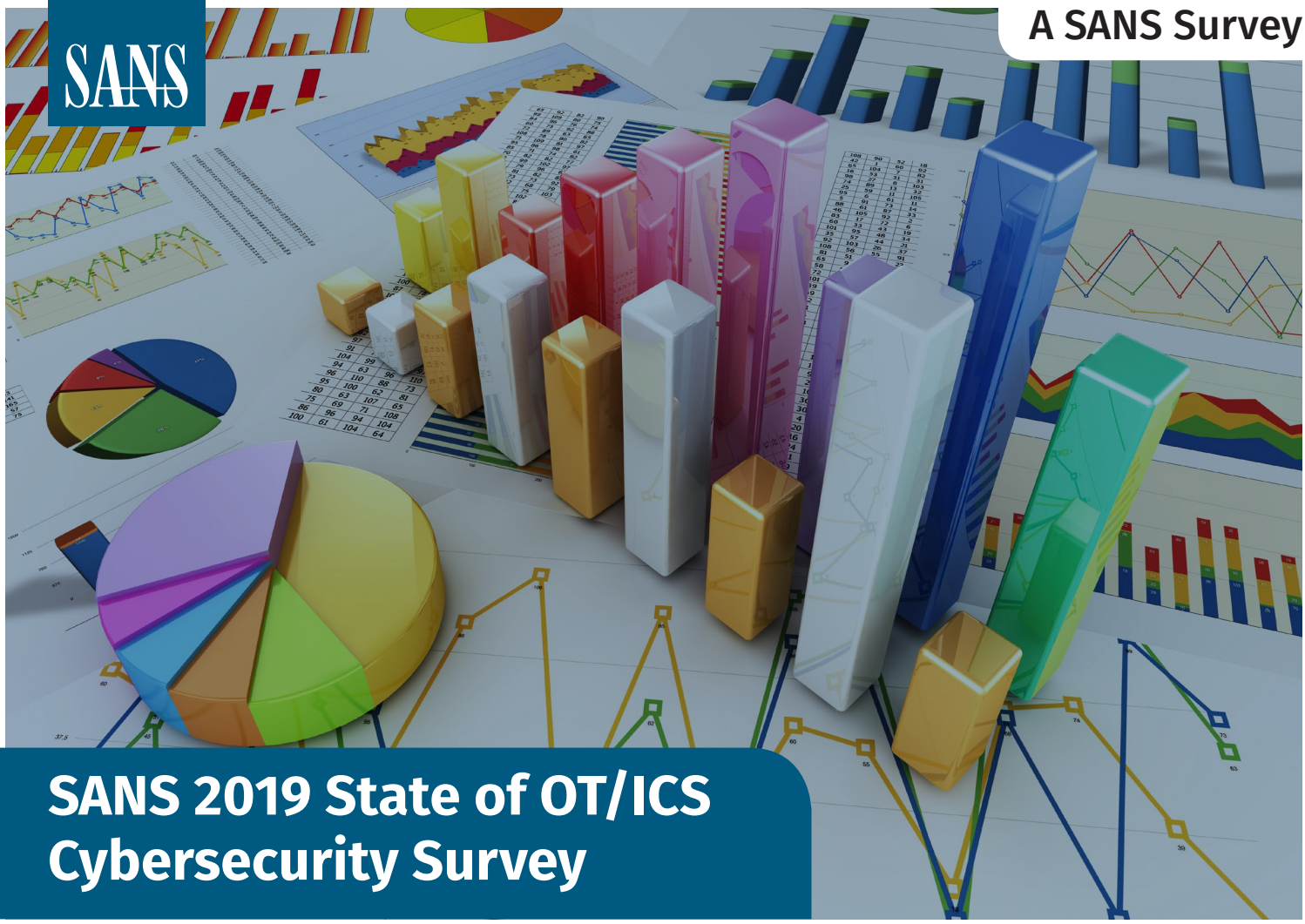
SANS

A SANS Survey



SANS 2019 State of OT/ICS Cybersecurity Survey

Written by **Barbara Filkins**
and **Doug Wylie**
Advisor: **Jason Dely**

June 2019

Sponsored by:
Radiflow

Analyst Program

Executive Summary

The 2019 SANS OT/ICS Cybersecurity Survey explores the challenges involved with design, operation and risk management of an industrial control system (ICS), its cyber assets and communication protocols, and supporting operations.

This year, SANS focused more broadly on the operational technology (OT) domain inside organizations, because industrial control systems are interwoven and interdependent, while also actively exchanging information with a myriad of other systems and processes. Fundamentally, a modern ICS is rarely, if ever, exclusively localized to an isolated, physical control system. Rather, it is an integral part of company operations. Operations now relies on these interactions of industrial control systems with IT, placing new emphasis on the integration of these two domains—especially around communications and data exchange.

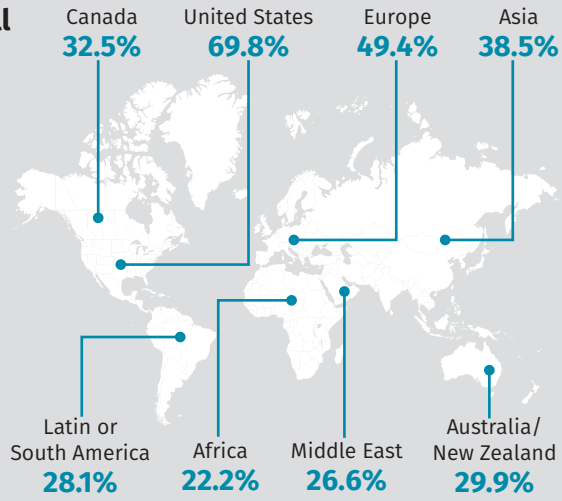
Even the lower levels of a modern ICS architecture (endpoints, field devices, instrumentation, intelligent sensors and actuators) now rely on remote connectivity for communication, control, configuration and data collection. As these boundaries become more fluid, OT and IT teams need to break down traditional communication barriers to support this new architectural norm for control systems across industries and throughout application domains.

Survey Demographics in a Nutshell

338 respondents including security and other professionals working or active in enterprise IT or operational control systems, such as ICS, SCADA, process control, distributed control or building/facility automation and control

Slightly more than 45% with a role where more than 50% of their work time is devoted to OT/ICS cybersecurity

Majority of respondents from organizations with operations in the United States (70%), Europe (49%) and Asia (39%)



The 2019 SANS OT/ICS Security Survey reveals a growing maturity in identifying potential risk and detecting and remediating actual events. People are considered the leading risk for compromise, signaling the need for a blended approach to addressing OT/ICS cybersecurity, one not solely reliant on technology. The top initiatives where respondent organizations are prioritizing and committing (i.e., budgeting) their efforts to increase OT/control system and network security align nicely with the broad risk categories of people, process and technology.

These initiatives emphasize the need to understand and chart the ICS environment. Internet connectivity has opened ICS network boundaries that historically were closed, well-defined and documented, resulting in the desire and need for visibility into critical communication links—especially wireless extensions to the ICS architecture.

Top 2019 Initiatives for Increasing OT/Control System and Network Security

1. Increase visibility into control system cyber assets and configurations **45.5%**
2. Perform security assessment or audit of control systems and control system networks **37.3%**
3. Invest in general cybersecurity awareness programs for employees including IT, OT and hybrid IT/OT personnel **29.5%**
4. Invest in cybersecurity education and training for IT, OT and hybrid IT/OT personnel. **29.1%**
5. Implement anomaly and intrusion detection tools on control system networks. **28.3%**
6. Bridge IT and OT initiatives. **26.6%**

At the same time, a growing reliance on cloud-based architectures and services reinforces the need for knowing what you have, where information is stored and exchanged, and even where the logic and control functions for the ICS reside. A comprehensive inventory of system assets, especially industrial embedded devices, becomes even more difficult in light of more porous system boundaries and virtual assets, leading to blind spots as to where and how much risk affects the modern ICS. Awareness, education and training of both the OT and IT workforce become the foundation for the effective use of people, process and technology to strengthen ICS security.

Achieving these initiatives, however, may be harder than anticipated. Security personnel working to defend their environment focus on the current and immediate threat landscape. For OT/ICS, this includes IoT growth, accidental insiders, supply chain issues and malicious external actors. In 2019, the leading business concerns are not fully aligned with the current threat landscape, flagging potential conflict in achieving the desired initiatives if an actual attack against the business occurs.

SANS believes collaboration between the IT and operational technology (OT) domains is essential as organizations come to rely more on internal staffing. Our data shows that cooperation is improving, but clashes in roles and responsibilities show the potential for conflict. According to survey results, IT takes a leading role in managing corporate security policy and implementing the necessary controls, including into OT's domain, while OT often controls the budget for safeguarding the ICS. The goals and objectives of these two domains are not well aligned: IT governance and risk management center on uptime and the protection of information and reputation (privacy), while OT focuses on the safety and reliability of cyberphysical processes. To ensure collaboration and reduced risk to the organization, a common understanding of these key concepts is needed, often requiring a common understanding of terminology, too.

The widely known security risk categories of people, process and technology can be viewed as the three pillars for a successful IT/OT convergence strategy. Results from the 2019 survey offer insights on where organizations can develop a strategy for improving collaboration and integration between the IT and OT domains.

As Expected, Risk Drives the Emphasis on Controls

Risk obviously drives organizations' approach to OT system security. Slightly more than 50% of respondents perceive the level of OT/ICS cyberrisk to their company's overall risk profile as either severe/critical or high. See Figure 1.

People (62%) present the greatest risk for compromise to an organization's OT/control systems—not surprising, because the human element lies at the heart of cybersecurity incidents and breaches. This element is followed rather distantly by technology (22%) and process (14%), raising an interesting question as to why process as a risk category does not

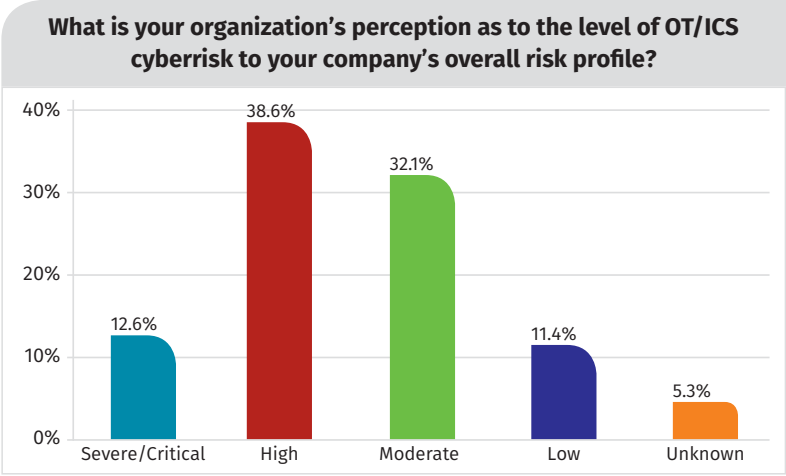


Figure 1: Perception of Organizational/ICS Cyberrisk

rank higher, possibly higher than technology. Process design and implementation represent key elements in determining both the ICS architecture and the technology used in its infrastructure. See Figure 2.

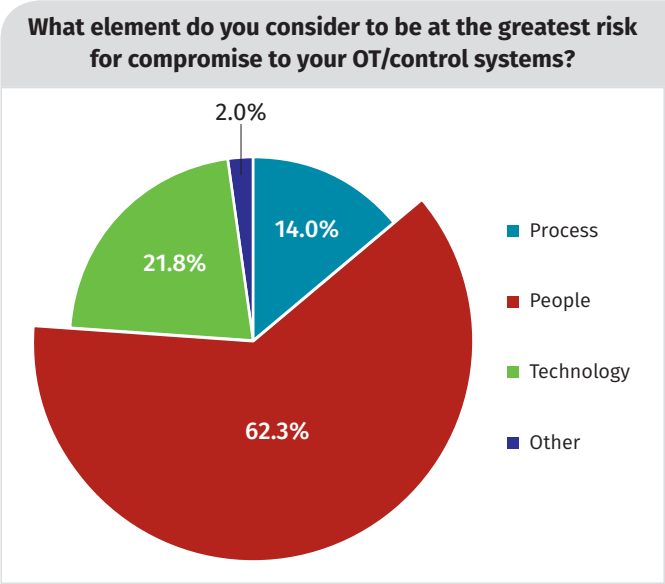


Figure 2. Risk Categories for Compromise

People is a broad risk category, encompassing external and internal actors, intentional (malicious) to unintentional (accidental, careless) actions. According to the 2018 Verizon Data Breach Investigations Report (DBIR), outsiders—including organized crime and nation-state or state-affiliated actors—perpetrated the majority (72%) of breaches.[1] Of possibly even greater concern, however, are the 28% involving insiders. Insider threats are particularly difficult to guard against, especially in the OT/ICS space, where situational awareness and process knowledge are essential to recognizing a potential safety or security issue. Furthermore, it's not uncommon in the OT domain for ICS personnel to carry higher privileges than necessary since technical options to restrict access may not be available or feasible, or these higher-level administrative privileges are broadly viewed as insurance available to be used during unforeseen events. This situation is exacerbated by staffing as well as technology limitations.

The primary business concerns related to the security and risk management of OT/controls remain essentially the same in 2019 as in 2017, although there are some small changes in the overall ranking. See Table 1.

Table 1. Leading Business Concerns

Business Concern	2017		2019		Change in Rank
	Percent	Rank	Percent	Rank	
Ensuring reliability and availability of control systems	52.3%	1	52.3%	1	—
Ensuring health and safety of employees	32.7%	3	42.2%	2	+1
Lowering risk/Improving security	33.3%	2	34.8%	3	-1
Preventing damage to systems	24.8%	4	27.7%	4	—
Meeting regulatory compliance	17.0%	7	22.3%	5	+2
Protecting external people and property	16.3%	8	20.7%	6	+2
Preventing company financial loss	21.6%	6	18.8%	7	-1
Protecting company reputation and brand	21.6%	5	17.6%	8	-3
Preventing information leakage	15.7%	9	14.8%	9	—
Securing connections to external systems	13.7%	12	11.7%	10	+2
Providing or coordinating employee cybersecurity education and awareness programs	13.7%	11	10.5%	11	—
Minimizing impact on shareholders	5.9%	14	9.8%	12	+2
Creating, documenting and managing security policies and procedures	14.4%	10	8.2%	13	-3
Protecting trade secrets and intellectual property	9.8%	13	7.8%	14	-1

Ensuring reliability and availability of control systems continues to be the top concern for respondents. However, ensuring the health and safety of employees is now the second highest concern for OT cybersecurity, increasing from 33% in 2017 to 42% in 2019—in fact, it accounts for the greatest shift in an area of business concern since the

[1] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf, p. 5

previous survey. It's important to point out that establishing the order of such business priorities continues to be hotly debated. Some people see interdependencies among these areas, leading to strong opinions that one priority must first be addressed before another can be addressed. For the purpose of this survey and its results, however, the increase in the ranking of the concerns for employee health and safety may suggest a growing recognition that safety and security risks are interdependent in the OT domain.

These combined concerns—reliability, availability, health and safety—are all interrelated. For many industrial control systems, network availability (in some cases high-availability [HA]) is essential to maintain ongoing safe operation. Furthermore, the availability of a system provides a means for operators to continue to monitor, diagnose, maintain and recover aspects of control and view of its operations, even when the process itself is not operating.

With more than a 30% increase (22.3% in 2019 vs. 17% in 2017), the business concern of meeting regulatory compliance is a likely indication that regulations have been effective in compelling companies to address security risks. However, contrast this with 43% decrease (8.2% vs. 14.4%) in the business concern to create, document and manage security policies and procedures. This reduction may indicate that companies consider (or perceive) their policies as well-vetted in meeting regulatory compliance demands where such requirements apply. It may also indicate some degree of maturity as companies shift from creating security programs to executing and maintaining their security programs.

However, for the other categories, SANS would have expected more of a shift in the ranking of the leading business concerns since the 2017 survey, especially in light of the threat categories that most concern respondents and that security responders will focus on during an actual incident or attack.

For example, although securing connections to external systems changed its ranking position to move up two places, the actual concern rating decreased, moving to 11.7% in 2019 from 13.7% in 2017. With OT's growing adoption of and reliance on off-premises services, a decrease in business concern such as this may be an early indicator that there's an underestimation of the risks these external connections introduce into an OT/ICS infrastructure. See Figure 3.

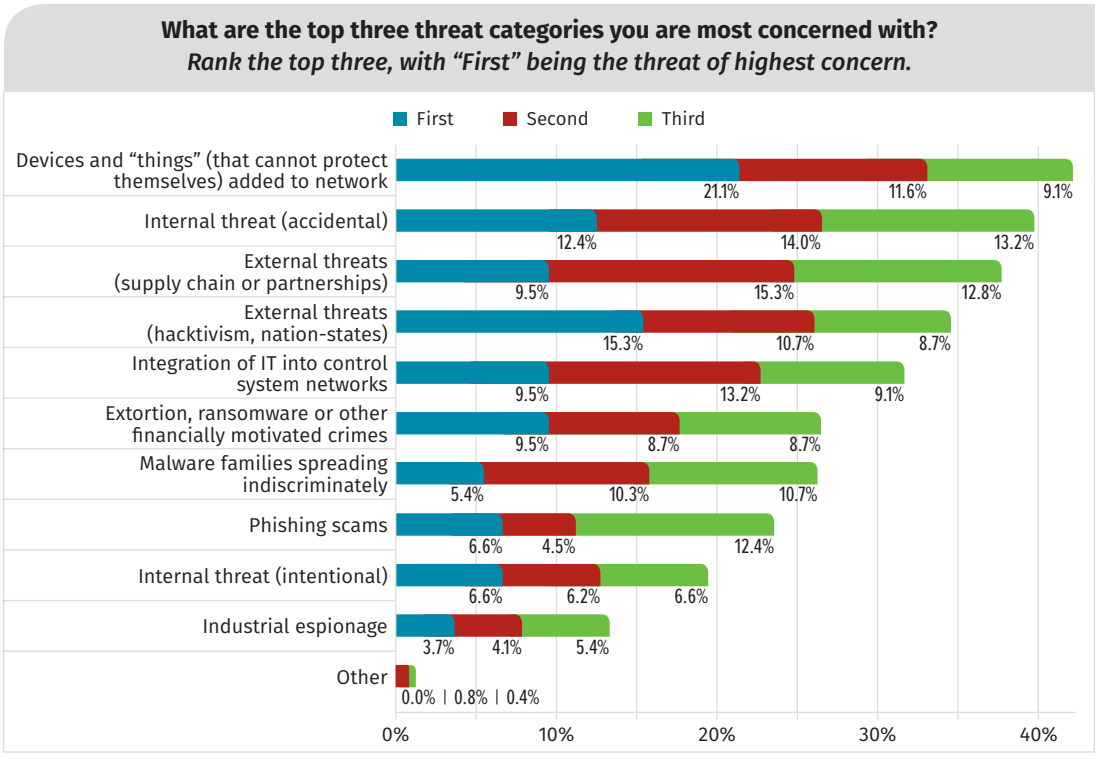


Figure 3. Leading Threat Categories

The leading concern, and top threat category overall, are devices and "things" (that cannot protect themselves) being added to the network, generating renewed emphasis on secure connectivity for an ICS infrastructure as well as the need to identify and characterize these items that are being attached to critical networks. SANS would expect that securing connections to external systems would figure more prominently as a 2019 leading business concern (see Table 1), especially as the integration of IT into control system networks is also one of the top five threat categories.

Interestingly, phishing scam concerns rated lower compared with other OT/ICS threats, yet there continues to be evidence from ICS attack research that this tactic is still a favored mechanism to establish an initial point of compromise and entry into many industrial control systems in the OT domain. In 2017, phishing scams were within the top five categories, with 30% of respondents expressing concern. For 2019, less than 25% of respondents expressed similar concerns. With more than 62% of perceived risks to OT/ICS being linked to people, the 2019 decrease in concern around phishing (i.e., campaigns intended to exploit people to gain system access) may lead to misplaced investments that leave OT even more susceptible in the future to phishing campaigns.

SANS recommends that the OT workforce be considered an important group to reach and include as organizations develop their comprehensive security awareness campaigns and educational programs around "securing the human."

The ICS community recognizes the importance of guarding against external threats. Supply chain relationships and partnerships also represent a leading threat category. An incident leading to disruption, damage or destruction that is encountered by an organization within a given supply chain can have a cascading effect on other members of that supply chain that rely, directly or indirectly, on the product or services of the affected party.

Some feel that cybercrime in the industrial sector has reached "pandemic proportions," fueled in part by the IoT explosion and the vulnerabilities devices introduce into the ICS.[2] Organizations must remain focused on the increasing potential of a nation-state attack,[3] which can damage or destroy critical systems and/or cause denial of service. Attackers look to monetize the access and control they gain into systems, devices and critical information. In some cases, ransomware is a means of holding digital data hostage. In other cases, adversaries are creating persistent denial-of-service conditions where operations are halted, or there's even the potential for an endpoint device or the production process itself to be altered. Even if disruption or physical damage isn't noticed by the asset owner or doesn't result, there's a possibility that proprietary information, including privileged credentials, might be harvested and exfiltrated to be used later for nefarious purposes.

Internal threats, although accidental, are the second highest overall threat category. However, the activities that can help remediate this concern—cybersecurity education and awareness, and security policy and procedure discipline—remain relatively low as a business concern and, therefore, not a priority despite being a leading initiative.

[2] www.advisen.com/tools/fpnproc/fpns/articles_new_20/P/336275501.html?rid=336275501&list_id=20

[3] www.darkreading.com/vulnerabilities---threats/destructive-nation-state-cyberattacks-will-rise/d/d-id/1332122

Internal threats, although accidental, are the second highest overall threat category. However, the activities that can help remediate this concern—cybersecurity education and awareness, and security policy and procedure discipline—remain relatively low as a business concern and, therefore, not a priority despite being a leading initiative.

Visibility into the network—including views of operational status and health of endpoints and the infrastructure, and precisely what a system's users are doing—can also help to mitigate risks of system downtime. Using such information aids networking, automation and security professionals in identifying processes and additional areas of potential security risk that might otherwise be overlooked. It also helps support these roles as they take proactive steps to counteract many security risks that can affect system reliability and availability.

How Are We Doing? Incidents and Compromise

One key question is whether there is actual improvement in securing industrial control systems and increasingly converged OT/IT networks and associated data and devices. A comparison between 2017 and 2019 reveals that, while the situation is not necessarily better, the trend appears headed in the right direction toward a maturing ability to understand and detect the new and evolving threats.

For those respondents reporting incidents involving their OT/control systems in the past 12 months, the number of incidents grew substantially in 2019 over what was reported in 2017. See Figure 4. Reasons may be due to the formalization of an incident response program, action taken or categorization of events as incidents that might otherwise have been ignored in the past, improved capabilities to detect incidents, or potentially increased exposure in OT attack surfaces. However, it's also likely there's a greater willingness by companies to publicly acknowledge aspects of security incidents, given that such events in the news are growing commonplace and, in some cases, both regulations and reputation-protections demand transparency and timeliness in disclosure.

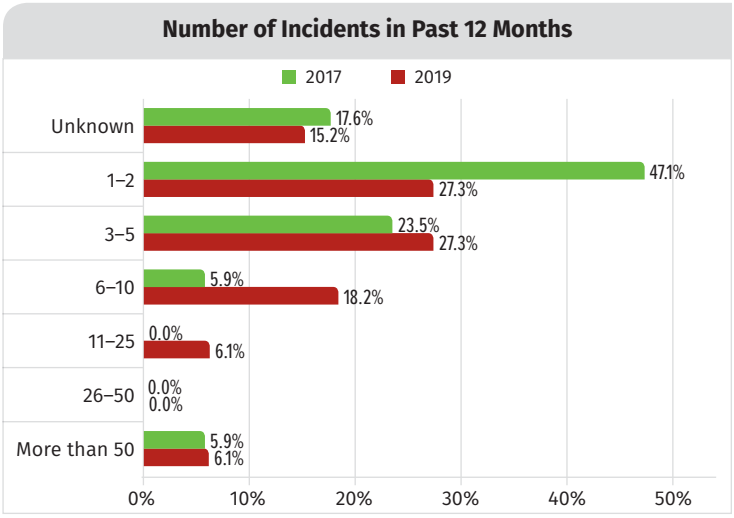


Figure 4. Comparison of OT/Control System Incidents 2017 vs. 2019

Table 2 compares the actors that were the source of OT incidents in 2017 and in 2019. We divided these actors into three broad sets: intentional malicious; unintentional; and both/unknown, where activities could be either malicious or not.

Several things immediately jump out in comparing 2017 and 2019 results. First, although malicious hackers are still the leading actor in 2019, there is a substantial rise in those external actors related to nation-state or criminal activity, as well as concerns over destructive actions by former employees and equipment providers. Second, the number of unknown sources has decreased almost by half. Finally, the unintentional activities by current service providers, consultants and contractors more than doubled.

Table 2. Actors Involved in Incidents

	2017	2019
Intentional Malicious		
Hackers	56.3%	44.8%
Foreign nation-states or state-sponsored parties	0.0%	27.6%
Organized crime	0.0%	24.1%
Activists, activist organizations, hacktivists	12.5%	17.2%
Competitors	12.5%	10.3%
Former employees	0.0%	10.3%
Former equipment providers	0.0%	6.9%
Both/Unknown		
Current employees	31.3%	34.5%
Unknown (sources were unidentified)	31.3%	17.2%
Unintentional		
Current service providers, consultants, contractors	12.5%	31.0%
Nonmalicious actors (internal)		20.7%
Current equipment providers	18.8%	13.8%
Domestic intelligence services	0.0%	6.9%
Suppliers or partners	12.5%	6.9%

While this data is telling, it's important to note that attribution of an attack is often one of the most difficult aspects of digital forensics and investigations to determine with certainty. It is most likely that respondents' answers represent their educated speculation as to the actual identity of a threat and are not necessarily always based on direct evidence.

In addition to increased exposure and/or threats, however, there appears to be an increased maturity in detecting OT-related security incidents. In 2019, 15% of respondents reported that they had experienced one or more security incidents as opposed to 12% in 2017, with a corresponding decrease in those that felt they didn't know (44% in 2017 dropping to 32% in 2019).

Being aware of OT-related incidents is becoming critical, especially with the growth in incidents being attributed to foreign nation-states and organized crime where disruption or destruction is the main objective. In 2019, 61% of all incidents had a disruptive effect on OT activities, with a disconcerting 27% of respondents remaining in the dark whether the detected incident was disruptive, or just how disruptive it was.

Along with this, however, comes a heightened concern about informal reporting of such incidents: 43% reported that they were unable to answer due to company policy as opposed to 25% in 2017. Despite the growing demand to publicly acknowledge incidents, a larger portion of respondents admit being restricted by internal policy from sharing such information outside of official organizational channels.

This increased maturity is also evident in the time between compromise and detection. While the real value for dwell time may remain unknown, if we consider time between compromise and detection as how long (on average) after the incident began the control systems security staff become aware of the situation, we can see a positive trend in 2019 from 2017 toward shorter and shorter times in the detection of anomalous activity. See Figure 5.

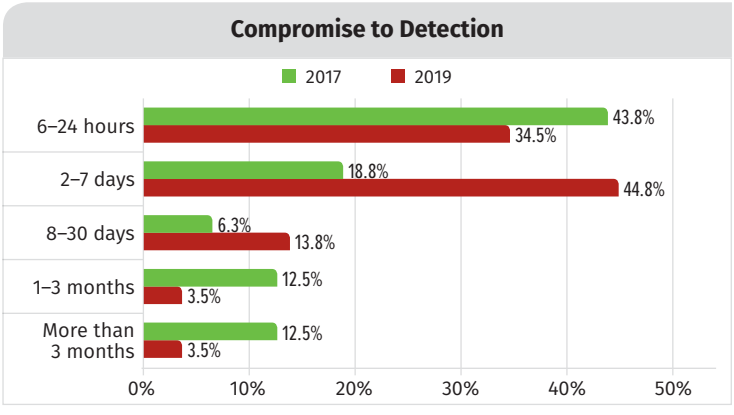


Figure 5. Time from Compromise to Detection 2017 vs. 2019

This, however, is only one piece of the complete timeline from compromise to remediation. In 2019, the specific results indicated a timeline range falling between four days (shortest) to 15 days (longest) based on the most commonly reported elapsed times for each key step. See Table 3.

Table 3. Timeline for Compromise to Remediation 2019

Step	Timeline	Percentage
Compromise to Detection	2 to 7 days	44.8%
Detection to Containment	6 to 24 hours	53.6%
Containment to Remediation	2 to 7 days	53.9%

Such a range could have a rapid cascading effect, given the real-time characteristics of ICS systems in the OT domain. Additionally, because many supply chain ecosystems operate just in time without slack, even a temporary disruption can ripple through a company and begin to affect other dependents. Real-time control systems demand the need to close the window of opportunity, possibly at higher rates than are required for traditional IT assets.

Another important consideration is being able to identify the initial attack vector (point of entry) involved in an OT/control system incident. For 2019, the leading vectors are physical, followed by remote access. See Table 4.

Table 4. Initial Attack Vectors 2019

	% Response
Physical access (USB stick, direct access to equipment)	56.3%
Remote access (bypassing intended architecture)	40.6%
Trusted remote access (through intended architecture)	37.5%
Service maintenance and consulting (configuration changes)	34.4%
Supply chain (i.e., altered/modified hardware or software; software/firmware updates and patches; maintenance tools/equipment)	18.8%

The actors involved underscore the need for increased security awareness training, physical perimeter controls, stronger physical asset management policies and procedures, asset inventories and identification, visibility into control system topologies, connected cyber assets and their device configurations. Physical access incidents are dominated by current workforce members (employees, service providers, consultants and contractors). Remote access events are overwhelmingly due to malicious hackers, while supply chain incidents are traceable to current service providers, consultants and contractors, as well as organized crime. See Figure 6 on the next page.

Architecture: Trends and Gaps

Looking at the OT/ICS control system capabilities from a risk and impact viewpoint helps determine and prioritize what is needed to protect OT/ICS systems. Areas of the greatest impact are not always tied directly to those of the highest risk. Compromise of field control network connections and embedded components are considered to have the greatest impact on production safety, security and process integrity, but are considered to be at a substantially lower risk than other assets. See Table 5.

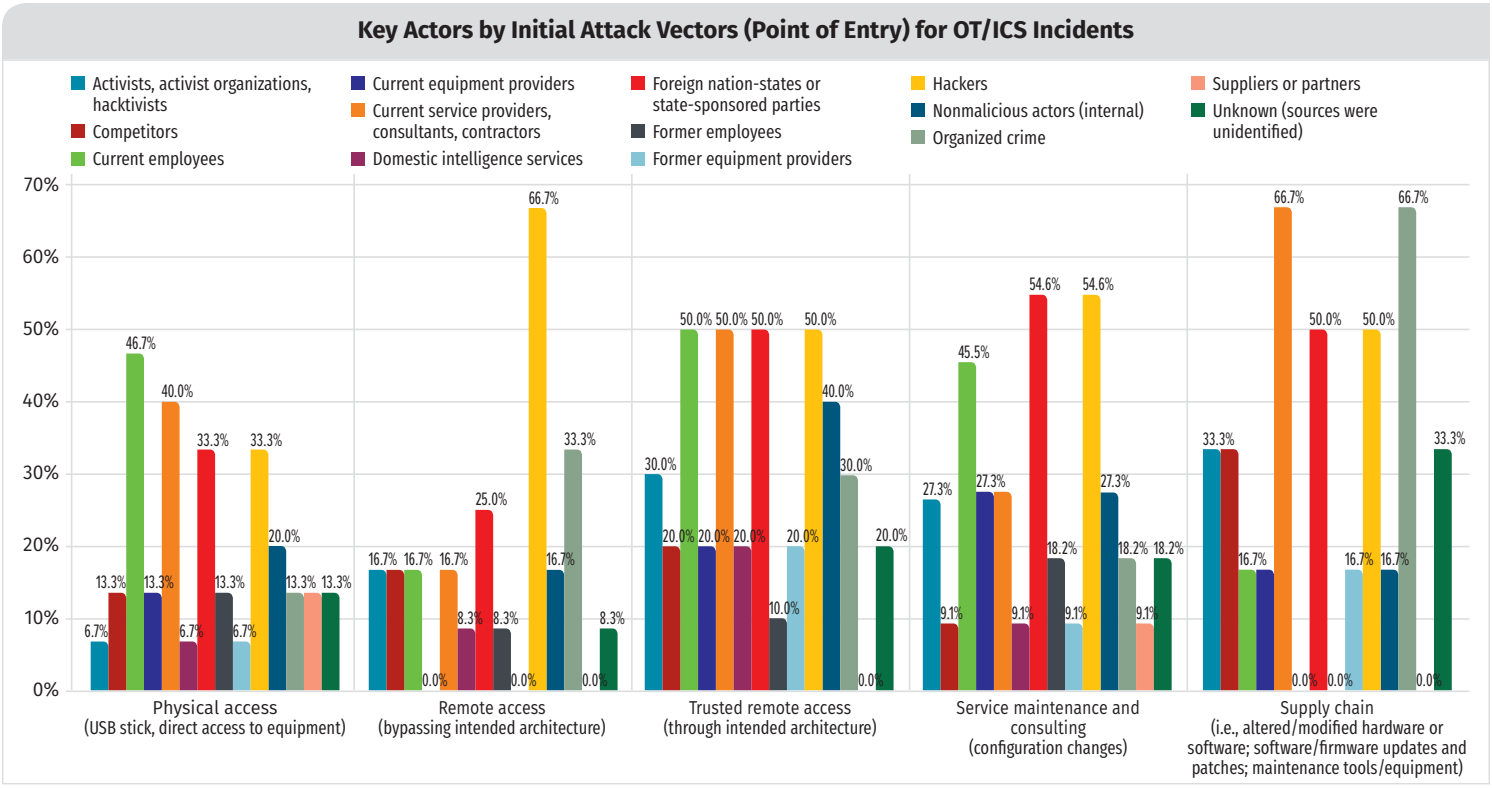


Figure 6. Key Actors vs. Initial Attack Vectors (Point of Entry)

Table 5. OT/ICS Control System Capabilities Compromise Risk and Impact

OT/ICS Control System Capabilities	Risk	Impact
Connections to the field control networks (SCADA)	36.1%	34.1%
Embedded controllers or components (e.g., PLCs, IEDs)	22.9%	33.2%
Server assets running commercial OS (Windows, UNIX, Linux)	57.6%	32.7%
Connections to other internal systems (enterprise networks, system to system)	42.0%	31.2%
Network devices (firewall, switches, routers, gateways)	30.2%	30.2%
Engineering workstations	38.0%	29.3%
Operator workstations	33.2%	28.8%
Control system communication protocols	23.9%	20.5%
Process control application	16.1%	20.0%
Field devices (digital sensors and actuators)	19.5%	19.0%
Remote access appliances (VPN)	25.4%	18.5%
Physical access systems	22.4%	16.6%
Wireless communication devices and protocols	27.8%	13.2%
Plant historian	14.6%	13.2%
Mobile devices (laptops, tablets, smartphones)	36.1%	12.2%
Analog modems	12.2%	6.3%
Other	5.9%	2.0%

Risks have dependencies. For respondents, server assets present the highest risk, due to the use of legacy OSes (e.g., NT, XP) and low rates for routine patching. If these server assets are within the OT architectural domain and managed by OT resources, as opposed to IT, there may be an even stronger likelihood for these devices to not be routinely patched. But strategically designed network and security architecture can enhance or mitigate vulnerabilities through how server assets are placed and protected at, or near, the boundaries between the IT and OT domains, specifically the industrial DMZ.

Therefore, it is not surprising that respondents consider connections to other internal networks as the next highest risk area. This, in turn, emphasizes the need for visibility to manage, monitor and maintain an asset across a boundary, especially when it's unclear whether IT, OT or both have responsibility for the asset and these activities.

The availability and adoption of software-defined networking (SDN) in the OT domain is a technology worth watching as an enabler for more flexible, dynamic logical segmentation of contemporary ICS. With SDN capabilities becoming more standard and available in newer network appliances, the options the technology offers have the potential to accelerate and simplify traditional approaches to logical segmentation, especially as the on-premises networking needs for new Industrial IoT solutions gain traction. SDN complements network access control (NAC), aids in enhancing network resiliency, and even provides a means for microsegmentation that continues to gain appeal as more and more devices are connected to ICS.

Looking at the security technologies currently in use, we see that effective basic security hygiene tools (access control, segmentation, awareness and endpoint security) are in use. Respondents told us that five of the 25 technologies available will be used increasingly in the next 18 months: OT/ICS network security monitoring and anomaly detection solutions, software-defined network (SDN) segmentation, security operations center (SOC) for IT/control systems, industrial DLP, and cloaking device IP addresses.

This evolution seems to indicate organizations are moving beyond the basic elements of network connectivity and control to more sophisticated approaches based on advanced technologies. However, this trend could also indicate that products such as network monitoring and anomaly detection solutions are becoming better understood and demonstrating tangible value to owners and operators as mainstream technologies, integral to the security of contemporary ICS. See Figure 7.

What security technologies or solutions do you currently have in use? What new technologies or solutions would you most want to add for OT/control system security in the next 18 months? ***Select only those that apply.***

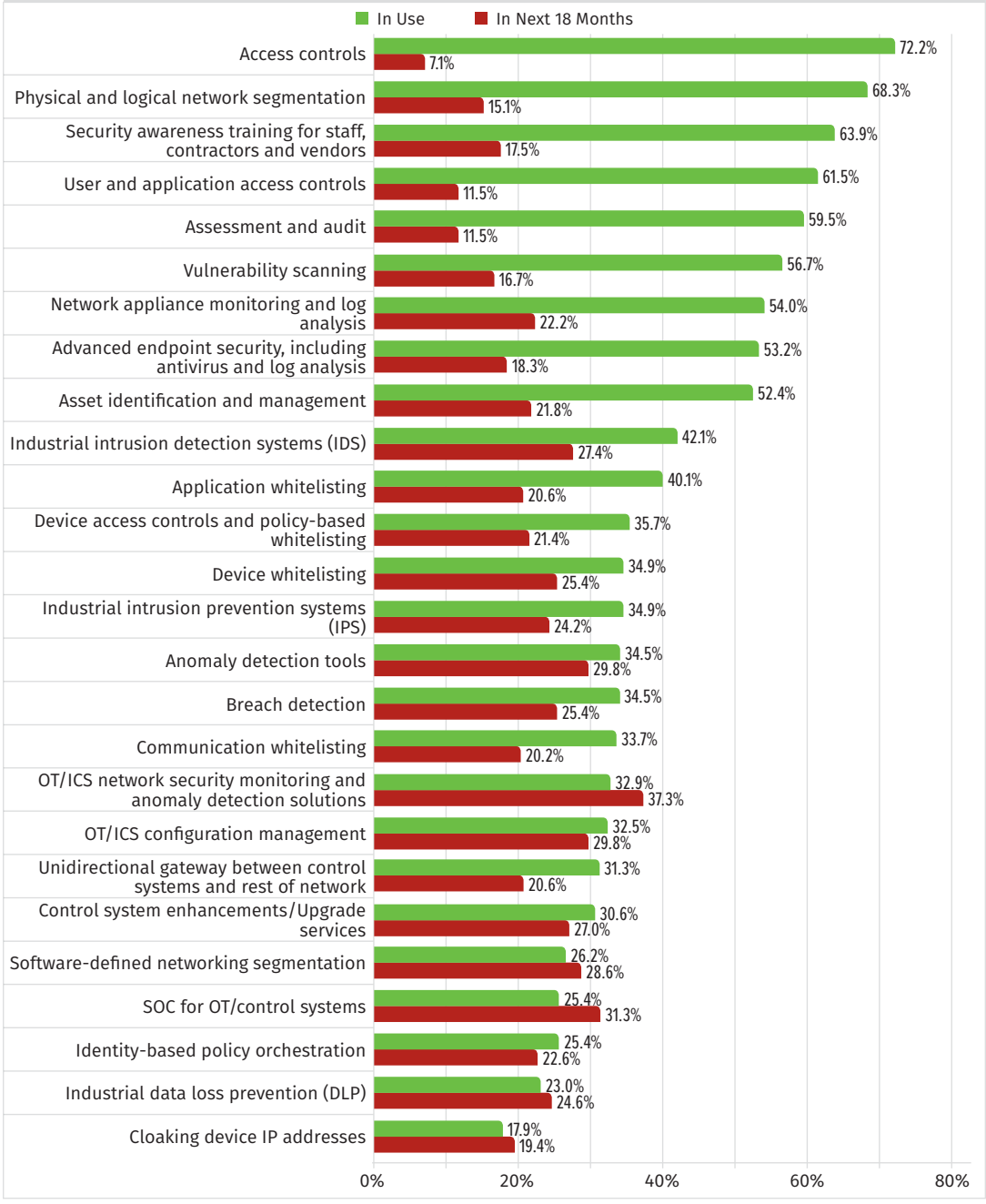


Figure 7. Security Technologies in Use and Planned

While the use of information collection and analysis solutions is growing, only 25% of respondents currently have embraced centralized management of their OT/ICS systems (i.e., an industrial SOC), implying that an investment is either being made at the point level, or that true integration (and automation) for OT/ICS security is still in the future. Organizations are now relying on dedicated (internal) resources for gaining visibility, with more than 40% looking toward centralization—either with increasing reliance on their IT infrastructure for OT/ICS security or an industrial SOC.

A Word About Mobile and Wireless

Mobile devices that replace or augment traditional desktops or fixed systems, while seen as one of the top five risk areas, are considered to have a low level of impact (almost last). While this reflects this survey's actual results, we note that mobile devices that replace engineering workstations have equivalent access rights and capabilities to affect operation of an ICS. Therefore, the impact represented by mobile devices should align more closely with engineering workstations, moving mobile devices into a leading position for impact as well as risk.

Mobile devices are not the only risk here. Noncellular wireless communication is the de facto method for mobile device connectivity. It also offers easy deployment options for the factory floor and production environments. However, most protocols—including WPA3, the next generation of protective protocols for Wi-Fi routers—have been compromised.[4] Considering that the expected life-span of an ICS is measured in one to two decades, unavoidably, a new system installed today with known vulnerabilities only becomes more vulnerable over time.

In addition, mobile devices, especially laptops, used in field technician work, represent the same risk and impact. Remember: If you have physical access to the asset, you own the asset, and you may in some cases be able to own the system!

As with the disconnect between the perception of risk for mobile devices noted previously, we see a potential issue with organizations not understanding the vulnerabilities inherent in wireless communication devices and protocols and, therefore, the potential risks. Organizations need to be aware of best practices for securing their nonwired connections, while also becoming proactive to plan and prepare for even faster product and technology changeover as end-of-useful-life situations arise.

Knowing the Boundaries (and Their Risks)

More than 60% of respondents have a well-defined (documented) system perimeter or boundary for their OT/control systems. For this 62% who know (and have documented) their system boundary, 57% connect their OT/control system DMZ to the enterprise business network, with another 35% connecting to the internet, either directly or through the OT/control system DMZ. See Figure 8.

Where do the connections from within your OT/control system boundary connect externally? ***Select all that apply.***

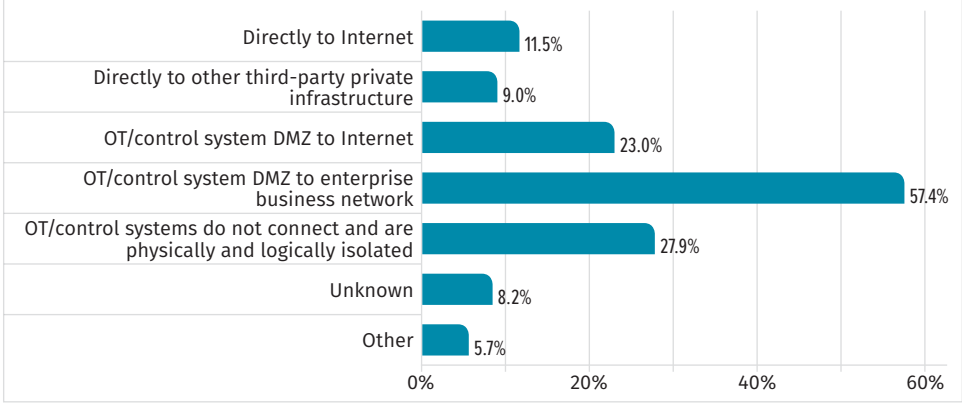


Figure 8. External Connections to OT/Control Systems

[4] www.schneier.com/blog/archives/2019/04/vulnerabilities_7.html

However, knowing the boundary also implies knowing what system assets lie within that boundary—the assets that comprise the system and must be protected. Only 36% of respondents claim that they have a comprehensive overview of all the elements of control system security for their enterprise or plant. The other implication that comes with a defined boundary is having control over what crosses the boundary. As cloud-based architectures emerge, the logic control functions of the ICS typically housed within a programmable logic controller (PLC) may more rapidly shift outside of a well-defined physical system perimeter into a virtualized or hybrid environment—demanding new approaches to maintaining the integrity of these devices.

Approximately 57% of connections are considered "wired" (cable modem, plain old telephone service [POTS], digital wired or leased fiber), while 37% are wireless (public or private cellular, satellite or radio). See Figure 9.

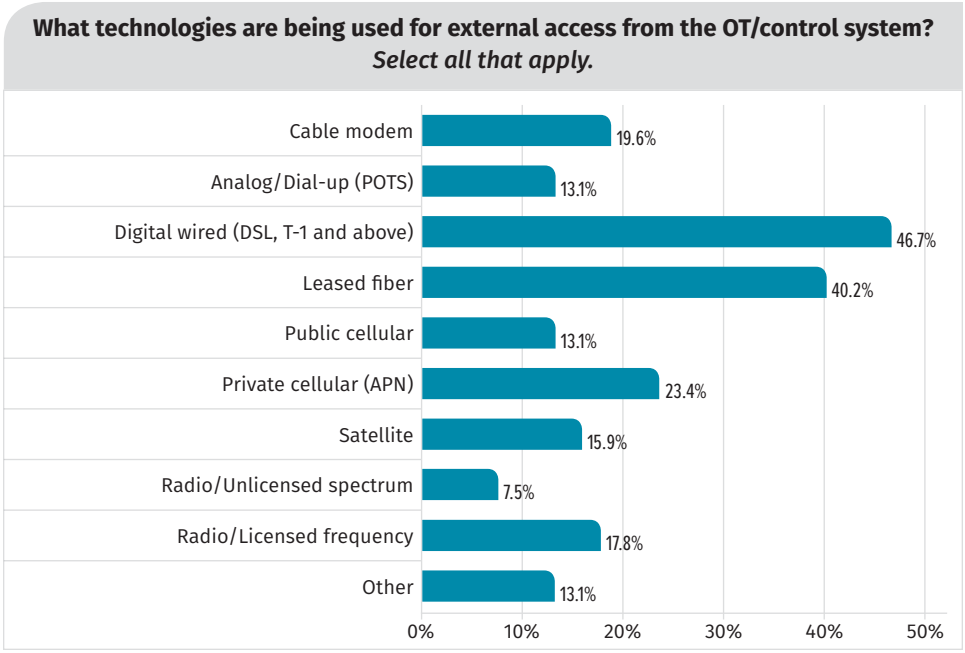


Figure 9. Communication Protocols in Use for External Connections

This points out another discrepancy in the results. Respondents did not rate wireless communications and protocols as subject to either high risk or impact related to compromise, yet arguably these represent some of the most rapidly evolving technologies, and sometimes the most reachable (without physical access) to an attacker in proximity to a system.

Extending beyond just mobile devices, wireless communication is also growing commonplace as a means to transfer information from sensor networks, including complex instrumentation. As such, a compromise in wireless communication for sensors and actuators could have a range of impacts on an ICS, even affecting safety, performance and quality. Periodic disruptions, loss of access to or view of diagnostic and prognostic information, even the potential for outright loss of integrity with sensor/actuator I/O (Level 0) that is essential to ICS operation could result from such a compromise. While the same effects of course apply to wired systems, wireless technologies extend network perimeters more broadly, often creating an attack surface by reducing the need for physical network access (see Table 5, earlier in paper).

More than 40% of respondents are using cloud-based services for a number of OT/ICS system functions. It is notable that our data shows that cloud-based services for "control system application virtualization, including remote logic" are employed by one of six (16.8%) respondents, leading to the growing importance of and dependence on cloud services.

Increasingly, the physical perimeter of the ICS is a poor representation of the actual logical perimeter. Over time, the notion of both a physical and logical network perimeter in ICS may evaporate altogether as control, configuration and data collection functions continue to fluidly move. See Figure 10.

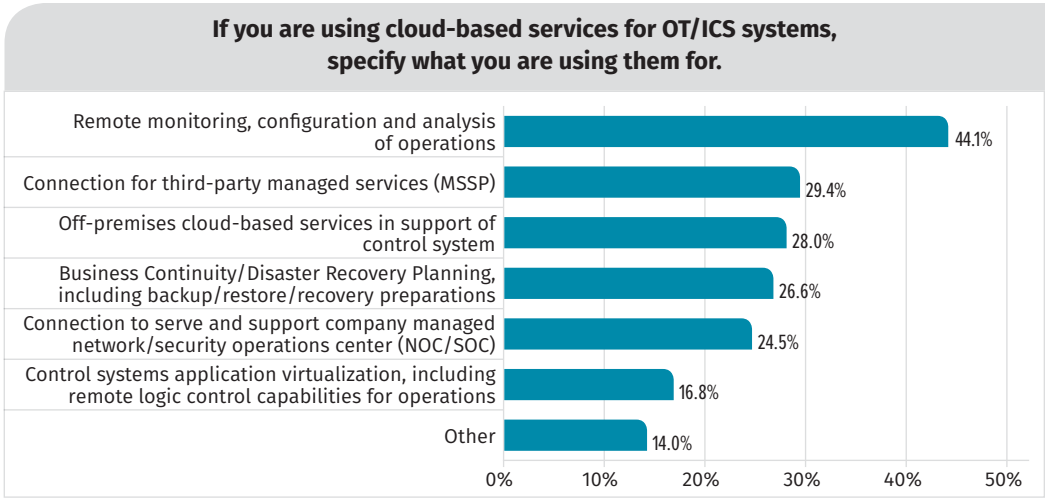


Figure 10. Use of Cloud-based Services for OT/ICS Systems

Another OT/control system critical interface (and boundary) is the connection between the internal OT/control system network and safety instrumented systems (SIS) and/or other functional safety systems. See Figure 11.

For cases where a restricted network (firewall) is employed to separate a control system network from an SIS, presumably the firewalls are configured to still allow some means for passing diagnostic information and potentially control commands across this boundary. Industry best practices show that any shared network between the OT/control system and an SIS is inadvisable, yet one out of seven respondents (15%) uses the shared approach, adding that the shared network is flat and unsegmented. With an additional 8% with converged or comingled logic and safety control functionality in control components, nearly 25% of respondents have a situation where an adversary has direct access to both critical control systems if it gains access to just one of them.

The use of cloud-based assets places additional reliance on the security of secure communication tunnels, often VPN connections. Remote access appliances (VPN) are currently not ranked as a leading area of risk or impact. However, SANS notes that organizations need to know how to remediate the risks involved in establishing a "trusted" VPN, especially as services migrate to the cloud.

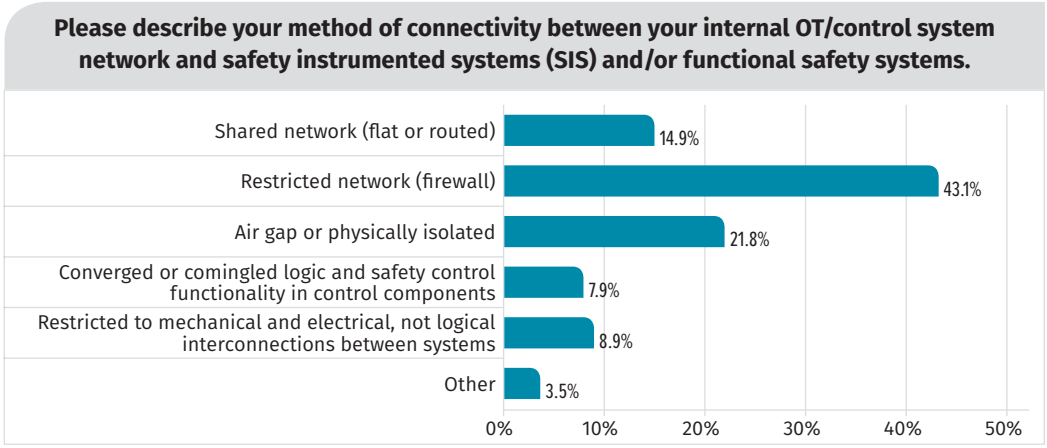


Figure 11. Method of Connection Between Internal OT/Control System and SIS

Gaining Visibility

Visibility is critical for managing OT/ICS systems. According to survey respondents, increased visibility into control system cyber assets and configurations is the top initiative organizations are budgeting for in the next 18 months. A first step in achieving visibility is identifying and understanding what initial OT assets (including a distributed control system [DCS], PLC, controllers, software, firmware and hardware) need to be prioritized and managed, while plans are made to span the balance of other assets over time.

While 62% claim they have documented the boundary of their OT/control system, only 36% of respondents claim a comprehensive overview of all the elements of control system security for their enterprise or plant. While 64% have identified

and inventoried over 75% of the servers and workstations associated with their OT/control systems, less than half have done so for control system devices (45%) and software applications (44%).

The next step is assessing what data should be collected from these assets and correlated to mitigate both the risk of compromise and the impact of exploitation. Comparing the data collection efforts against the risk and impact associated with OT/control system components (see Table 5, earlier in paper) reveals exceptional blind spots. The data collection process is very IT oriented, with roughly 70% of organizations collecting and correlating data from these computer assets and network devices.

Based on this data, it appears that surveyed organizations are not reaching down into the ICS infrastructure to monitor those assets considered to have the highest impact if exploited, specifically connections to the field control networks and embedded controller or components. See Table 6.

The Center for Internet Security (CIS) Critical Controls offers a framework of prioritized actions that have proven to deliver a highly effective and efficient level of defense against the majority of real-world attacks.[5] The first two CIS Controls (Inventory, and Control of Hardware and Software) focus on what is needed to establish a foundation for visibility. The premise is simple: You should be able to see what is on your network, know which systems belong to whom, and use this information to prevent unauthorized users from connecting to the network.

CIS recently released its Controls Implementation Guide for Industrial Control Systems, which provides practical steps to help ICS operators better safeguard control systems. This guide helps to define how automation and security professionals can apply security controls and best practices known to reduce risks and increase system availability, reliability and resiliency to cyber threats.[6]

Table 6. OT/Control System Components Support of Visibility

OT/Control System Components	Risk	Impact	Collection
Server assets running commercial OS (Windows, UNIX, Linux)	57.6%	32.7%	73.6%
Network devices (firewall, switches, routers, gateways)	30.2%	30.2%	65.3%
Connections to other internal systems (enterprise networks, system to system)	42.0%	31.2%	54.4%
Engineering workstations	38.0%	29.3%	50.3%
Operator workstations	33.2%	28.8%	48.2%
Remote access appliances (VPN)	25.4%	18.5%	43.5%
Connections to the field control networks (SCADA)	36.1%	34.1%	38.9%
Physical access systems	22.4%	16.6%	30.6%
Control system communication protocols	23.9%	20.5%	28.0%
Wireless communication devices and protocols	27.8%	13.2%	27.5%
Process control application	16.1%	20.0%	21.2%
Plant historian	14.6%	13.2%	19.7%
Mobile devices (laptops, tablets, smartphones)	36.1%	12.2%	19.2%
Embedded controllers or components (e.g., PLCs, IEDs)	22.9%	33.2%	18.7%
Field devices (digital sensors and actuators)	19.5%	19.0%	13.5%
Analog modems	12.2%	6.3%	4.7%

SANS finds it interesting that data shows the relative risk and impact potential attributed to field devices (digital sensors and actuators) are low, given that these various devices are the first and last step to link digital information to physical effects. The results indicate higher perceived risks and impacts with network connections than with field devices, yet the networks and their protocols are merely a means to an endpoint.

[5] https://www.dlt.com/sites/default/files/resource-attachments/White%20Paper%20-%20Focus%20on%20the%20First%20Six%20CIS%20Critical%20Security%20Controls.pdf

[6] www.cisecurity.org/webinar/cis-controls-implementation-guide-for-industrial-control-systems-launch-event/

Maintaining Visibility

The resources used by organizations to maintain visibility have shifted since the 2017 survey. Enterprises are moving away from reliance on external third-party service providers, and instead are using internal resources. Looking at the budget initiatives for the next 18 months shows that 30% are planning to invest in general cybersecurity awareness programs for employees and 29% in cybersecurity education and training for IT, OT and hybrid IT/OT personnel as opposed to 13% that plan to increase consulting services to secure control systems and control system networks.

This trend is evident in other ways. Organizations are depending on trained staff as first detectors and defenders. Since 2017, there has been a 23% increase in the use of trained staff to search out events, along with an increased use of anomaly detection tools to identify trends. See Table 7.

Table 7. Sources of Intelligence 2017 to 2019

Source of Intelligence	2017	2019	% Change
We rely on our trained staff to know when to search out events.	37.8%	60.4%	+22.6%
We use third-party intelligence provided by our security vendors.	53.8%	51.8%	-2.0%
We work closely with government agencies to ensure up-to-date intelligence is available.	38.7%	44.7%	+6.0%
We actively participate in industry information-sharing partnerships.	46.2%	44.2%	-2.0%
We use anomaly detection tools to identify trends.	35.3%	44.2%	+8.9%

This trend indicates a more proactive, rather than reactive approach to OT/ICS security. In 2017, 53% waited for their ICS vendors to inform them of vulnerabilities in their control system (or to supply a patch). In 2019, 33% rely on their vendors and supplier to inform them of a potential weakness. Reliance on vendors and suppliers during FAT and SAT has fallen from 40% in 2017 to 28% in 2019. Slightly over 50% are using continuous active monitoring to detect vulnerabilities. See Figure 12.

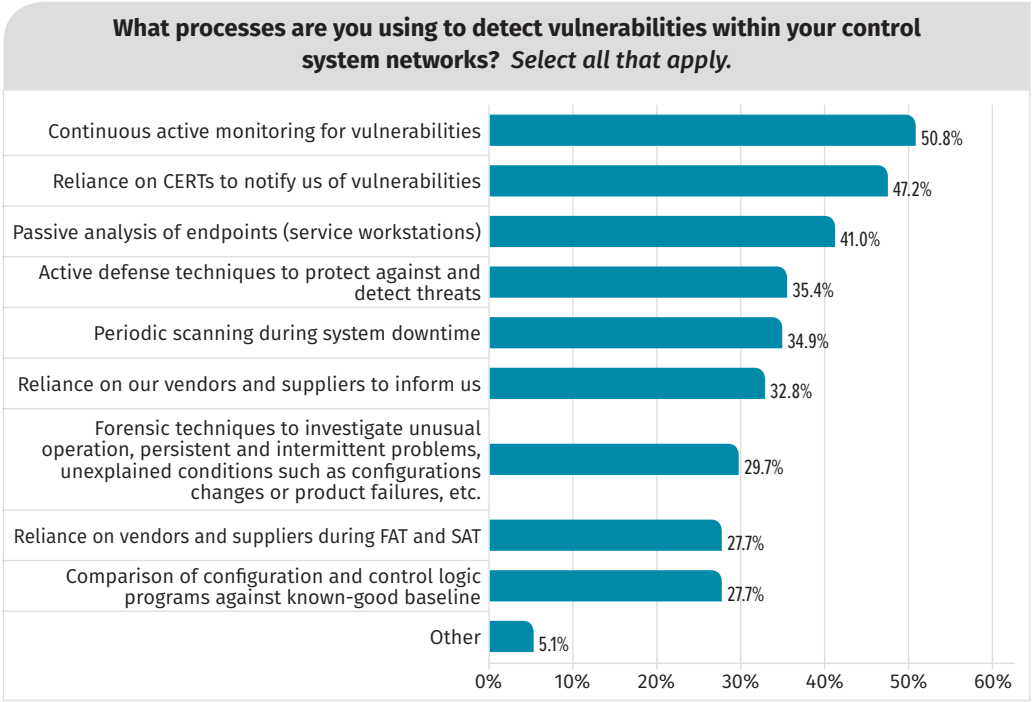


Figure 12. Processes to Detect Vulnerabilities Within Control System Networks

Improving Outcomes: People and Process

To improve security, organizations need to know how they are doing with regard to the security of their assets and infrastructure. The second top budget initiative, selected by 37%, is performing security assessment or audit of control systems and control system networks.

The terms *assessment* and *audit* are different but complementary processes. Together, they define how things should be done and how things have been done. Audit implies a formal procedure, often carried out by an independent third party, which evaluates policies and processes for alignment to or compliance with requirements, specifications, standards, processes or other agreements, generally carried out in a highly structured manner. Assessment implies evaluation, also often formalized and standardized, of organizational processes and practices against a reference model (e.g., "process reference model"), and is often an internal function at an organization.[7] Furthermore, assessment is also a fluid and agile process to evaluate actual states and conditions that may be overlooked, not well known, undocumented, or may not meet intended or desired operation, or it may even surface unforeseen areas and issues of concern.

The Process of Evaluation and Improvement

Most respondents (69%) report their organization has conducted a security assessment of its OT/control systems or networks in the past year, with 47% leveraging an external consulting firm or service provider achieve an independent assessment. However, assessment team composition for the past 12 months demonstrates yet again the increased use of internal IT and/or OT resources, another indication of the growing capabilities and confidence in internal resources to conduct risk assessments. See Figure 13.

Assessments can occur many times during the system life cycle: initial procurement, testing patches, periodic evaluation as to how the system is performing, and meeting external regulatory compliance.

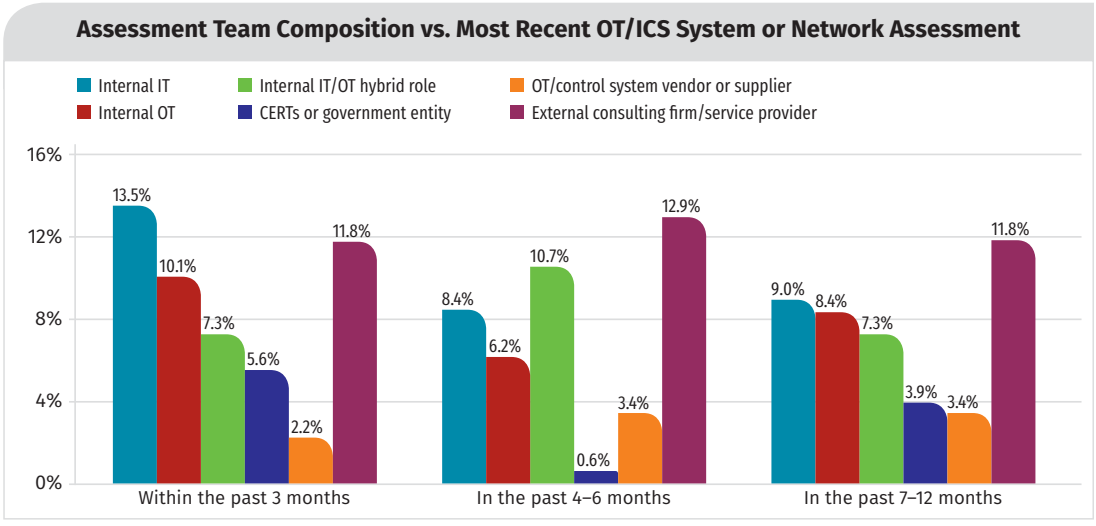


Figure 13. Assessment Team Composition for Assessments within Past 12 Months

Qualification of security controls by vendors and suppliers is rated highly important by the majority of respondents (41%) and mandatory by another 27%. Yet only 39% of respondents have an established set of requirements, including conformity to established standards (ISA/IEC 62443), during procurement. Organizations need a

[7] www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf

formal assessment process for their potential partners. Lack of a formal process in establishing requirements and comparing possible solution vendors can lead to technical incompatibility and support limitations down the road, especially for organizations that have highly integrated and complex environments, both from the technical and human infrastructure perspectives.

Component testing is another form of assessment, one that is necessarily based on the visibility achieved through vulnerability scanning and threat intelligence. Most (41%) claim they pretest and apply vendor-validated patches on a defined schedule. We consider pretest as a strong positive that ensures compatibility and avoids potential disruption. However, in an OT/control system environment, a potential exists for a long delay between when an applicable patch is known and when it can be applied without disrupting the operational mission (e.g., scheduled downtime).

The application of "layer additional controls instead of patching" is low, only 7%.This may be a missed opportunity to mitigate risk, especially in legacy environments where ICS systems may be too old to patch (e.g., the operating system is past its end of life). Often, compensating controls can provide a means for an ICS to continue its uninterrupted operation until such time as a patch or upgrade can be made. In some cases, based on assessed risk and known potential impact, compensating controls applied around a known vulnerability may prove a better solution for addressing associated security risks than applying the product update. Careful considerations such as these to manage risk throughout the life cycle of OT/ICS systems are all good examples of how differences in risk management are approached between the IT and OT domains.

Regulations and standards provide a strong basis for conduction audits and assessment. Table 8 shows the top 10 regulations, standards or best practices used by respondents.

Reviewing the use of these top 10 regulations, standards or best practices against when the most recent assessment was conducted, we see that the use of the CIS Controls has steadily increased from more than 24 months ago, peaking in overall use for assessments conducted in the past four to six months and that ISA/IEC 62443 has gained in popularity within the past three months. See Figure 14.

Table 8. Top 10 Regulations, Standards, Best Practices Used

Rank	Regulation	% Response
1	NIST CSF (Cyber Security Framework)	38.1%
2	ISO 27000 series	32.0%
3	NIST 800-53	31.4%
4	NIST 800-82	30.9%
5	ISA/IEC 62443	30.4%
6	CIS Critical Security Controls	29.9%
7	NERC CIP	23.7%
8	GDPR	15.5%
9	C2M2 (Cybersecurity Capability Maturity Model)	10.3%
10	NIS Directive (EU)	8.3%

Which cyber security standards, regulations or best practices do you map your OT/control systems to?
Select all that apply.

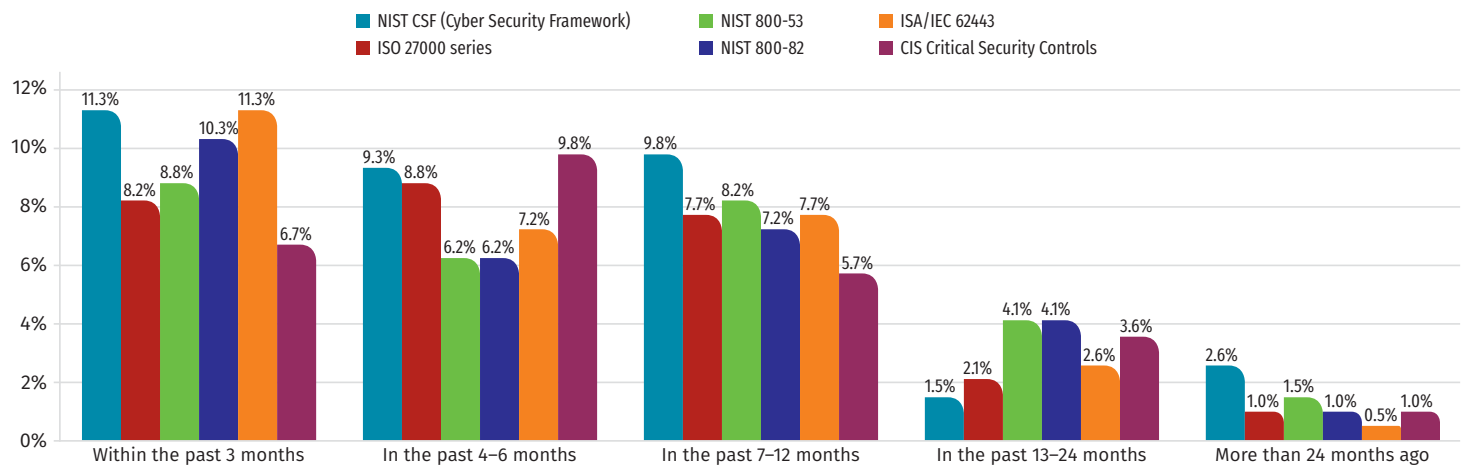


Figure 14. Trends in Use of Cyber Security Standards, Regulations and Best Practices

Bridging IT and OT Initiatives

Bringing OT/control system security in-house will necessarily accelerate IT and OT team convergence as organizations work to align their corporate priorities and maintain their budgets. This raises the question as to who is in control of major initiatives in each domain and how effective this approach is in balancing resources against investments.

Historically, engineering-focused OT has concentrated on safe, reliable and profitable production and has been unaccustomed to information governance issues relating to compliance. On the other hand, IT—which generally had a longer history of information security and protection, assessment and audit—has traditionally lacked the situational awareness and appreciation for tangible physical impacts that can result and must necessarily be considered for the operational, automated domain.

Collaboration and communication must occur between both camps to avoid conflict and to ensure that contemporary business objectives can be met. This is especially true as more OT architectures shift to take advantage of off-premises services, and as Industrial IoT (IIoT) solutions are adapted into operations that require persistent internet connections that pass through IT and deep into the OT domain.

The essential need for IT and OT collaboration and communication often shows itself clearly during incident response activities. Close to 60% of organizations in this survey first consult a variety of internal resources when signs of an infection or infiltration of their control system cyber assets or network are detected. Forty-five percent involve their company leadership, including the legal department, indicating that organizations are aware that accountability and culpability for security are linked to C-suite positions.

From policy and implementation standpoints, results indicate IT retains the upper hand. For 54% of organizations, the CISO/CSO establishes security policy around OT assets, while the IT manager (42%) bears primary responsibility for implementation of the related controls.

On the other hand, operations and IT jointly control the actual budget, where operations maintains an upper hand. Comparing 2017 to 2019, SANS notes that the allocations for both operations and IT have grown, with a corresponding decrease in the shared budget. See Table 9.

Table 9. Organization Controlling OT/Control System Budget 2017 vs. 2019

Organization Controlling Budget	2017	2019	% Change
Operations	30.8%	48.7%	+17.9%
Enterprise IT	17.1%	31.6%	+14.5%
Shared budget between IT/OT	38.5%	29.4%	-9.1%

This dichotomy emphasizes how essential it is that a good relationship exists between OT and IT, especially where OT can help IT gain the situational awareness to address the unique risks for OT/control systems. According to 65% of respondents, the current collaboration level is moderate or better, and the trend is definitely toward growing collaboration.

Since 2017, there has been progress by organizations either adopting or planning to adopt an ongoing implementation and management strategy or plan that addresses OT/IT convergence. See Table 10.

Table 10. Adoption of OT/IT Convergence Strategy 2017 vs. 2019

Organization Controlling Budget	2017	2019	% Change
We have no strategy nor plans to develop one.	18.1%	15.7%	-2.4%
We have no strategy but are developing one.	31.0%	33.0%	+2.0%
We have a strategy and are implementing it.	37.9%	30.9%	-7.0%
We have a strategy in place.	12.9%	20.4%	+7.5%

It is also imperative that the C-suite has proper visibility into IT- and OT-related activities, especially because the budget may be spread across numerous activities. The absence of a well-thought-out IT and OT implementation and management strategy can lead to wasted investments and unknown additional risks to OT/control systems that may be otherwise avoidable.

The Biggest Risk: Not Necessarily the Biggest Budget

As in 2017, most (44%) did not know their budget for OT/controls systems, but for those that did, budgets were weighted toward less than $1 million. For 2019, 42% reported an increase in their control system security budget for the past two years as opposed to 29% in 2017. See Figure 15.

The biggest identified risks—people—do not necessarily equate to the largest budget being allocated to that risk category. Although people account for the highest risk area (62%), most budgets allocated to this category are less than $100,000 USD. See Figure 16.

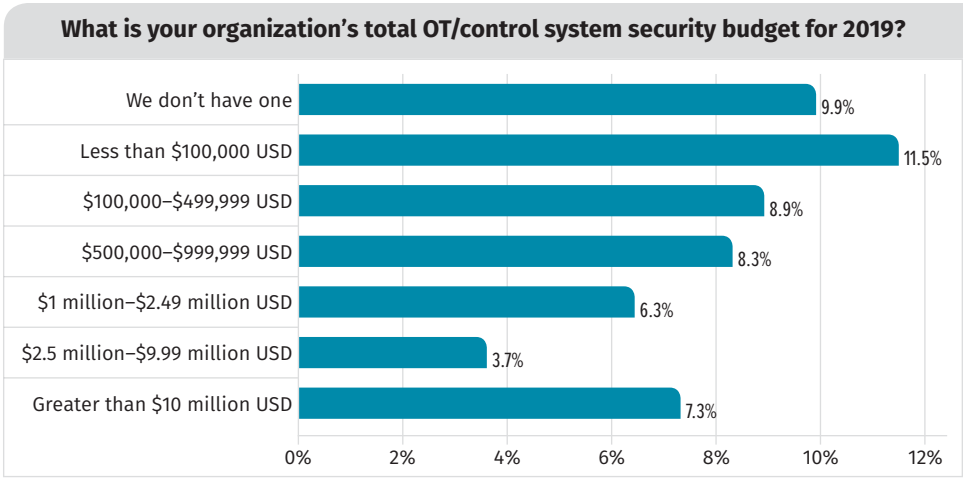


Figure 15. OT/Control System Security Budget for 2019

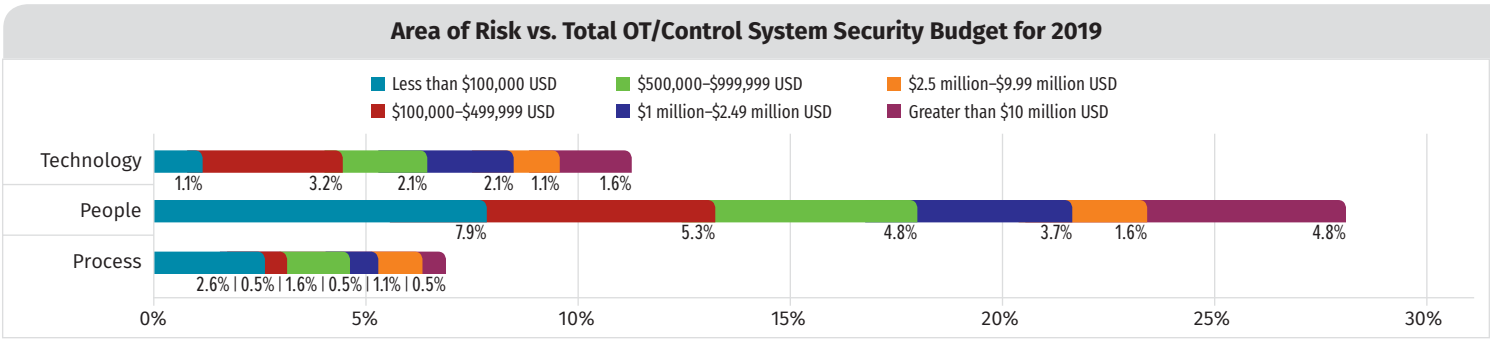


Figure 16. Risk Category vs. Budget for 2019

This raises an interesting question as to where organizations are placing their efforts and making investments, because larger investments are more heavily weighted toward technology. While people may well be viewed as a leading risk factor, at the same time people can also be the leading factor to mitigate and avoid risk when they become more aware and vigilant. Although technology may not be considered as great a risk for compromise as people, it's important to note that the selection, implementation and overall use of technology relies directly on decisions of people.

Figure 17 shows the emphasis within the budget area allocated to employees for the security of control systems and control system networks. Again, reliance on training the internal resources dominates. Only 16% are considering utilization of external consultants and service providers, as opposed to the 21% who are looking to increase staff.

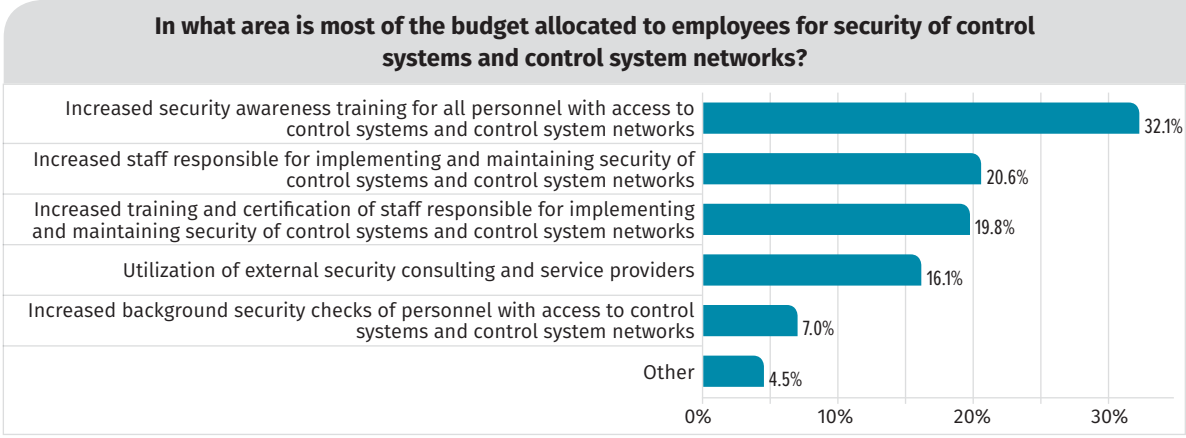


Figure 17. Budget Allocation to Employees

As one survey respondent noted in a comment, the emphasis should be to first build an efficient awareness program that includes higher management, then to develop an efficient working methodology between the IT and OT teams, including a good curriculum that addresses training and integration between the areas.

Conclusion: A Call to Action

Effective OT/control system security begins with a clear vision and strategy of where the organization is and where it wants to go. It depends on the architectural soundness of the entire design and its operations that span OT and IT, and are even external to the enterprise—not just the hardware and software of the system and/or network, but the people and processes as well.

In 2019, the majority of organizations are either adopting or planning to adopt an ongoing strategy or plan that addresses convergence. Based on observations gleaned from the survey, SANS would like to offer advice that organizations should take into account as they shape and implement their convergence strategy. See Table 11.

> *The greatest challenge is around governance and workforce skills/manpower. From a technology perspective, moving from away from simplistic blacklisting antivirus (AV) to next-generation antivirus (NGAV) solutions, risk measurement and analysis, and comprehensive asset inventories are the biggest challenges for this year.*
>
> —Survey Respondent

Table 11. Strategy Advice for Convergence

Strategy Pillar	Key Observation	Advice
People	Roles and responsibilities around policy, implementation and budget reflect potential conflicts that can impede convergence.	Develop a specific action plan as to how OT will operate with IT into the future, giving both the opportunity to work together, learn from each other and continually improve the OT/control system maturity level of the organization. Align business concerns with the current threat environment to ensure that awareness and education of your hybrid workforce is actually achieved.
Process	Processes should lead, not lag, technology as a factor in developing strategy, since automating a poor process can increase the risk to organizational safety and security.	Invest in a formal assessment of your "as is" processes and identify the weak links before creating a "to be" environment, including procuring technology. Treat an assessment done with internal resources as if it were a formal audit where you are paying an external third party.
Technology	Barriers to proper security hygiene of the OT/ICS infrastructure are evident, such as absence of asset identification and inventory and the blurring of the OT/IT network boundaries.	Start with basic hygiene, considering for example the top five CIS Critical Controls as a basic road map that provides a solid foundation for improved security and supports an important first step: improved visibility into assets and infrastructure. Evaluate factors affecting the current infrastructure: use of mobile and wireless, changes to operational procedures in light of moving to cloud services, and completeness of documentation. Establish an inventory of OT assets before expanding the use or expansion of industrial automation and control technologies to support operational processes or production; establish the process of maintaining an OT/ICS asset inventory over time, and also baseline operational known-good states for future comparison.

Perhaps the initial question to be asked is, "Where should my organization spend its first dollar on convergence to gain the greatest value?" Based on this survey's results, the answer is simple and definite—people. Knowledgeable people are needed to make qualified decisions around both process and the supporting technology. And, as we have seen, the budget to increase staff understanding, awareness and skills does not necessarily require the largest budget commitment.

> *Do not underestimate that your "biggest challenge with integrating [will be] changing the mindset of both IT/OT to think like each other and leverage each other's expertise."*
>
> —Survey Respondent

About the Authors

Barbara Filkins, a senior SANS analyst, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

Doug Wylie directs the SANS Industrials and Infrastructure business portfolio, helping companies fulfill business objectives to manage security risks and develop a security-effective workforce. His lengthy career spans a wide array of industries. He served as Rockwell Automation's director of product security risk management, where he founded and led its industrial cybersecurity and risk management program. Doug works around the world with companies, industry and standards bodies, and government entities to help safeguard converged IT-OT systems from contemporary cybersecurity threats. He holds the CISSP certification and numerous patents, as well as being an accomplished writer, speaker and presenter.

Jason Dely, SANS instructor for ICS515: ICS Active Defense and Incident Response, directs the ICS and critical infrastructure services and product business for Cylance Inc. He has more than 17 years of operational, technical and security experience, spanning multiple industry verticals, such as power utility, water utility, oil and gas, manufacturing, mining and chemical.

Sponsor

SANS would like to thank this survey's sponsor:

radiflow
Secure your Assets