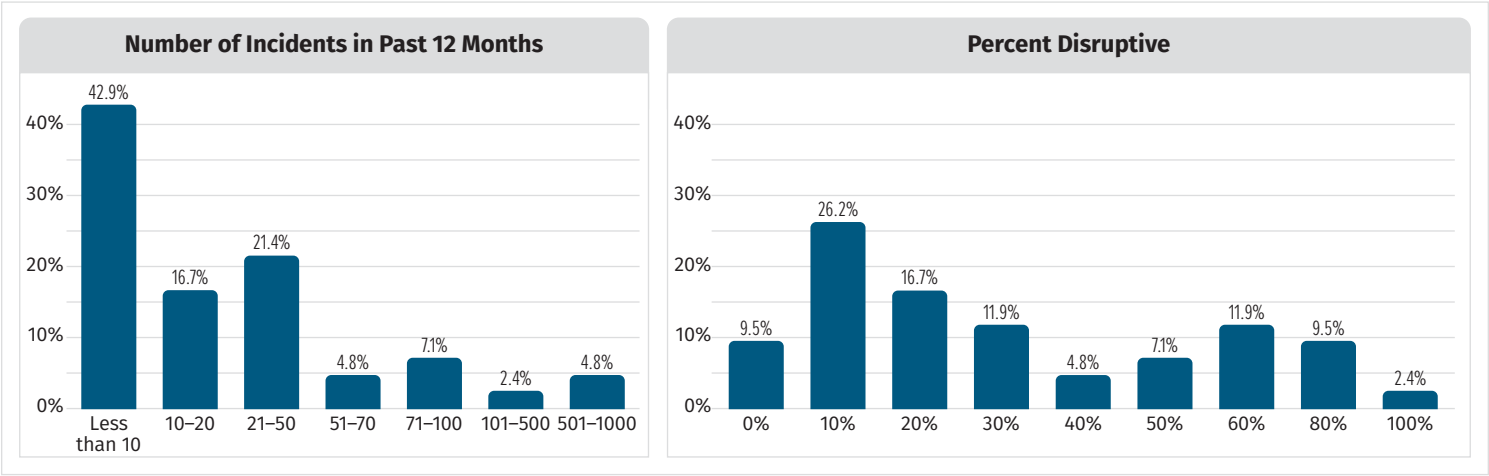


Figure 9. Incident Frequency and Process Disruption

On a positive note, the timeline of compromise to detection has improved markedly since 2019. The 6-to-24 hour category moved from 35% in 2019 to 51% in 2021 (see Figure 10), and the under-6-hour rate in the 2021 survey (not asked in 2019 survey) ranks at 30%.

Continued investment in OT incident-detection technologies, monitoring, and OT cybersecurity analysts and security operation centers likely drive these improvements. This trend also represents a significant break with historical OT intrusion cases such as Havex[2] and BlackEnergy,[3] where adversary dwell time was plus-three years before detection. Containment also shows promising results, with the majority of incidents contained within the first day of the incident.

However, issues persist. The number of incidents reaching or impacting the OT enviornment remains troubling because or potentially immediate effects on the OT environment even if an organization rapidly contains the incident. Remediation efforts appear somewhat delayed, as expected, with with the bulk occuring within the first week of containment.

Public reporting on cyber incidents impacting OT networks is not broadly available. The community would benefit from more transparent reporting data, which might allow us to study these incidents further to better implement defensive measures to protect our operations.

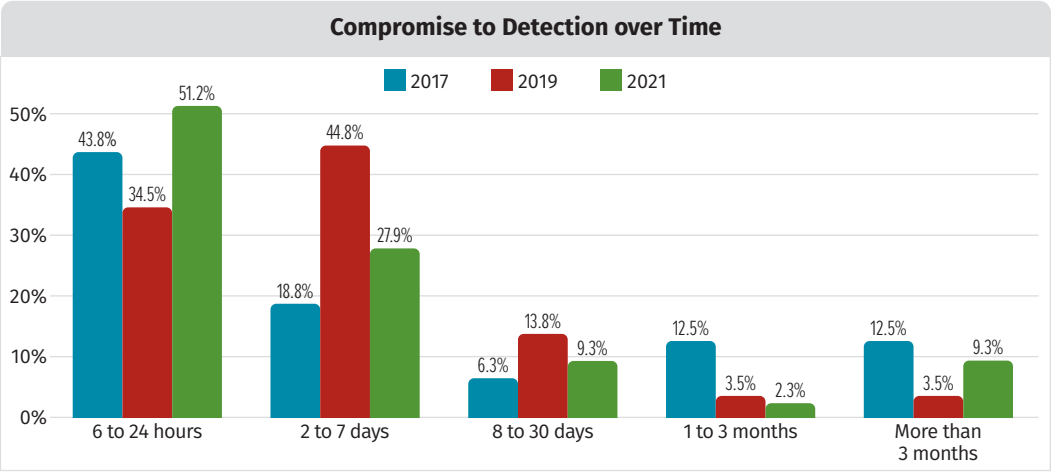


Figure 10. Compromise Detection Speed over Time

[2] "Havex," https://en.wikipedia.org/wiki/Havex

[3] "BlackEnergy," https://en.wikipedia.org/wiki/BlackEnergy

Remote access services (37%) led the reporting of initial access vectors, which aligns with the perceived risk (outlined in the next section) from external connectivity sources when respondents ranked their perceived acute risk sources. With increased industry focus on securing remote access technologies, we hoped for a more significant drop from 2019, when remote access accounted for 41% of initial attack vectors. Clearly, we need to more strongly promote the adoption of secure remote access technology. See Figure 11.

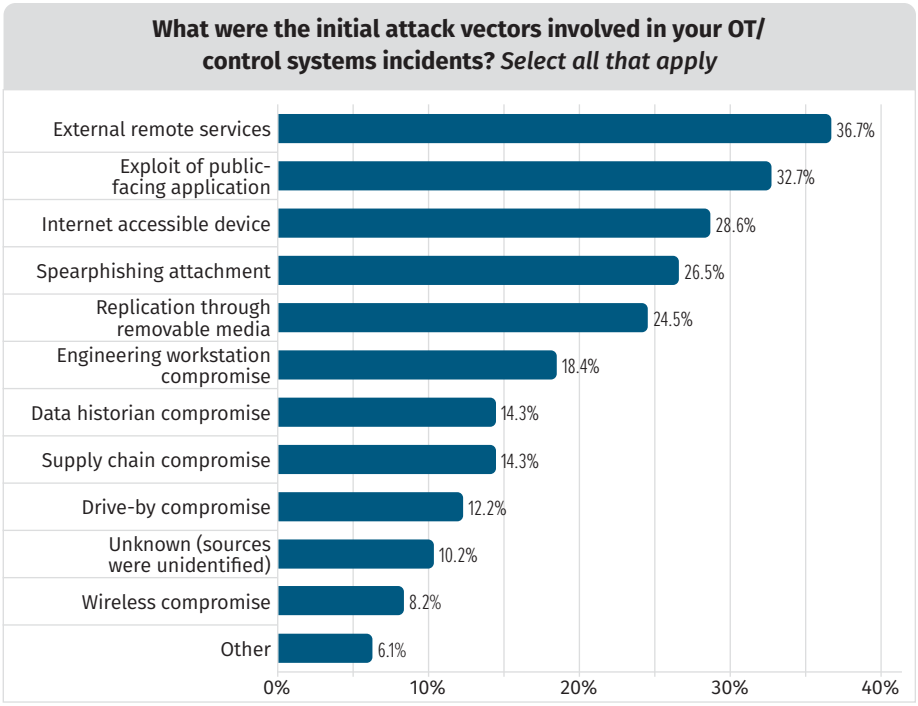


Figure 11. Incident Initial Attack Vectors

With regard to the next several leading attack vectors, we find it interesting that although not considered remote access technologies, they leverage interconnectivity as an enabling function:

- **Exploit of public-facing applications—**What level of connectivity or control is possible from applications exposed to the internet, and what arcitecture is in place to mitigate risks to the ICS?
- **Internet-accessible devices—**Is device connectivity bypassing the DMZ?
- **Spear-phishing attachment—**Properly configured OT environment should not have direct access to email services directly, yet phishing continues to be a relatively high-ranked vector.

Of particular concern is the 18% of initial vectors leveraging the engineering workstation. This percentage raises some concern because engineering workstations represent key terrain to accomplish a variety of effects in stage 2 of the ICS Cyber Kill Chain and could have contributed to the high numbers of incidents with impact on processes.

Component Risk, Impact, and Exploitation

Given these results regarding initial attack vectors, let's revisit the question of risk perception from the standpoint of the ICS components. Not surprisingly, most respondents agree that endpoints—engineering workstations and ICS server assets—present the greatest risk for compromise. See Figure 12.

Collectively, however, connectivity issues account for the second-highest risk concern (when factoring together internal system connections, remote access, connections to the field network, and wireless). So, organizations need to focus on remote access and connections to other networks as a source of risk. This risk evaluation agrees with the reported incidents that leverage remote access as an initial vector. However, currently applied security controls do not sufficiently mitigate this risk.

Perceived risk correlates well with the perceived impact on operations for fixed assets (endpoints) but tends to diverge when connectivity and mobility come into play. For example, connections to internal office networks rank fourth for risk, but they rank ninth for impact if compromised. Similarly, mobile devices rank sixth for risk, but they rank eleventh for impact if compromised. Finally, the risk from embedded controller compromise ranks eleventh, but the impact ranks fourth. This misalignment argues for a systematic approach to develop integrated plans that factor in both probability and severity. See Table 4 on the next page.

Which control system components do you consider at greatest risk for compromise? ***Select your top three in each category in no particular order.***

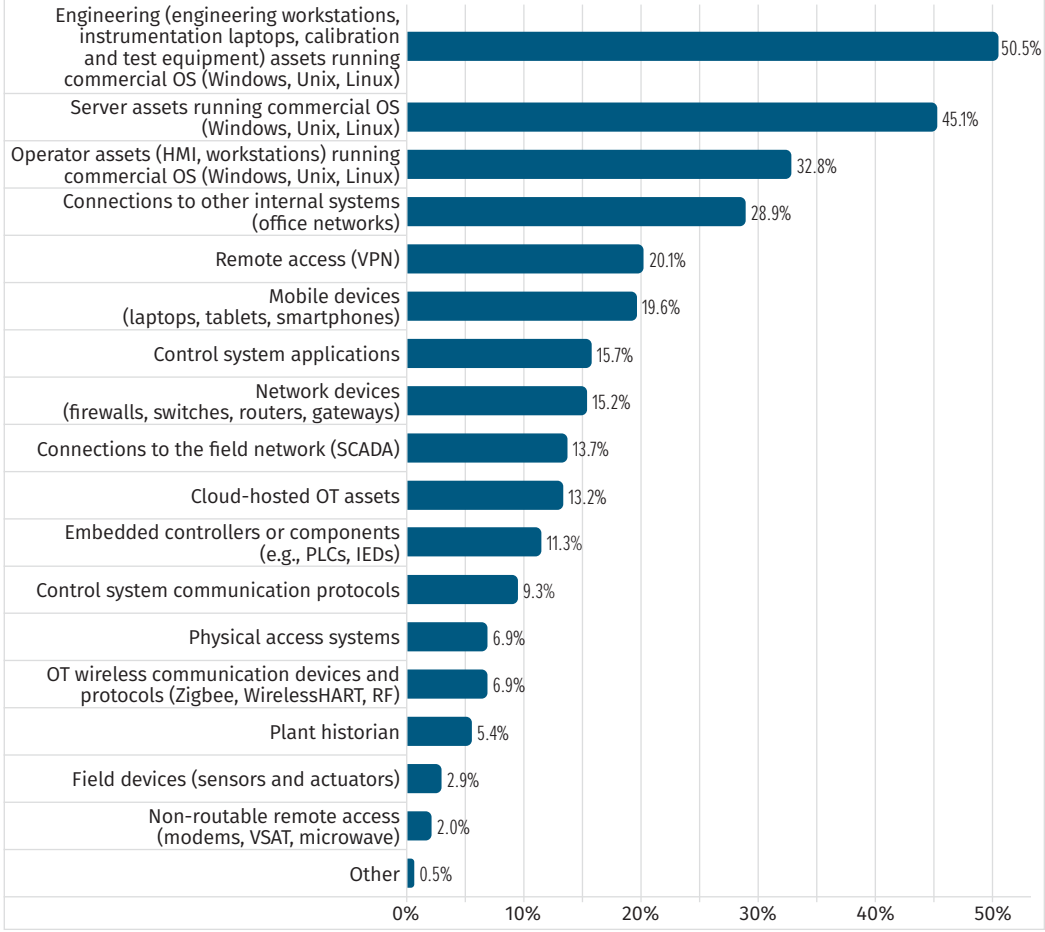


Figure 12. System Component Risk

By their nature, wireless and non-routable communications pathways (modems, VSAT, microwave) risk manipulation by personnel off-site. Relatively few security tools enable us to monitor or secure these communications pathways. Yet, these assets receive a relatively low risk ranking with regard to compromise. Given this apparent disconnect, organizations should invest in research and technical innovations to learn how to better secure these assets.

Table 4. Component Risk Compared to Impact

Component	Risk Rank	Impact Rank
Engineering (engineering workstations, instrumentation laptops, calibration and test equipment) assets running commercial OS (Windows, Unix, Linux)	1	1
Server assets running commercial OS (Windows, Unix, Linux)	2	2
Operator assets (HMI, workstations) running commercial OS (Windows, Unix, Linux)	3	3
Connections to other internal systems (office networks)	4	9
Remote access (VPN)	5	8
Mobile devices (laptops, tablets, smartphones)	6	11
Control system applications	7	7
Network devices (firewalls, switches, routers, gateways)	8	6
Connections to the field network (SCADA)	9	5
Cloud-hosted OT assets	10	10
Embedded controllers or components (e.g., PLCs, IEDs)	11	4
Control system communication protocols	12	12
Physical access systems	13	14
OT wireless communication devices and protocols (Zigbee, WirelessHART, RF)	14	16
Plant historian	15	15
Field devices (sensors and actuators)	16	13
Non-routable remote access (modems, VSAT, microwave)	17	17

Incident Response: Who to Call?

Repondents identify a mix of outsourced and internal resources as their top-three resouces to consult: an outsourced cybersecurity solution provider for primary response support, followed closely by internal resources, and then an IT consultant. See Figure 13.

Forty percent of respondents indicate that they leverage an IT consultant to support their OT response efforts. The SANS ICS team has witnessed this many times, generally when called in to remediate a failed response effort by an IT-only response company. When vetting partners for incident response support, be sure to ask about previous case histories (anonymized) and experience in OT response.

Whom do you consult when you detect signs of an infection or infiltration of your control system cyber assets or network? ***Select all that apply***

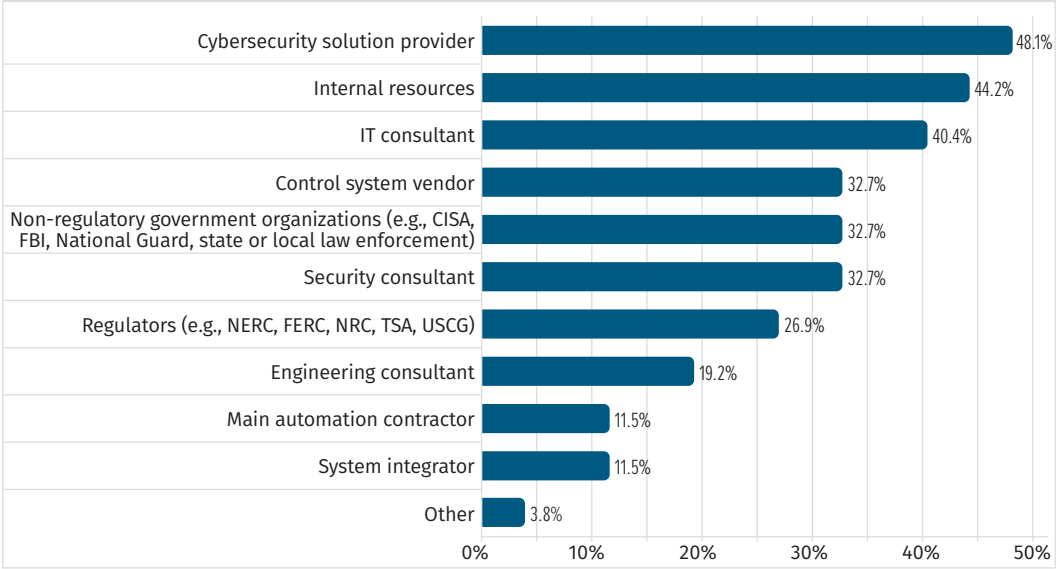


Figure 13. Incident Response Support Organizations

These results present an interesting contrast with 2019 survey results. Table 5 shows a sharp decrease in the reliance on internal resources, with the increase having shifted to the use of IT consultants and cybersecurity solution providers.

Table 5. Trends in IR Support 2019 to 2021

Response Support	2019	2021
Cybersecurity solution provider	35.6%	48.1%
Internal resources	59.0%	44.2%
IT consultant	18.4%	40.4%
Control system vendor	45.6%	32.7%
Non-regulatory government organizations (e.g., CISA, FBI, National Guard, state or local law enforcement)	40.6%	32.7%
Security consultant	37.2%	32.7%
Engineering consultant	13.4%	19.2%
Main automation contractor	8.4%	11.5%
System integrator	15.1%	11.5%
Other	2.1%	3.8%

Today's Defenses and Tomorrow's Security

Organizations leverage a variety of security technologies and solutions in their OT environment. Table 6 shows the current leading solutions:

1. Access controls (82%)
2. Antivirus solutions (77%)
3. Assessment/audit programs (65%)

Investment planning for both old and new solutions spans the next 18 months, with leading contenders identified as follows:

1. Security operations center (SOC) for OT/control systems (37%)
2. Security orchestration, automation, and response (SOAR) (33%)
3. A four-way tie for third (industrial IDS, EDR, data loss prevention, and zero trust principles) (31%)

Table 6 also compares 2019 and 2021 in terms of the technologies in use and planned. Key trends include:

Table 6. Solutions with Adoption Rate Change (2019 to 2021)

Response Support	In Use Change	Planned Change
Access controls	9.5% ▲	4.31% ▲
Anti-malware/antivirus	23.9% ▲	-3.39% ▼
Assessment and audit	5.2% ▲	10.47% ▲
Asset identification and management	8.3% ▲	4.18% ▲
Monitoring and log analysis	6.4% ▲	1.62% ▲
Security awareness training for staff, contractors, and vendors	-5.7% ▼	4.83% ▲
Vulnerability scanning	1.5% ▲	5.93% ▲
User and application access controls	-4.2% ▼	4.90% ▲
Anomaly detection tools	19.3% ▲	0.89% ▲
Communication allowlisting	15.2% ▲	2.98% ▲
Application allowlisting	8.2% ▲	8.78% ▲
OT/ICS network security monitoring and anomaly detection solutions	14.1% ▲	-8.51% ▼
OT/ICS configuration management	12.7% ▲	-1.28% ▼
Device access controls and policy-based allowlisting	6.7% ▲	4.58% ▲
Control system enhancements/upgrade services	10.9% ▲	0.88% ▲
Industrial IDS	-0.9% ▼	3.89% ▲
Device allowlisting	5.9% ▲	-0.63% ▼
Industrial intrusion prevention systems (IPS)	4.1% ▲	6.44% ▲
Data loss prevention	15.1% ▲	6.36% ▲
Software-defined network segmentation	10.7% ▲	1.77% ▲
Unidirectional gateway between control systems and higher risk networks	5.5% ▲	7.54% ▲
SOC for OT/control systems	11.1% ▲	2.71% ▲
Identity-based policy orchestration	5.3% ▲	6.17% ▲
Cloaking device IP addresses	10.3% ▲	10.59% ▲

- **Movement toward a threat-hunting and hypothesis-based security model for OT—**An increase (14%) in the implementation of OT network security monitoring and anomaly detection evidences this trend, as well as the 19% growth in the use of anomaly detection tools, signaling a welcome change from jus traditional indicator-based defense capabilities. Support for this trend also shows in increases in allowlisting for communications, applications, and devices, as well as device access controls and policy-based allowlisting.

- **Additional investment and focus on OT cybersecurity, detection, and response—**OT SOC adoption rose sharply from 2019 to 2021, as did adoption of data loss prevention (DLP) technologies. Recent high-profile ransomware incidents likely contribute to this trend, as do the increasingly common hack-and-leak style intrusions. Interestingly, respondents indicate adoption of EDR and user behavioral analysis tools, despite limited OT-specific offerings in the marketplace.
- **Increased use of anti-malware/antivirus solutions—**The 2021 survey shows a sharp increase (24%) over 2019, which may reflect the OT community's overall baseline defenses of passive analysis technologies catching up with the IT environment, a positive trend.

Surprisingly, respondents report low automation adoption (28%), an irony in a community focused on physical process automation. However, 22% plan to implement SOAR in their OT defensive architectures over the next 18 months. As a community, we want to increase our automation adoption rates for cybersecurity, to ensure we achieve cybersecurity outcomes with as little manual intervention as possible.

Unidirectional gateway use remains relatively constant (6% increase). With a focus in the industry on isolation technologies, we expected a higher percentage here.

Growing businesses always need to augment existing capabilities and upgrade functionality with new OT solutions. With regard to deploying new technologies, 71% of respondents consider prequalifying vendor or solution-provider cybersecurity postures before bringing in new capabilities as either mandatory or highly important. Most organizations (65%) take a standards-based approach to these evaluations, with only a minority using an ad hoc approach. See Figure 14.

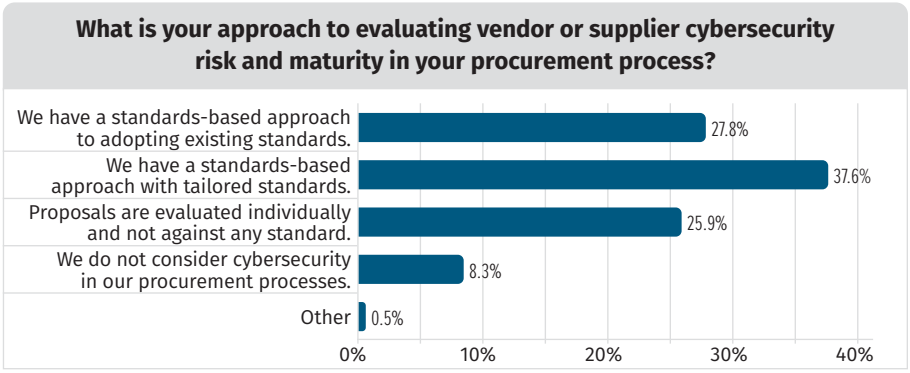


Figure 14. Vendor Assessment Process

The Industry Becomes Cloudy

Increasingly, cloud-native technologies and services impact OT environments. Forty percent of respondents report the use of some cloud-based services for OT/ICS systems, with many using cloud technologies to directly support ICS operations as well as cybersecurity functions (NOC/SOC, BCP/DR, and MSSP services). See Figure 15.

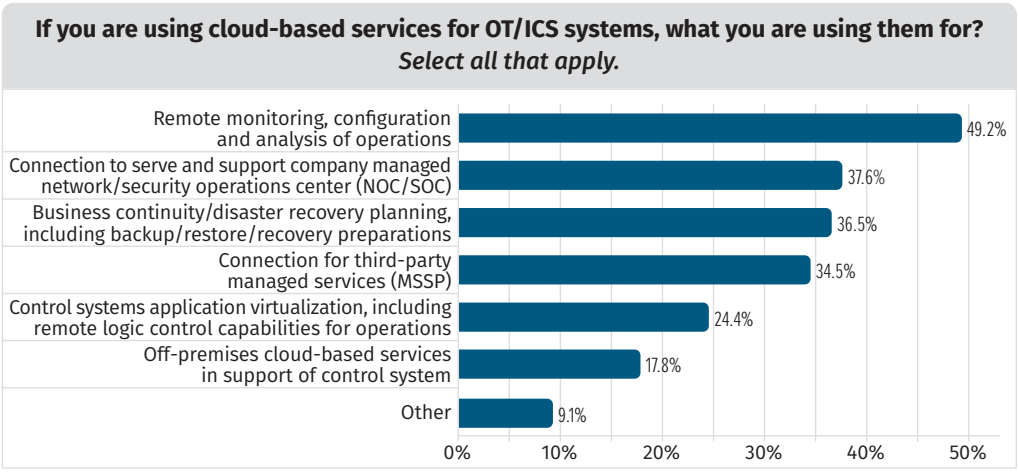


Figure 15. Functional Use of Cloud Technologies

The use of off-premises technologies to support core ICS functionality represents a recent development in the industry. Organizations need to be aware that this new potential risks, especially when combined with the recent high-profile supply chain intrusions into cloud service and managed service providers by advanced actors.

Frameworks and Standards

Organizations look to frameworks and standards to help ensure a structured defense of control systems. Most organizations map their control systems to the NIST Cyber Security Framework to help support and structure their security practices, with IEC 62443 as the second most popular choice. Some organizations must also use specific industry (e.g., NERC CIP) or locality-specific (e.g., NIS Directive) standards to govern their cybersecurity practices. See Figure 16.

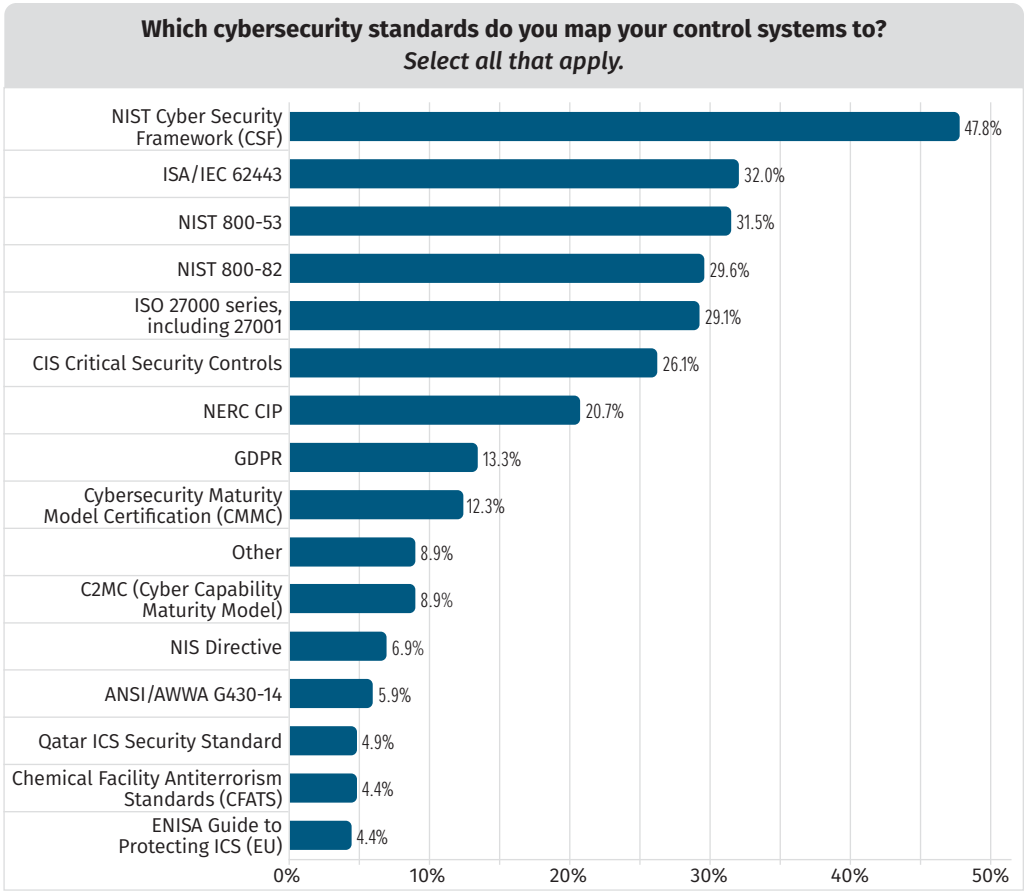


Figure 16. Cybersecurity Standards Usage

The OT security landscape has changed significantly since 2019 after the release of the MITRE ATT&CK® ICS framework.[4] This new framework provides a common lexicon to describe adversary behavior and consequences in an ICS context as an extension of the ATT&CK for Enterprise model.[5] In the 2021 survey, 47% of respondents leverage MITRE ATT&CK® for ICS in some way as part of their security framework: 43% for assessment only, 31% using it as part of penetration testing, 16% for threat activity, and 11% for adversary emulation.

[4] https://collaborate.mitre.org/attackics/index.php/Main_Page

[5] https://attack.mitre.org/

Of those using ICS ATT&CK, 50% had completed a MITRE ATT&CK® for ICS coverage assessment. The coverage was distributed relatively evenly, but initial access, lateral movement, and persistence had some of the most comprehensive coverage. See Figure 17.

Threat Intelligence

The ICS threat intelligence market has matured over the past two years. In 2019, several smaller vendors provided ICS-specific threat intelligence. In 2021, this marketspace has expanded. Although the majority of respondents still use publicly available threat intelligence, half have vendor-provided ICS-specific threat intelligence feeds, and they rely less on IT threat intelligence providers (36%). See Figure 18.

Are you leveraging ICS-specific threat intelligence in your OT defensive posture? *Select all that apply.*

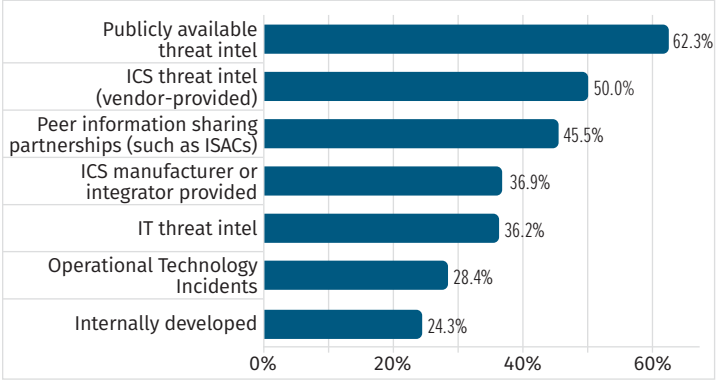


Figure 18. Threat Intelligence Sources

If you have completed an assessment of your MITRE ATT&CK® ICS technique coverage in your ICS, what coverage (to the nearest percent or percent range) do you have in each of these areas?

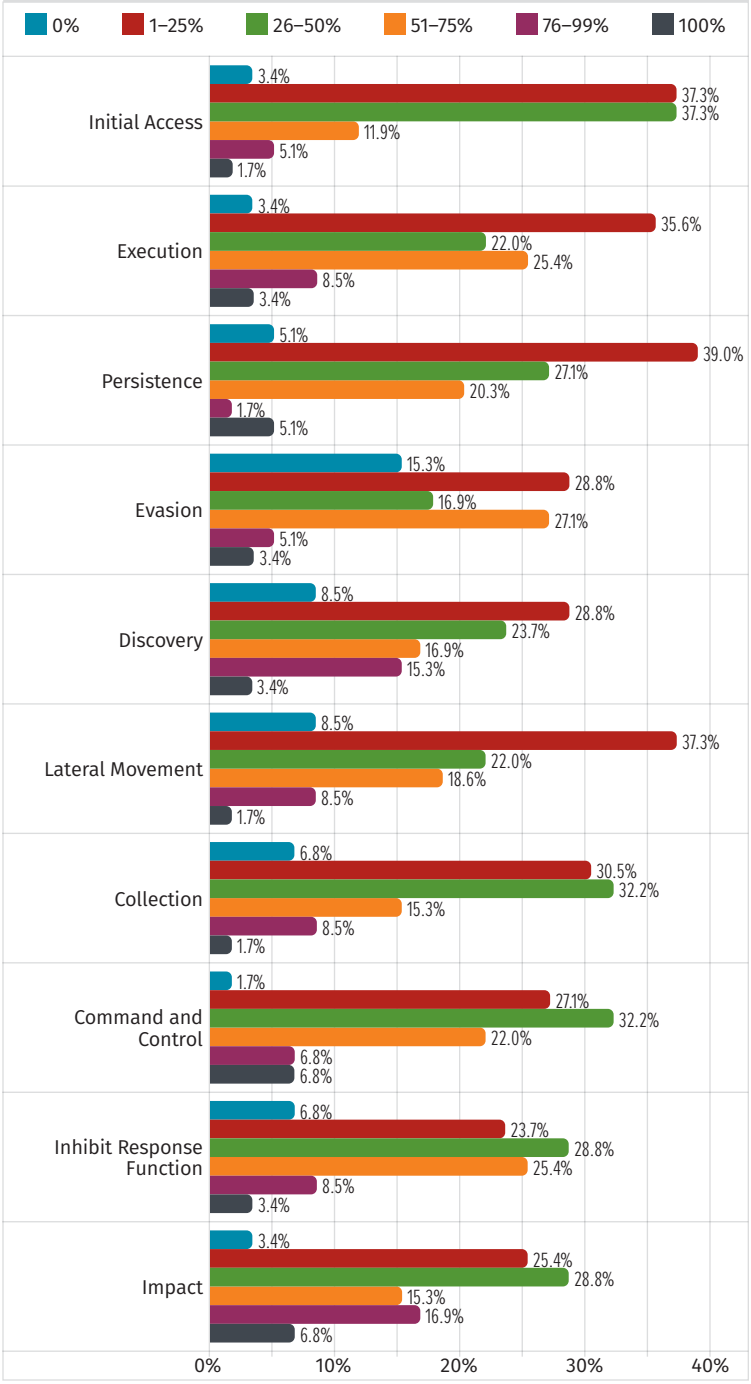


Figure 17. MITRE ATT&CK® for ICS Coverage Assessment

Improving the Defenses

Monitoring

Almost 70% of respondents to the 2021 survey have a monitoring program in place for OT security. Most of this monitoring (56%) comes from the IT security team, which also monitors the OT environment. Thirty-two percent of respondents report that they have a dedicated OT SOC monitoring their OT assets, and 25% use an outsourced OT MSSP for monitoring. With regard to OT SOC and OT MSSP, 57% of survey respondents use an OT-specific monitoring capability. See Figure 19.

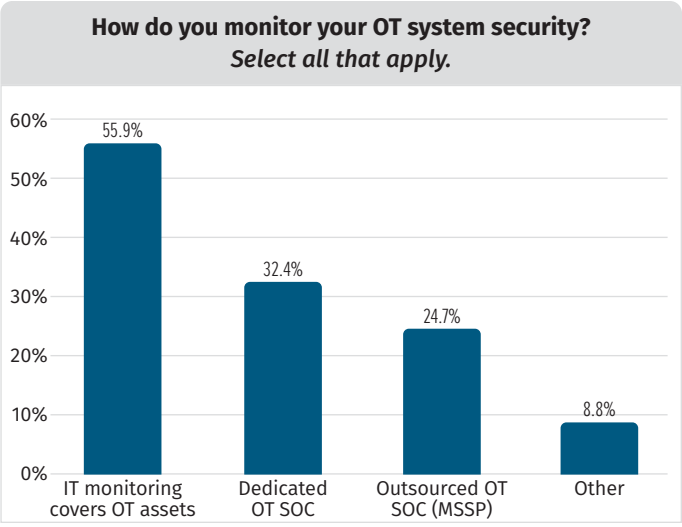


Figure 19. OT Security Monitoring

The majority of monitoring telemetry comes from either networking devices or server assets that more closely resemble IT assets. Much of the monitoring telemetry from ICS-specific devices does not appear to have widespread adoption. Only 24% of respondents correlate data from their process historian with their cybersecurity data. Correlating the cyber-relevant data with the process data is a critical aspect of OT cyber-incident investigation, especially when that incident has an impact on the process (see Figure 20). Without cross-comparing these datasets, identifying root causes becomes more challenging; even still, few solutions in the marketplace facilitate this correlation.

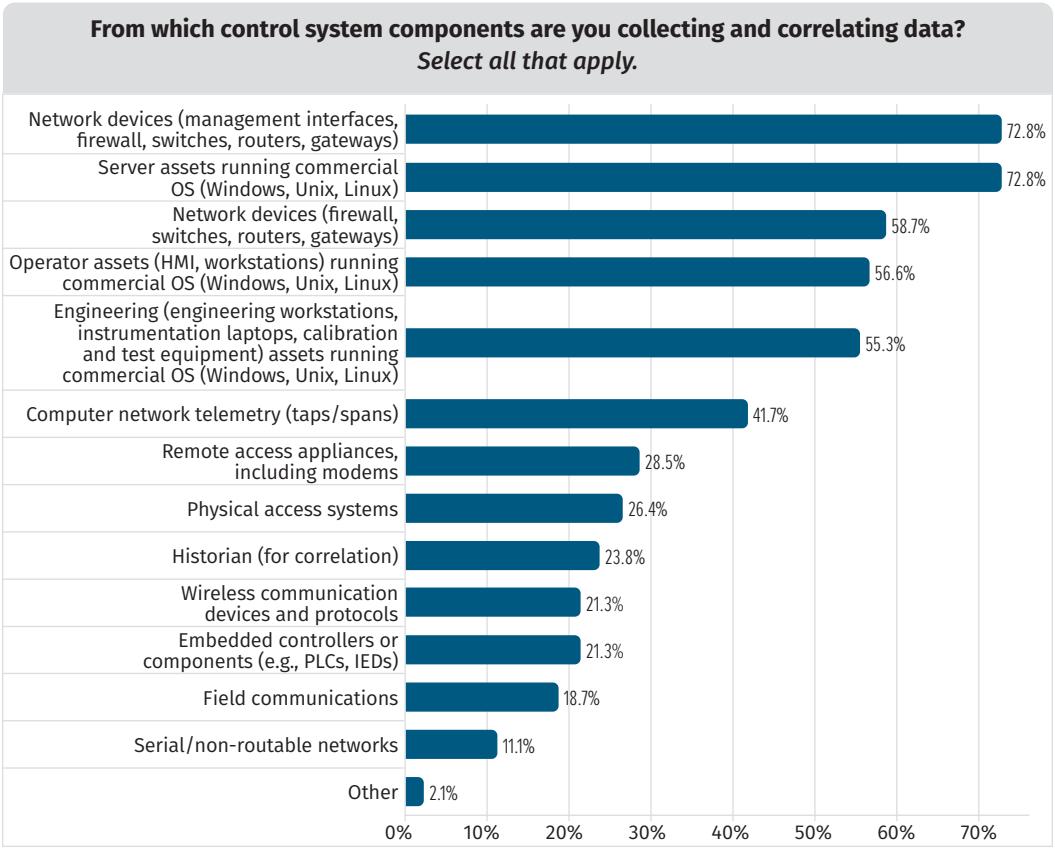


Figure 20. OT Monitoring Sources

Although organizations monitor most assets, much of that monitoring still relies on automated detections and signatures such as AV and IDS to identify active risks. A significant portion of respondents also use a threat-hunting methodology (35%) or anomaly-based detections (30%) to search for active threats in their OT

environments. Twenty-four percent do not have a formal threat-hunting process, and 17% do not look for threats in their OT environments (indicating some areas of improvement for adoption). See Figure 21.

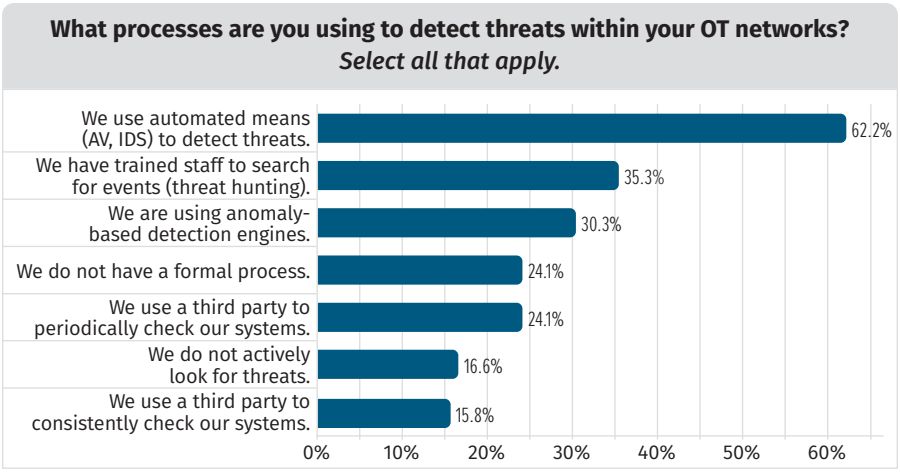


Figure 21. OT Security Analysis Methodology

Asset Inventory

Without a solid understanding of the assets on your ICS network, you cannot develop and implement a strategy to manage risk and to ensure reliable operations. Although a majority of respondents (58%) indicate that their organization has a formal program to inventory OT assets, we must do more work to ensure adoption of this foundational step.[6] The survey did not cover the methodologies used to develop asset inventory, neither did the survey ask what resource-allocation changes fund this work.

Of the assets that make up an OT network, servers and ICS devices were the most inventoried assets in the environment, with 29% and 22% of respondents indicating they had 100% coverage, respectively. Monitoring of these assets, however, lagged by 7% for each category, indicating that even in well-inventoried environments, monitoring of the known assets remains a challenge. Software assets and applications lagged significantly in both the inventory and monitoring categories. See Figure 22.

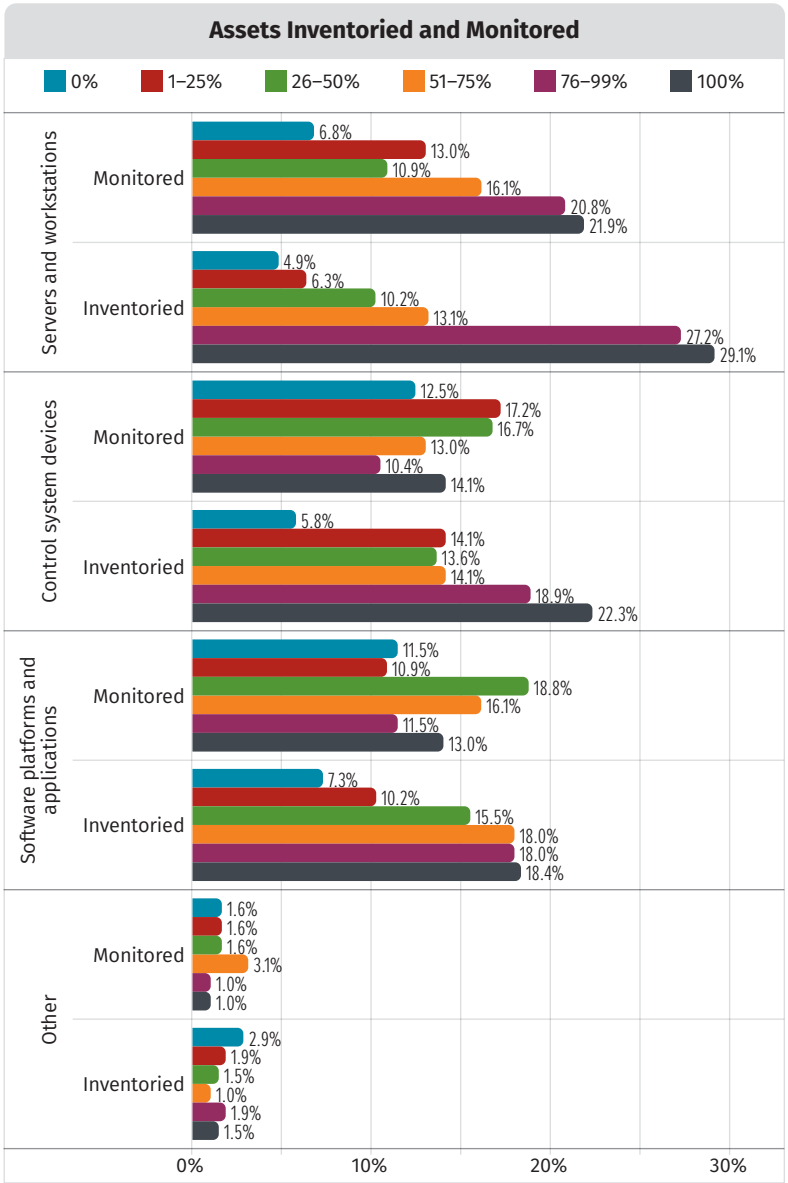


Figure 22. Percentage of Monitored/Inventoried Assets

Connection Inventories

Similar to asset inventory results, only 57% of respondents have documented all connections that lead outside of the OT environment, down from 62% in 2019. This decrease perhaps results from respondents better understanding the complexity of the ICS networks and being, therefore, less willing to indicate that they had all the connections documented. This trend remains concerning and likely contributes to the prevalence of connectivity-related incidents.

[6] You can find additional information on ICS asset inventories in the SANS whitepaper "ICS Asset Identification: It's More Than Just Security," by Mark Bristow, www.sans.org/white-papers/39650/

Once an organization has a well-defined boundary and has accounted for all communications pathways, organizations need to assess how they secure those communications. As in 2019, most respondents report using a DMZ between the OT network and the corporate network to separate communications. The percentage of respondents in this category, however, declined from 57% in 2019 to 49% in 2021.

Security experts consider having a DMZ between the OT network and corporate network a best practice if connectivity is required. In 2019, 28% of survey participants reported that they had 100% isolated systems. In 2021, that number drops to 8%. A number of factors might influence this drop; perhaps more comprehensive data has become available, indicating connectivity where it was previously assumed not to exist, or perhaps organizations have adopted additional cloud-based technologies that necessitate communications. In the 2021 survey, 42% indicate that their control systems had direct connectivity to the internet versus a 12% response rate in 2019. Once again, this change might result from a better understanding of communications pathways, as opposed to a change in actual connectivity to the internet.

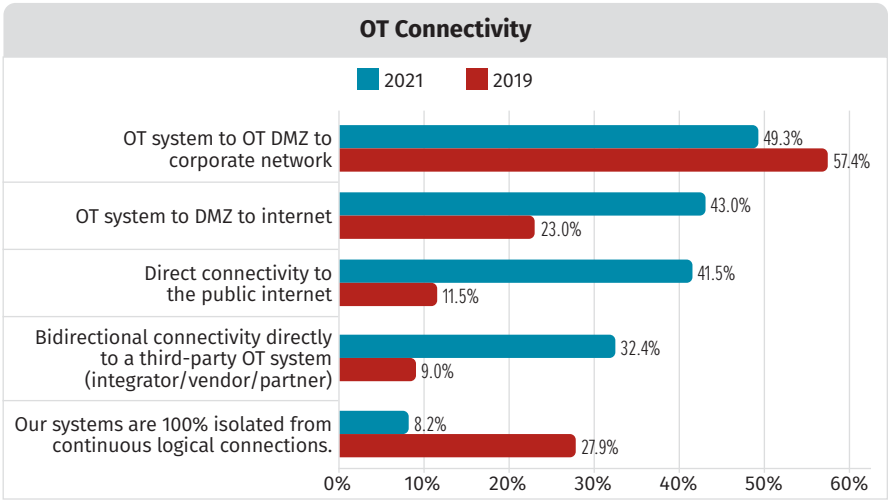


Figure 23. OT Connectivity to External Networks

This trend remains concerning, however. Twenty-six percent report outbound internet connectivity only, with additional details on verification details unavailable. See Figure 23.

Methods of connectivity also represent an important indicator of overall system security. Dedicated circuits and communication mechanisms inherently offer more security (requiring physical access to the medium) than leased, satellite, or wireless communications. Based on the responses to this question, organizations use a wide range of OSI Layer 1 technologies to move ICS data into and out of their control networks. Most use dedicated or leased fiber, but many use public internet systems (cable, DSL) or similar technologies. Seven percent report still using dial-up communications. See Figure 24.

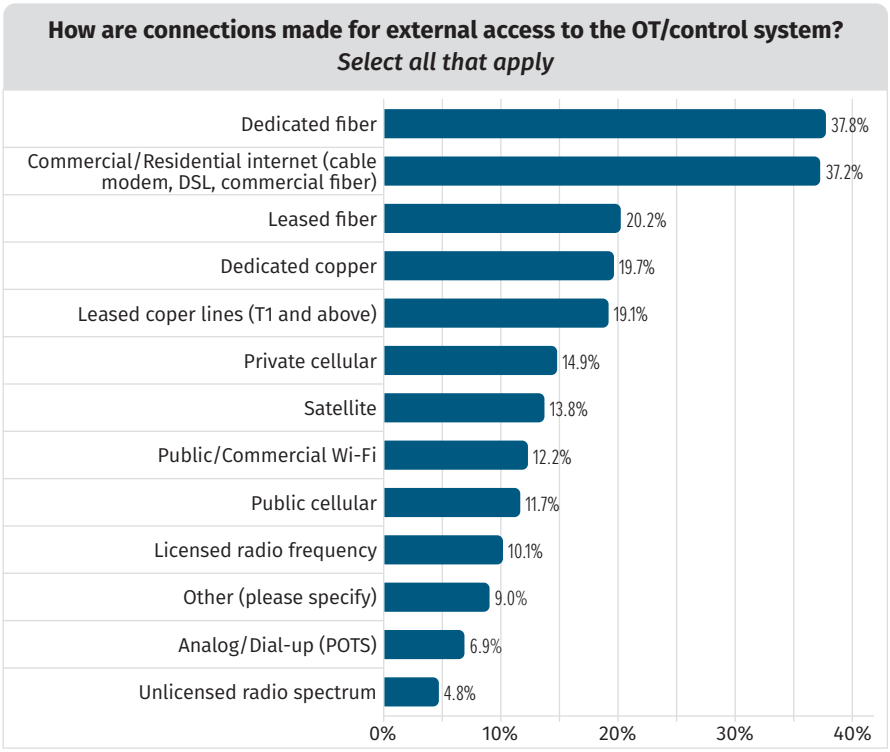


Figure 24. OT Connection Mediums

Assessing and Remediating Vulnerabilities

Organizations have made significant improvements with regard to assessments of ICS environments. Thirty percent of respondents have implemented a continual assessment program, and 76% have completed an assessment within the past year, leaving only 10% of respondents who have never completed an assessment of the control system network.

For those completing assessments, most leverage resources with OT-specific expertise—a testament to the maturing of robust OT security assessment offerings. See Figure 25.

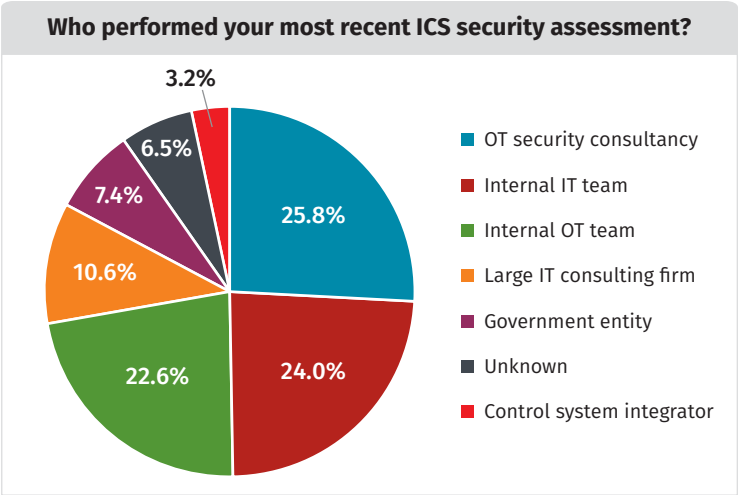


Figure 25. Security Assessors

After completing an assessment, organizations need to identify vulnerabilities in their control system environments. For this, respondents leverage processes to detect vulnerabilities in their systems. Most (61%) use public notices of vulnerabilities as the information becomes available. See Figure 26.

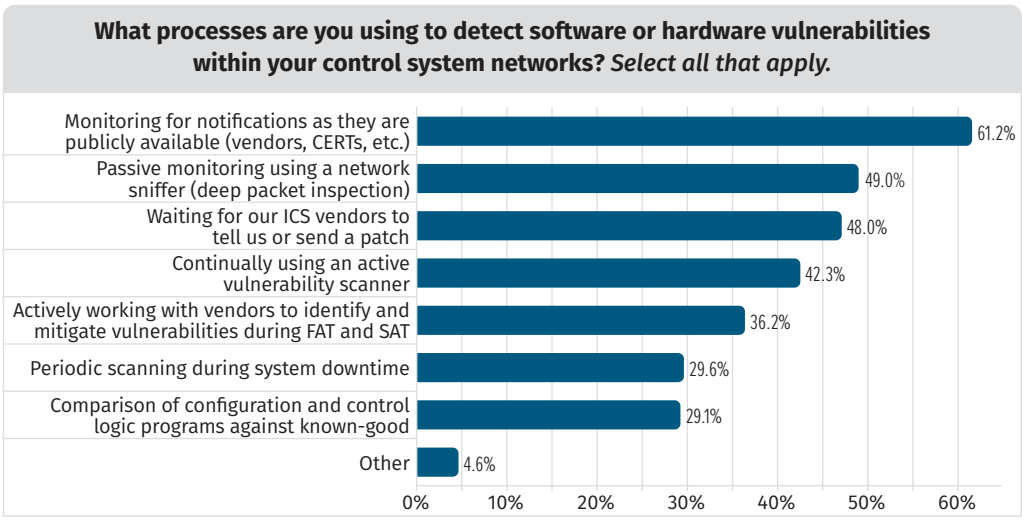


Figure 26. Vulnerability Data Sources

SANS was encouraged to see some developments:

- Strong adoption (42%) of active vulnerability scanning technologies, historically viewed as risky in legacy control environments. This adoption indicates additional trust from asset owners with regard to implementing these technologies in a modern ICS environment.
- Broader adoption (36%) of organizations leveraging opportunities to discover vulnerabilities in factory acceptance testing (FAT) and site acceptance testing (SAT) to mitigate risks before they are fielded.
- Roughly 30% use known good configurations matched against current configurations and logic to validate that processes run as expected.

After identifying vulnerabilities, most use a mitigation plan to reduce risk, with only 6% taking no action. See Figure 27.

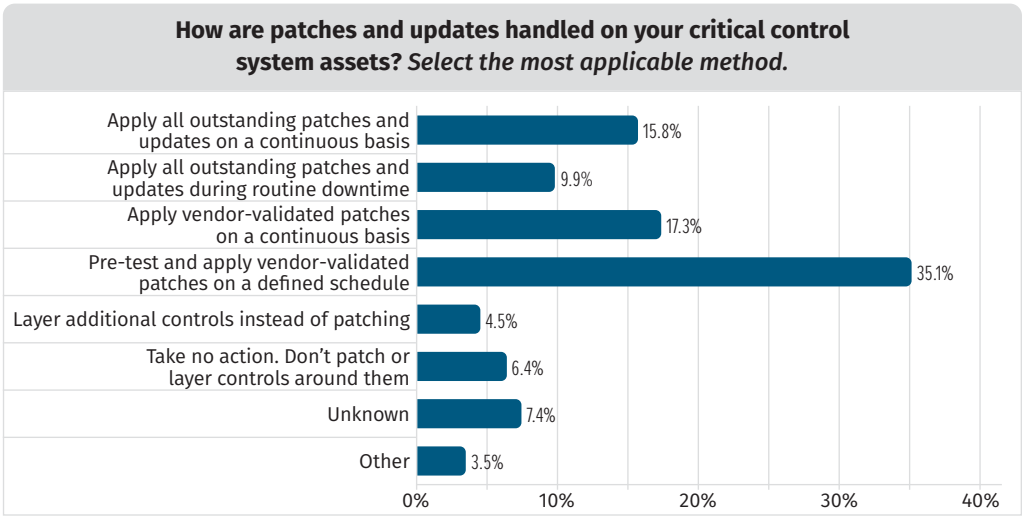


Figure 27. Vulnerability Remediation Methods

Until recently, most process environments could not continually apply patches. Consequently, the 16% of respondents that apply patches on a continual basis represents a welcome sign of the improving reliability in ICS patch management cycles. Energy sector respondents were the most likely to have a continual patch cycle but also most likely not to address the vulnerability (thus presenting a paradox).

People Drive Process

Along with technology, people and processes represent critical elements of a robust ICS cybersecurity program. Leadership that understands ICS is key.

Thirty-six percent of respondents indicate that the CISO sets the policy for ICS security. Only 8% of respondents report that these policies derive from the plant level, and the chief technology officer ranks as the second-highest corporate officer setting policy. See Figure 28.

Implementation, however, remains largely in the hands of IT management (39%), although 35% indicate that the CISO has a hands-on role in implementing the processes and strategy they set for the organization. See Figure 29.

Because OT and IT often have different philosophies, distinction between policy and implementation can have significant implications. So, to create a solid ICS security team, organizations need to continue prioritizing communications, outreach, and education between the two groups.

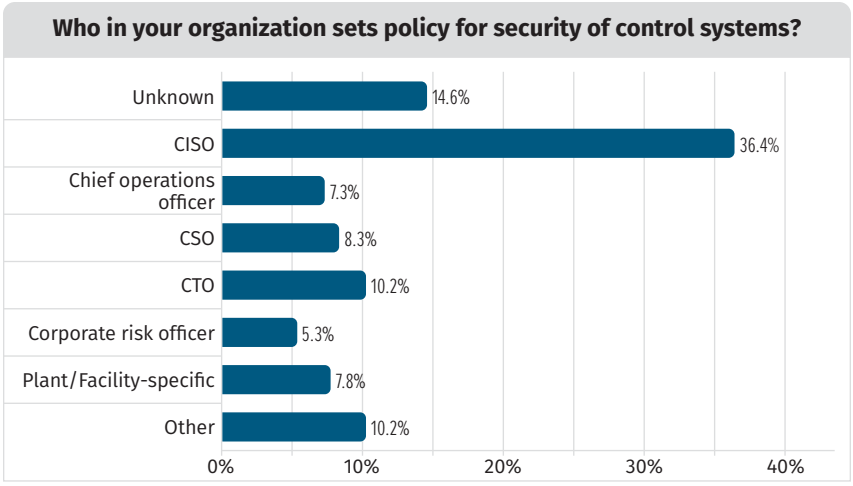


Figure 28. Security Policy Responsibility

Figure 29. Security Control Implementation

Where Do We Go from Here?

Effectively defending OT environments requires a multifaceted and integrated strategy that considers internal and external risks, understands vulnerability to those risks, and prioritizes mitigation measures via people, processes, and technology to manage identified risks. This approach requires a solid understanding of the state of play across similar entities and key partnerships internally, especially with IT security teams and with peers in other organizations.

The gaps and challenges that the ICS community needs to address include:

- Better understanding of the threat landscape, with enhanced sharing of incidents to improve collective defense
- Understanding the process-related impacts of incidents
- Correlating process control telemetry with cybersecurity telemetry for root cause analysis
- Meeting current ICS security hygiene fundamentals—improved asset identification and connectivity management
- Improving OT/ICS endpoint visibility as key technologies continue to mature

The ICS community faces an inflection point. We continue to see investments and outcomes from OT security efforts increase, but risk drivers do not remain static. OT security dominates the national cyber conversation in ways not previously imagined. Although the ICS/OT security community has made great strides, we still have hard work ahead.

About the Author

Mark Bristow, a SANS instructor for ICS515: ICS Active Defense and Incident Response, is an active member of the ICS cybersecurity community at both the operator and policy level. Mark is passionate about growing the "army of smart ICS cybersecurity people" and helping to defend the critical systems that underpin modern life. Over his career, Mark has been on the front lines of headline-grabbing incident response efforts, such as the attack on the Ukrainian power grid, intrusions into US election infrastructure, and Russian attempts to gain access to the US power grid. Mark earned a bachelor degree in computer engineering from Pennsylvania State University and currently works for the Cybersecurity and Infrastructure Security Agency, a part of the Department of Homeland Security.

Mark wants to thank Lindsey Cerkovnik, Jason Dely, and Dean Parsons for their contributions to and peer review of this paper.

Sponsor

SANS would like to thank this paper's sponsor:

tenable®