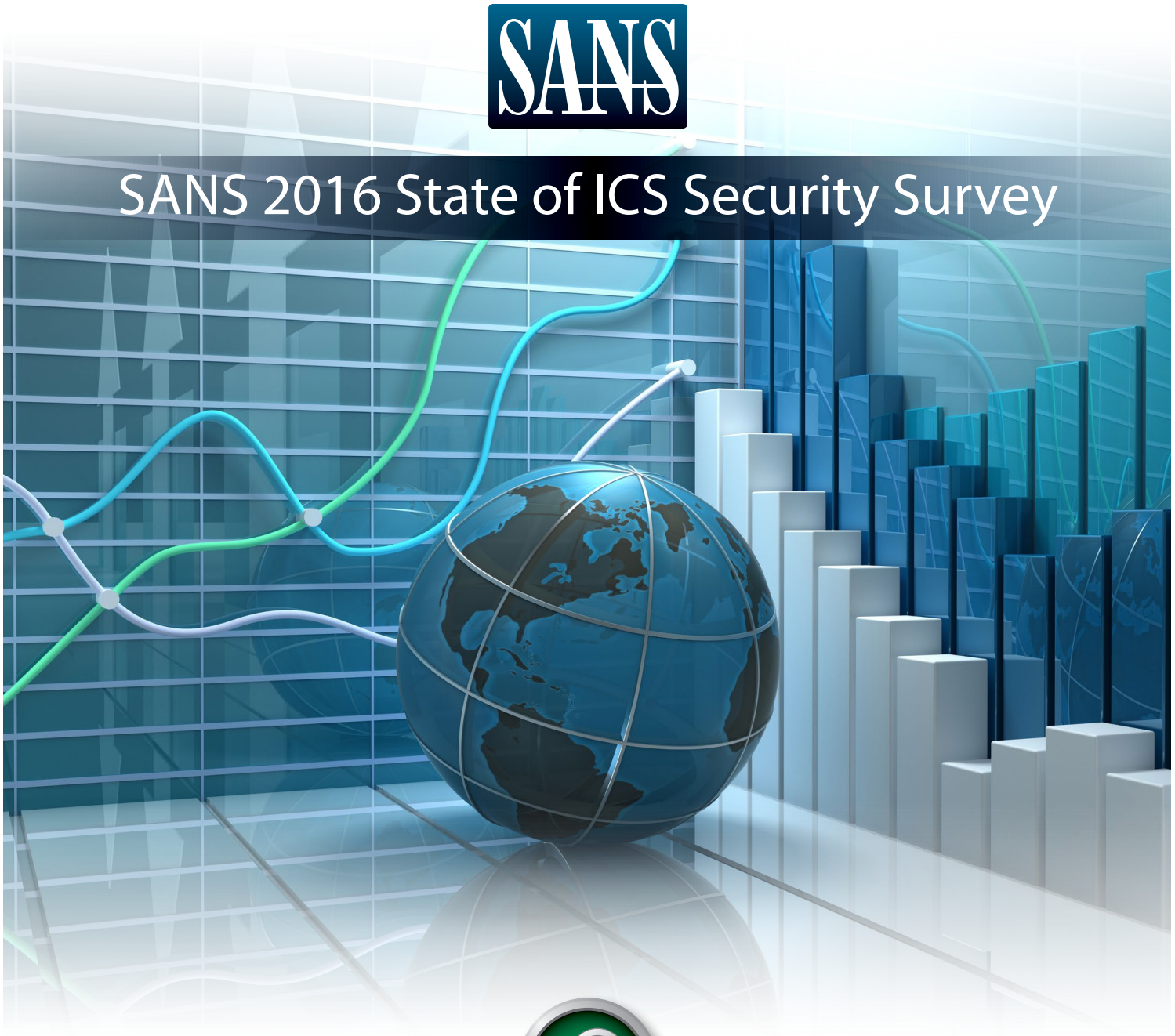


SANS 2016 State of ICS Security Survey

A SANS Survey

Written by Derek Harp and Bengt Gregory-Brown

June 2016

Sponsored by
Belden

Executive Summary

It is our intent, and the intent of SANS ICS as a whole, to not only gain information and report on the state of industrial control system (ICS) security, but also to contribute toward improving that condition. Unfortunately, this report contains some disappointments on this score. Analysis of survey data collected between January and April 2016 indicates that security for ICSes has *not improved* in many areas and that many problems identified as high-priority concerns in our past surveys remain as prevalent as ever. In this report, therefore, we focus on identifying and prioritizing recommendations to address the greatest concerns.

Key Findings

perceived severe or high levels of threat to control systems, up from 43% in 2015

place responsibility for threat intelligence on internal staff, and 43% place responsibility for security assessments on internal staff

consider their supply chains or partners a top threat vector

Contrary to other industry verticals, security incident information-sharing is down

Planned ICS security improvements are behind schedule

Control systems increasingly permeate all aspects of modern societies. Several ongoing and accelerating trends of networking devices together have grown from niche tech geek topics to general public awareness. Driven by market forces and technological considerations, the wired and wireless web of consumer devices, often referred to as the Internet of Things (IoT), and the interconnection of industrial equipment, termed the Industrial Internet of Things (IIoT), encounter each other with greater and greater frequency as we approach a hypothetical future state of total connectivity, the Internet of Everything (IoE), and the distinctions between them tend to blur.

In this survey we focused on the security of clearly industrial control systems: the supervisory control and data acquisition systems (SCADA), distributed control systems (DCS), process control systems (PCS) and building automation/control systems (BAS/BCS) used to manage automated manufacturing, pharmaceutical processing and food production, as well as critical infrastructure, such as water, oil and gas, energy, utilities, and aerospace and defense networks. Systems that manage traffic, transit and transportation, and keep the lights on, the data flowing, and the water clean and running—all out of the public eye—are the highest priority. SANS took on the task of investigating and improving ICS security several years ago, by forming the SANS ICS Security practice to develop and deliver training and by launching the first annual survey in 2013.

Participant Demographics

The great majority of the 234 participants who completed the survey work for companies headquartered in the United States (69%), with the remainder distributed widely around the globe.

Representation

The single largest group of participants works in the energy/utilities industry (25%), with the next strongest representation being in business services (10%). Although not many in total numbers, we observed a notable increase in responses from individuals employed as educators, which may be a leading indicator of efforts to address the security skills labor shortage (see Figure 1).

What is your organization's primary business?

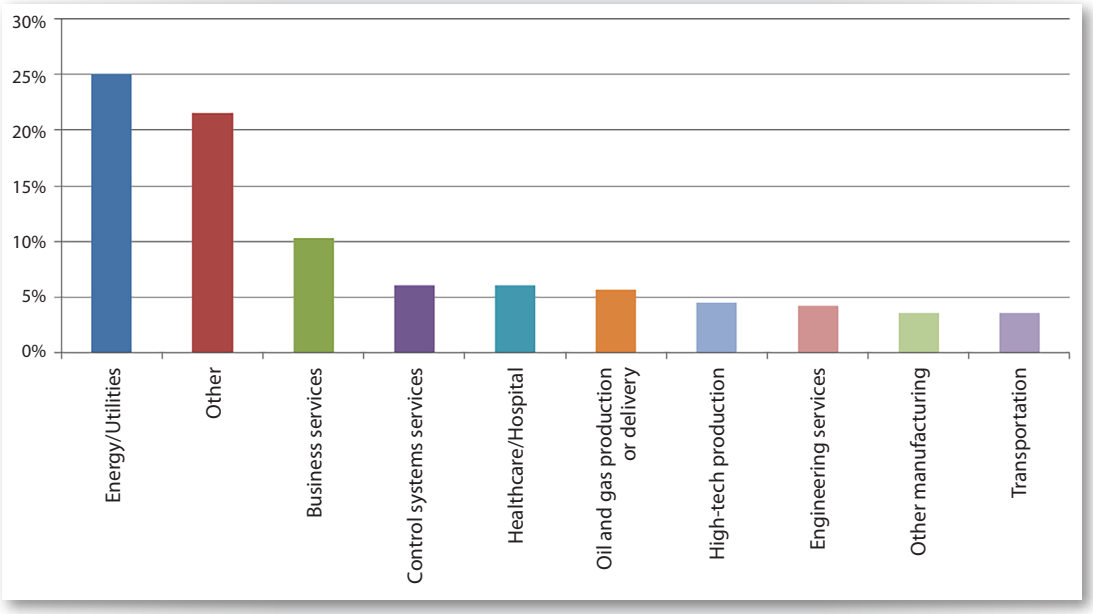


Figure 1. Top 10 Industries Represented

Size of the organizations represented was fairly evenly split, with 39% having fewer than 1,000 employees, 31% having 1,000 to 10,000 employees, and 31% with more than 10,000. In 2015, organizations tended to be slightly larger, with 30% representing small organizations, 34% representing medium-sized organizations, and 36% representing large ones.

Possibly correlating with the increased allocation of funds to security, the largest percentage of respondents who knew about their budgets worked for organizations with budgets in the $500K to $999,999 range (see Figure 2).

What is your organization's total control system security budget for FY2016?

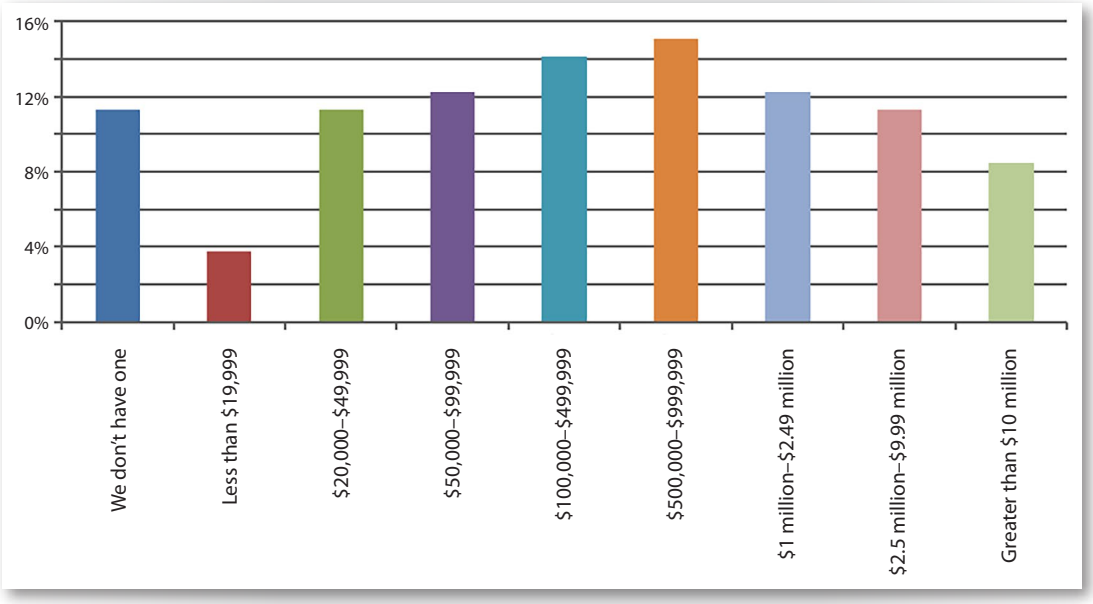


Figure 2. Control System Security Budgets

Roles and Certifications

Once again this year the largest group of participants hold security administration/analyst positions (29%). We also saw several encouraging new titles in the "Other" responses, including ICS cyber security program manager, ICS security project manager, IT/OT (IT/operational technology) architect, and director of cyber security for building and facilities systems.

Having the largest group of security practitioners or stakeholders among the administrator/analyst segment reinforces the need for more executive ownership of security strategy. More often than not, CxOs, managing directors, and even board members are held liable at all stages of a security incident. Businesses, therefore, need to engage proper representation of budget managers and senior stakeholders across the enterprise. This will help to ensure proper budgeting for the operational security needs of the business.

We added a question this year to look into how many of our respondents have responsibilities in both IT and ICS/OT security, and it appears that 46% straddle that line.

A number of this year's survey participants have gained control system security certificates or achieved certification in this area. The largest number (66%) hold Global Industrial Cyber Security (GICSP) certifications, with 28% holding the ISA99 Cybersecurity Fundamentals Specialist Certificate, as illustrated in Figure 3.

Please indicate what certifications you hold. ***Select all that apply.***

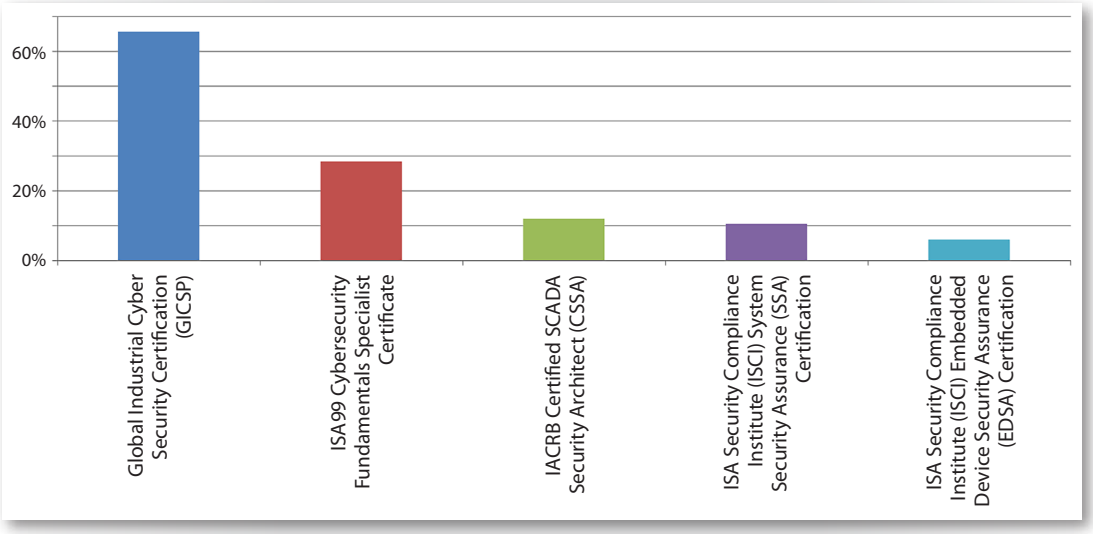


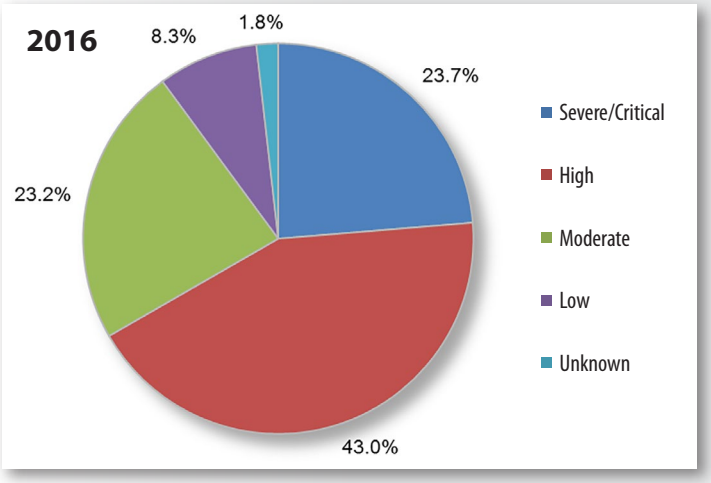
Figure 3. Respondents' Certifications

Risk calculation is a mathematical exercise. For each threat considered, the product of estimates of potential impact and likelihood of occurrence within a given period of time guides selection of strategies to manage related risk. The cyber threat to ICS systems is such a recent development and is changing so rapidly that very little hard data exists to feed those calculations; this strengthens the influence of subjective perceptions on the process in these situations.

Threats and Drivers

Companies clearly feel their control systems are more threatened than a year ago, as evidenced by the 24% shift from the moderate or low threat-level perceptions to high or severe/critical levels since SANS completed its 2015 State of Security in Control Systems Survey.[1] In 2016, 24% of respondents perceive the threat to be severe/critical, a greater than 15% increase when compared with 2015 (see Figure 4).

How serious does your organization perceive that current threats are to the cyber security of its control systems?



At what level does your organization perceive the current cyber security threat to control systems?

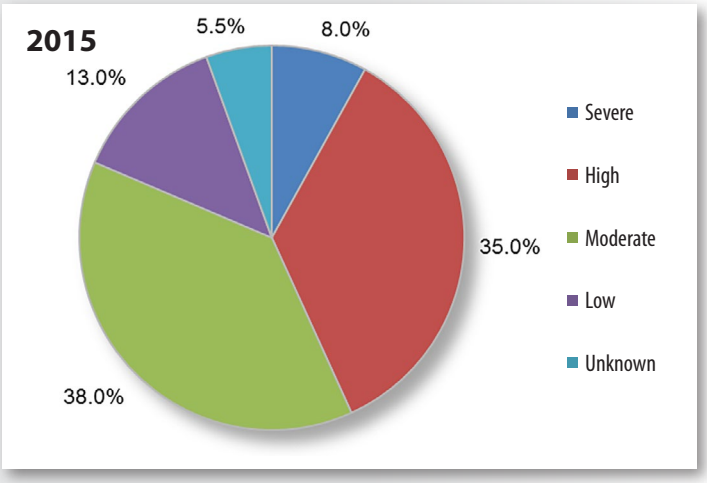


Figure 4. Comparison of 2015 and 2016 Perceived Levels of Threat to Control Systems

Multiple factors contribute to the increased perception of threat, notably the ever-increasing numbers of unsupported or unpatchable systems in ICS ecosystems. The increase in threat can be correlated with the increase in end-of-life systems that destabilize the balance of control on these systems and the ability to manage change.

[1] "The State of Security in Control Systems Today," www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042

The increase in high-profile examples of successful attacks on controls systems, such as the German steel mill[2] and Ukraine power grid,[3] undoubtedly also affects the increased perception of threats. Basic scorecards built around the wealth of collectable and analyzable data by security solutions can aid in evaluation of controls' effectiveness and guide decision making as corporate security and risk maturity advances. SANS advises organizations to allocate the necessary financial and human resources to improve their security protocols and protect their stakeholders, assets and operations. Failure to put appropriate safeguards in place may put corporate survival at risk.

The majority of respondents (61%) ranked external threats as the top threat vector with which they were concerned, followed by internal threats, selected by 42%, and malware families, chosen by 41%. Figure 5 illustrates the top three rankings of potential attack vectors with which organizations are concerned.

What are the top three threat vectors you are most concerned with?
Rank the top three, with "First" being the threat of greatest concern.

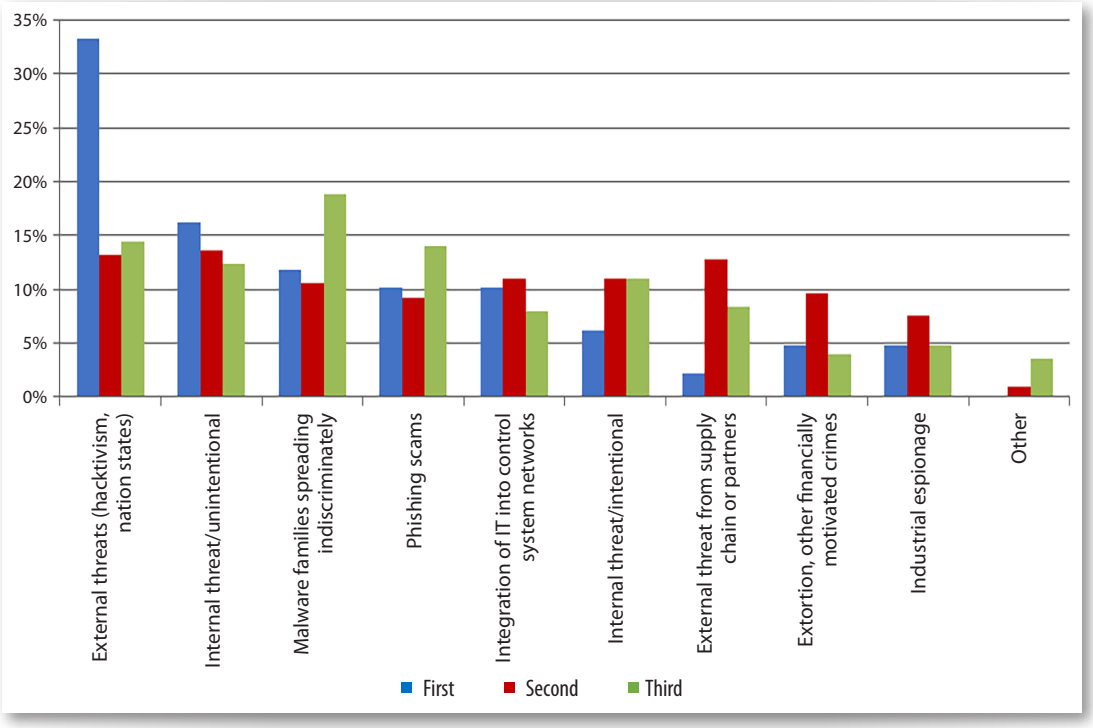


Figure 5. Top Threat Vectors of Concern

[2] https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[3] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

The anticipated source of these threats has changed significantly in the past year. Most notable are an increased concern with internal threats (up by 21% over 2015, with 42% expecting accidents as a top threat and 28% anticipating intentional malfeasance) and 23% of respondents stating that their supply chains or partners are one of the top three vectors for threats to their control systems.

This may reveal an awakening to the degree of exposure inseparable from the increasingly connected nature of control systems. As the process of migrating from analog equipment to digital and networked devices that communicate with each other—as well as with monitoring and control systems distributed across the boundaries of operations, enterprises, vendors and manufacturers—continues inexorably forward, organizations must recognize that the concept of the perimeter as primary safeguard is obsolete, and they must adapt their security practices to the new reality. While third-party risk is only a recently acknowledged threat within ICS, industries with more mature digital information-sharing business models have recognized this area as a top cyber security concern for years. Control system defenders can learn from work in that area.

Rising acceptance of the trend toward ubiquitous device connectivity may also be reducing concern about the integration of IT technologies into control system networks, which decreased from 46% in 2015 to 29%. This finding matches other indications that IT/OT integration is proceeding more smoothly than it did a year ago.

Turning to business drivers for control system security, ensuring reliability and availability of control systems continues to lead, chosen by 56% of respondents. Figure 6 provides a snapshot of the importance respondents' organizations place on a variety of business concerns.

What are your primary business concerns when it comes to security of your control systems?
Rank the top three, with "1" indicating the most important driver.

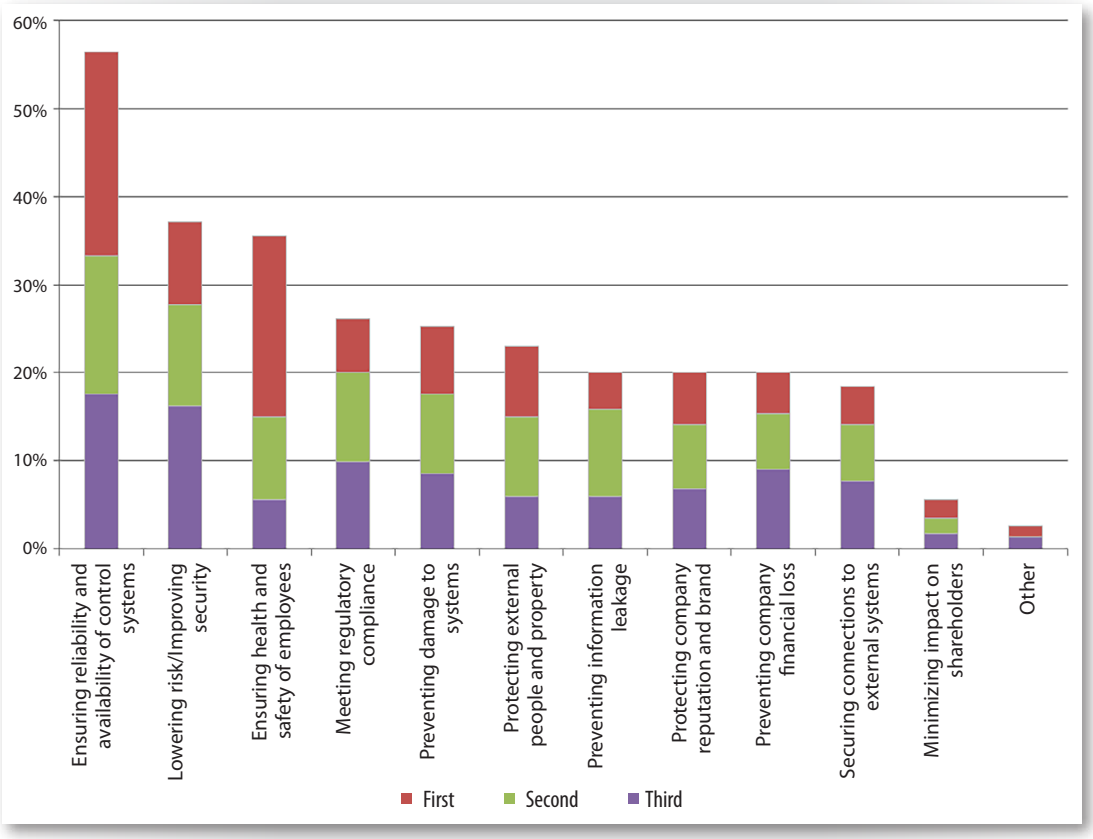


Figure 6. Business Drivers

We did see increased emphasis on other concerns in this year's data. Ensuring the health and safety of employees rose significantly (up 9% over last year to 36%), tracking with a demographic shift in respondents to include heavier representation by the healthcare sector. There is also a lesser but notable increase in the importance placed on protecting company reputation and brand (up 7% to 20%). Regulatory compliance remains a steady motivator, despite the shift in respondents' industries.

Security Assessments

Our respondents' level of confidence in their awareness of their control system external network connections remains steady. Fully half (51%) believe at least 75% of the existing external connections are documented, as illustrated in Figure 7.

Approximately what percentage of your company's industrial control system external connections are fully documented?

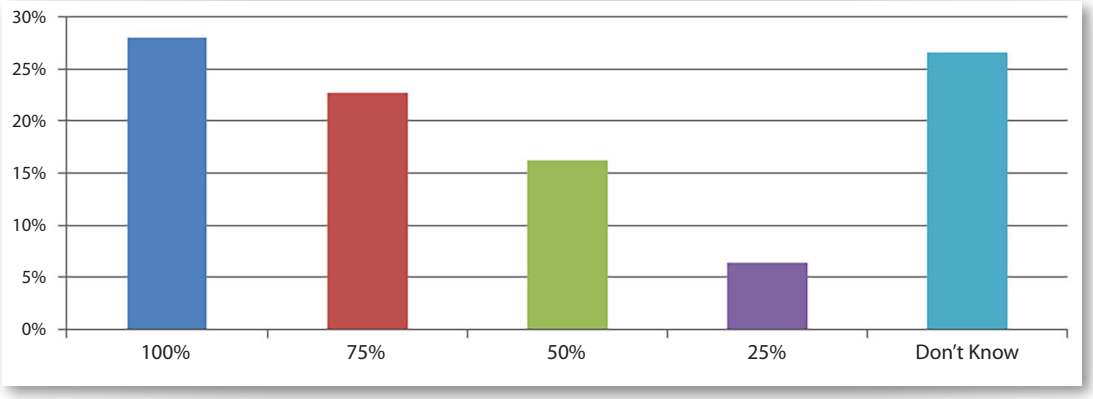


Figure 7. Documentation of External Connections

Many consulting ICS security professionals have told the authors they find just the opposite to be true in their experience: Very rarely are those connections fully documented. While we are proponents of valuing data over anecdotes, we believe it important to at least consider the possibility that some of our survey participants are excessively confident. It is, of course, impossible to verify what is not known.

Why Perform Security Assessments?

Security assessments are invaluable. Conducted regularly by trained and experienced staff or third-party specialists according to best practices, they provide multiple security benefits:

- **Asset inventory.** Staff must know what is—and is not—on their networks. Security assessments routinely discover undocumented devices, *as well as the absence of expected assets*.
- **Network traffic baselining.** ICS networks are largely deterministic, so it is possible to identify normal operations traffic and use this fingerprint to identify anomalous activity.
- **Security breach detection.** Many infiltrations of control system security networks are discovered only during the in-depth examination of a security assessment.

TAKEAWAY:

Large control systems network environments are dynamic, and it is essential to their security that assets and connections are inventoried on a regular basis to ensure the accuracy of existing documentation. We recommend including regularly scheduled inventories of assets and connections as part of your security assessments.

- **Vulnerability identification.** Security weaknesses of control systems and network equipment are discovered by vendors, clients and researchers on an ongoing basis. Assessments are planned with the latest information on vulnerabilities, providing a checklist from which assessors work.
- **Confirmation of remediation.** Each assessment includes a list of issues to address to improve security, bring systems into compliance and so on. Each assessment should also confirm the degree to which the issues listed in the previous assessment have been resolved.
- **Security posture insight.** Senior stakeholders need metrics to guide business decisions. Information regarding security risks and actions planned or taken to manage those risks is essential for allocation of appropriate resources, and security assessments are excellent tools with which to gather and provide that information.

Frequency of Assessment

With the importance of knowing the environment and assessing security configurations, it is perhaps concerning that 31% of respondents report that their organizations haven't completed a security assessment in the past 12 months. Figure 8 illustrates how often survey respondents' organizations assess the security of their control systems and networks.

When did your organization most recently perform a security assessment of your control systems or control system networks?

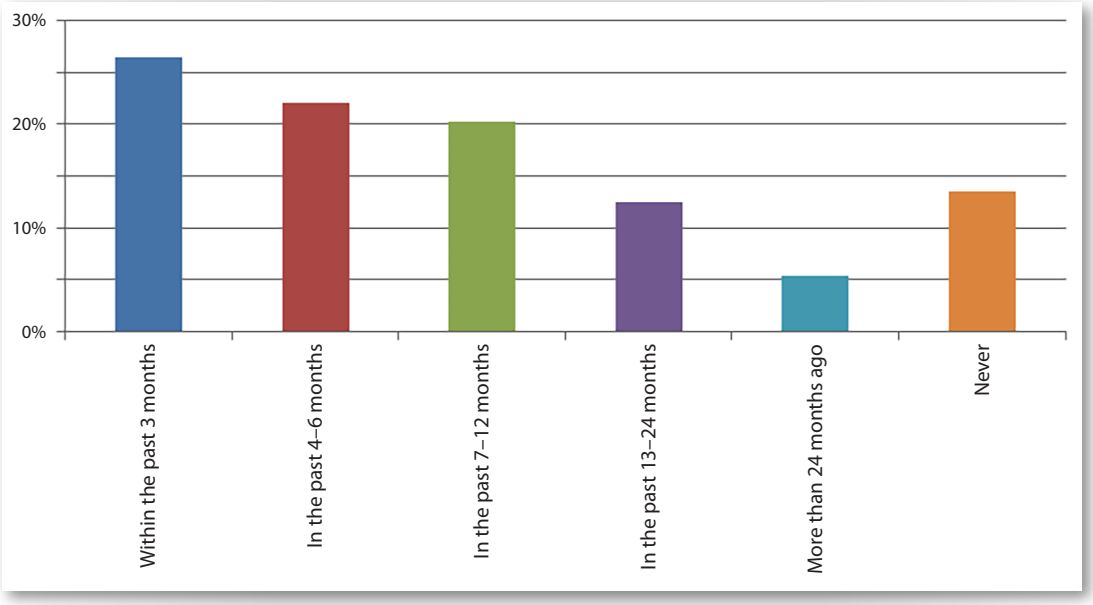


Figure 8. Recency of Security Assessments

Only 26% of participants' organizations have performed a security assessment within the past quarter. Considering that the average length of time between a breach and the discovery of an infiltration (dwell time) is between four[4] and six months,[5] according to multiple sources,[6] we feel very comfortable arguing that assessments be conducted once per quarter at an absolute minimum. Further, these assessments must be augmented with the essential activities of continuous network traffic anomaly monitoring and frequent device and network connection monitoring. Unfortunately, when 14% of respondents can state that their organizations have never performed a security assessment of their control systems, we recognize that this is a challenge.

Security Assessments Are Not Enough

Security assessments are deep inspections of the state of systems and components performed periodically to evaluate important configuration and operation details. Done well, they provide a high degree of confidence in the current state of network systems' security, identification of weaknesses and vulnerabilities, and a list of prioritized activities to remediate those concerns. Security assessments can also serve as a measurement of an organization's current state of security as it stacks up to policy and as a baseline measure to develop realistic goals to improve one's security posture. They are not sufficient, however, to ensure security. Security assessments are a stepping-stone to building a proactive, positive security threat model within ICS devices, increasing their security posture and allowing for alignment of both business and cyber security policies.

The greatest weaknesses of assessments are inherent, and they cannot be overcome by changes to assessment procedures but only by supplementing them. The value of even the best security assessment begins to degrade as soon as it is completed. As attacks increase in frequency, this becomes an increasingly important concern. Similarly, assessors use the best information regarding security threats and vulnerabilities available to them at the time of the assessment. They cannot check for zero-day exploits or unknown vulnerabilities. ICS defense requires an active threat-mitigation posture, with monitoring of devices and network traffic behavior to identify patterns indicative of security threats and take action before damage results.

[4] https://securityintelligence.com/news/global-security-report-shows-majority-of-companies-do-not-detect-breaches-on-their-own

[5] www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches

[6] http://techbeacon.com/how-discover-stop-security-breaches-fast-tracking-dark-web

TAKEAWAY:

Organizations should conduct security assessments, complete with inventories of assets and connections, at least quarterly. Assessments should include evaluation of the effectiveness of security controls. Such assessments should be supplemented with continual monitoring to identify anomalous traffic and behaviors and prompt action to remediate security vulnerabilities.

Continual monitoring, therefore, is the essential partner to periodic security assessments. Control system networks are more deterministic than their business counterparts; they have less traffic and it is more predictable. Unexpected network traffic can reveal changes to devices, network connections and software configurations, for example, alerting defenders to investigate further and take protective action if needed. Awareness of new security vulnerabilities or zero-day attacks is not needed to visualize and recognize network traffic deviating from the norm. Detecting anomalous network activity is analogous to noting an elevated temperature in a medical patient; it's a relatively easily observed symptom that prompts action.

Resources

In line with recommendations made in our 2015 State of ICS Security report,[7] significantly fewer organizations (43%, down 26% when compared to 2015) are relying solely on internal resources to perform their security assessments, with the shift to external resources being spread across control system integrators and consultancies of varying sizes. Large consulting services, used by 25%, and boutique consultancies (19%) are the most common resources employed (see Figure 9).

What resources did you employ for the security assessment?

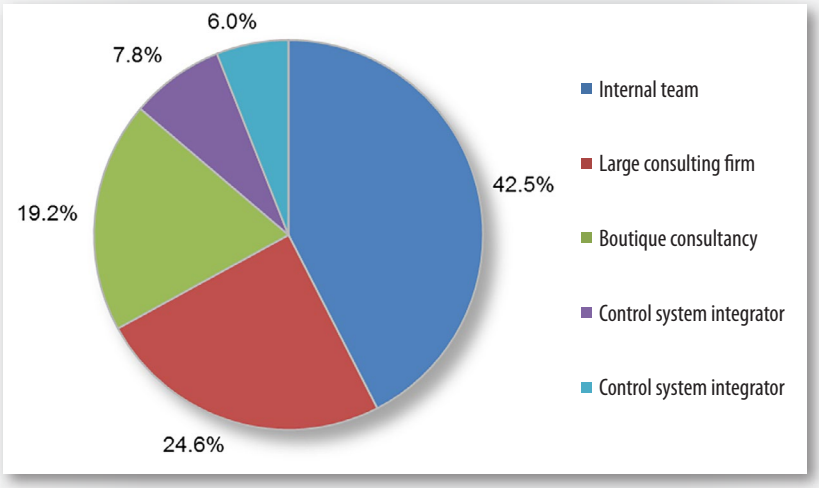


Figure 9. Resources Used for Security Assessments

[7] "The State of Security in Control Systems Today," www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042

The reliance of 43% on their own people supports the argument for funding greater training of these resources to improve their knowledge and competency in this specialized area. Participants ranked staff training and certification, chosen by 34%, as the third most planned and budgeted initiative to improve control system security. Defenders, of course, need to be well-armed with tools designed for their jobs (see the "Tools" section).

Most (54%) also rely on internal staff to gather and report on threat intelligence (see also the "Threat Detection" section later in this paper), which is a specialized skill even among security practitioners. Organizations need to support training to ensure that the skills and experience of their own personnel in these roles align with the requirements of these tasks or risk suboptimal accuracy and thoroughness in completing these mission-critical evaluations, which are foundational to the protection of business and infrastructure operations.

Breaches

The 27% of respondents reporting successful breaches of their control system networks is close to the 32% who reported a breach 2015. Similarly, 13% are sure they have not experienced a breach in 2016 versus 12% in 2015. Media coverage of the very limited number of publicly known attacks and the often-lengthy dwell times notwithstanding, survey results provide few clear indicators that the number of infiltrations into these systems has risen measurably. Figure 10 illustrates the breakdown of organizations' experience with breaches.

Have your control system cyber assets and/or control system network ever been infected or infiltrated?

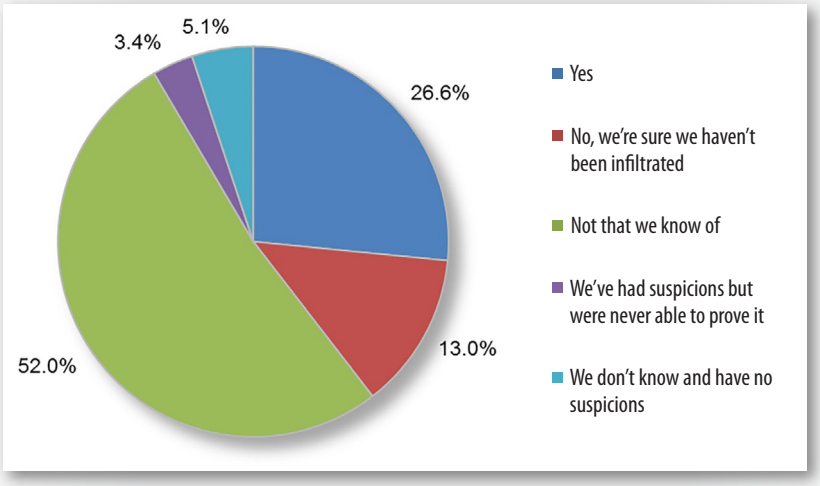


Figure 10. Breach History

It is interesting to note that 31% of respondents continue to state that they are unable to answer questions about breach history due to company policy. Those responses are not included in the calculation of percentages represented in the figure.

Because the survey is anonymous and no details about any incidents were requested, this may be an overly cautious interpretation of their employers' restrictions. Companies are often understandably hesitant to share information, fearing damage to their brand, loss of client confidence and so on. Regardless of whether policies actually prevent providing this information, restrictions on sharing incident information hinder the work of those striving to secure and defend control systems and their networks by making it more difficult both to gather resources to address control system security issues and to focus those resources on the best targets.

Who's Not Telling?

Why More Information Sharing About ICS Attacks Is So Important

Verifiable, quantifiable data on ICS security breaches is essential to advance this field of expertise and protect those very systems. Organizations need to share this information for their own benefit. Limited data decreases the ability of security practitioners to carry out their responsibilities by reducing the certainty and accuracy of their knowledge regarding the threats they are defending against and the effectiveness of current protections. Perhaps no work is of greater relevance for this point than that of Sun Tzu's *The Art of War*. Knowledge is the key to winning every battle, including those for resource allocations. SANS advises companies join and participate in an organization such as ICS-ISAC,[9] ICS-CERT[10] or InfraGard.[11]

The Cybersecurity Information Sharing Act of 2015[8] recognized the truth of those difficulties. Its lack of mandate to share cyber security information is considered by some to minimize its effectiveness, but it did establish provisions for sharing cyber threat information among federal agencies, technology companies and manufacturing companies in the interest of national security.

Setting successful breaches aside, attacks on control systems and networks are ongoing and growing in frequency.[12] Greater awareness of factual data (vs. anecdotal) is key to fostering positive change. Attacks on the NSA's Utah Data Center can exceed 300 million in a single day[13] (10K times as many as only five years ago), and a percentage of those target the BAS/BCS managing the environment for the data systems—an outlier example, we hope, but a worthwhile illustration of the rapidity with which malicious actors are bringing more resources to bear on their targets. Although exploration of subjects such as the commercialization and commoditization of online criminal activity is beyond the scope of this report, these developments contribute significantly to the high growth rate of the attacks under discussion here. To implement the information gathering required, business leaders need to understand this, as well as have a safe, confidential method for sharing information.

[8] https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015

[9] http://ics-isac.org/blog

[10] https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

[11] www.infragard.org

[12] www.ibtimes.com/cyberattacks-increase-companies-lack-malware-hacking-security-report-2311107

[13] http://thehackernews.com/2016/02/nsa-utah-data-center.html

Turning to those who did provide answers, we see an ongoing trend over the past three years of data, with more respondents annually aware of breaches and a general rise in the number of events within that period. The largest increase was of respondents experiencing more than 26 breaches (7% in 2016 compared to 2% in 2014). Figure 11 illustrates the number of breaches emanating from the reported incidents.

How many times did such events occur in the past 12 months?

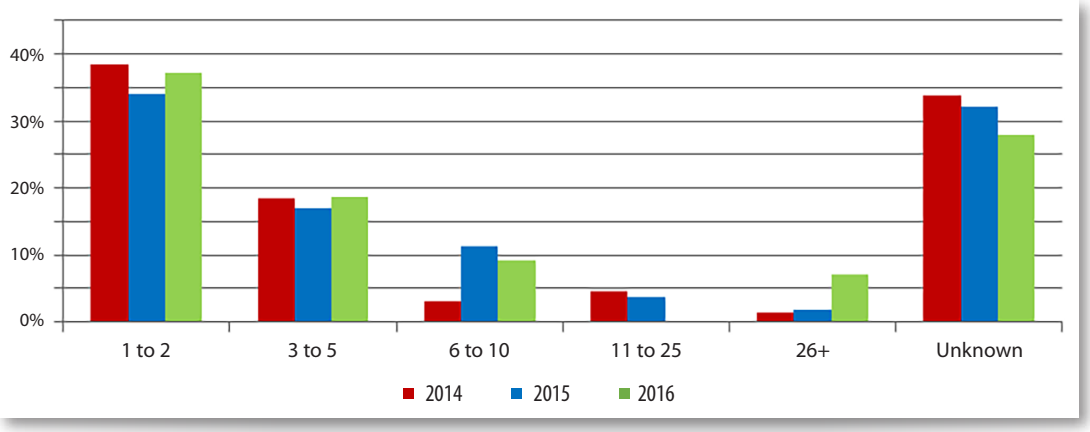


Figure 11. Number of Breaches Year over Year

The time between the start of an infiltration and recognition of that breach is a key indicator of the effectiveness of security systems and controls. Respondents' organizations appear to be recognizing breaches more quickly, with 56% making the determination that a breach has occurred in 24 hours or less. On the opposite end of the spectrum, 16% estimate this dwell time to be between eight days to more than three months (see Figure 12).

How long (on average) after an incident began did your control system security staff become aware of the situation?

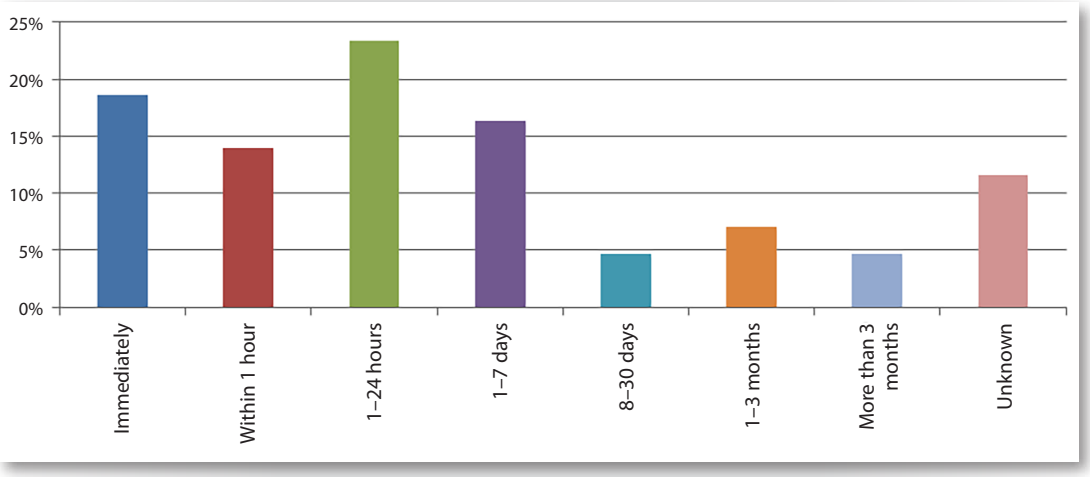


Figure 12. Time to Awareness

Overall responses indicate that control system defenders are improving at discovering successful infiltrations of their networks. Those reporting immediate awareness of breaches grew from (7% in 2015 to 19% in 2016), as did the group achieving detection within 1 to 24 hours of a breach (15% in 2015 to 23% in 2016). How security teams accomplished this is a topic well worth pursuing to help identify best practices.

We also observed a decrease in the percentage stating that the dwell time was unknown, the credit for which often belongs with the forensic specialists, who track down the point of the initial breach once the infiltration is discovered. Many IT security and forensics tools can't be used in an ICS environment without risk of service disruption, and some forensic investigative techniques require taking resources offline, which can equate to the same thing. The demonstrated ability to identify the initiation point of an attack is a good indirect measure for greater insight into all the details of an attack.

Further evidence of advances in forensic capabilities comes with the increased frequency of breach source attribution. While 30% of our survey participants were not aware of the status of efforts to identify breach origins, that number decreased significantly from the 44% unable to attribute the sources in 2015. Hackers took most of this blame, at 36%, followed by current employees and activists/hacktivists, at 34% and 23%, respectively (see Figure 13).

What was the identified source or sources of the infiltrations or infections?
Select all that apply.

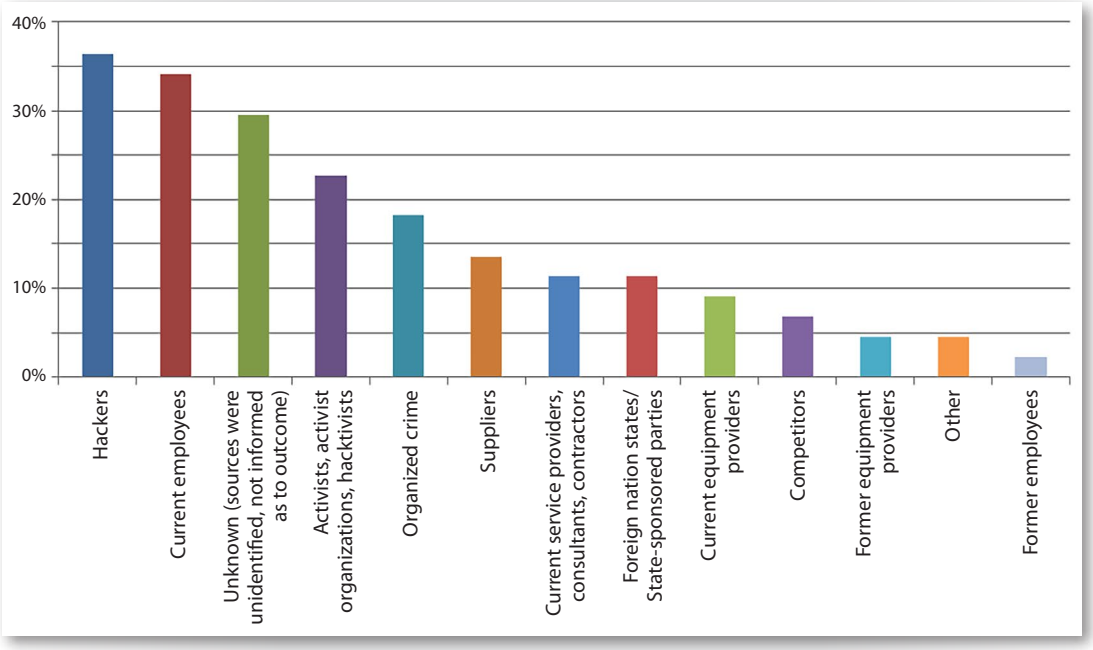


Figure 13. Sources of Infiltrations and Infections

In 2016, 17% more respondents placed blame on hackers, and attributions to organized crime were up 11%. Suppliers were also held to be at fault, up 8% over 2015.

While respondents consider overall threats to be on the rise, the specific risks to individual technologies and system components are a separate topic. Let's look at which of these they believe most likely to be targeted or to cause disruption through accidents.

Risk Levels

Although respondents believe the threat of compromise is greater this year than last, as noted previously, they consider most individual ICS components to be at roughly the same level of risk as a year ago. Computer assets running commercial operating systems still lead, with 72% considering them in the top three risks, surpassing all others by 25%. The reasons for this are plentiful and well-known, including the greater availability of attack tools and information for hacking IT devices, although this variation is shrinking as ICS hacking activity rises. The same category of assets ranked as the leading concern this year (see Figure 14).

Which control system components do you consider at greatest risk for compromise?
Rank the top three, with "First" indicating the component at greatest risk.

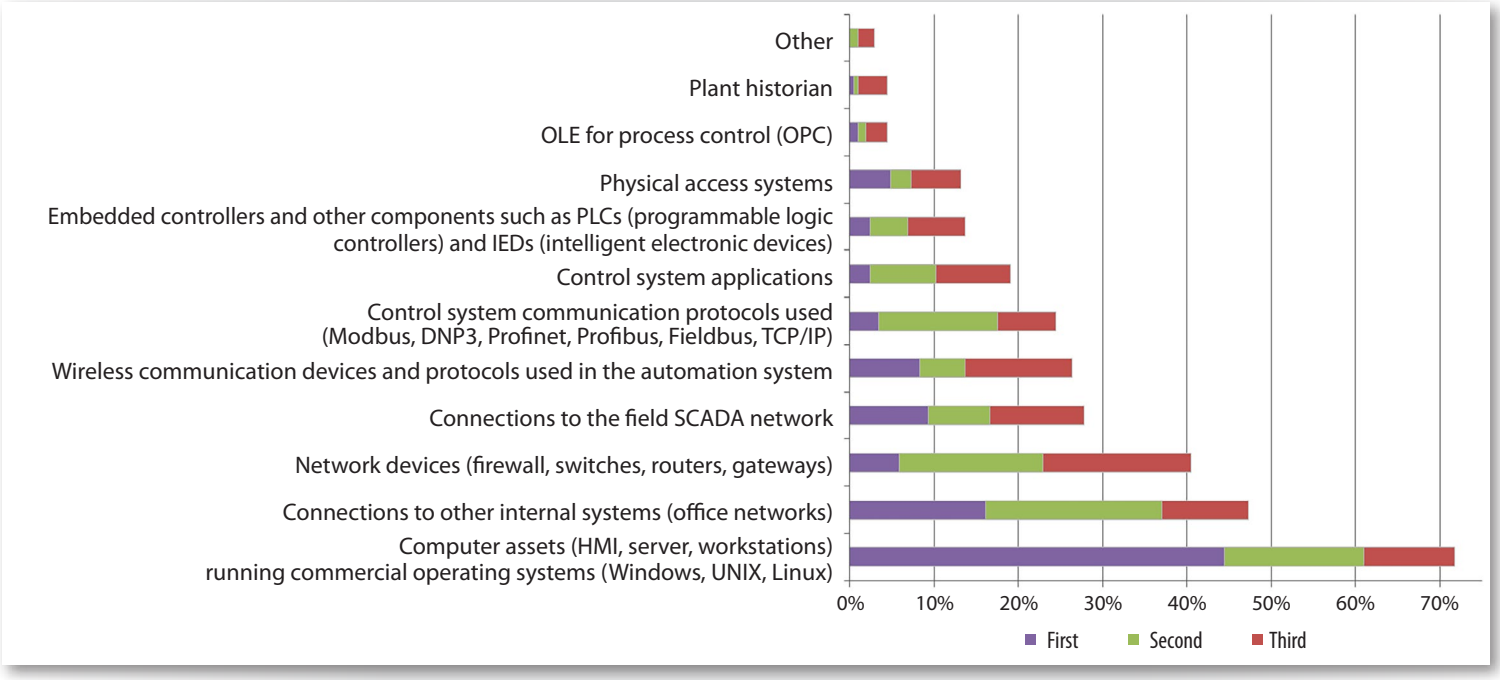


Figure 14. Control Systems at Greatest Risk of Compromise

Connections to other internal systems, with 47% ranking them in the top three, were seen as the second greatest risk. Networking devices, at 41%, rose four places in ranking from 2015, and embedded controllers slipped four places overall. These changes in where respondents perceive the greatest risk of compromise are reasonable, recognizing that threats generally utilize the network layer to propagate. Attacking and compromising networking devices is a relatively mature industry. Targeting the specialized embedded controllers is of interest to and within the capabilities of a smaller and more select group. As controls continue to proliferate with the growth of the IoT, the distinction between these groups may lose meaning.

That OLE for Process Control (OPC) continues to be at the bottom of the list, chosen by only 4%, 5% fewer than in 2015, is worrisome. OPC provides communication between business networks and control systems. Malicious actors often use it to reach ICS networks from hacked IT systems because of its vulnerability and ubiquitous distribution in the ICS space. With evidence that at least as many business networks are compromised as are not,[14] leaving this pivot point—from which adversaries can launch further attacks from inside the network defenses, thus avoiding perimeter defenses and operating at an enhanced trust level—unguarded is clearly a risky position.

There are always competing demands for personnel and financial resources, and security is often treated as an afterthought by those who haven't suffered the costs of a disruptive attack. These truths likely drive the relative deprioritization of ICS security efforts evident in survey responses. With publicly known cases of successful attacks revealing highly capable and well-funded malicious actors causing physical damage[15] and affecting large numbers of businesses and individuals,[16] we had hoped to see more organizations working to find their vulnerabilities and remediate them.

[14] www.gov.uk/government/publications/cyber-security-breaches-survey-2016

[15] https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[16] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Most respondents (56%) continue to rely on monitoring CERT notifications using an active vulnerability scanner. Somewhat fewer use passive monitoring using a network sniffer, chosen by 51% (see Figure 15).

What processes are you using to detect vulnerabilities within your control system networks? *Select all that apply.*

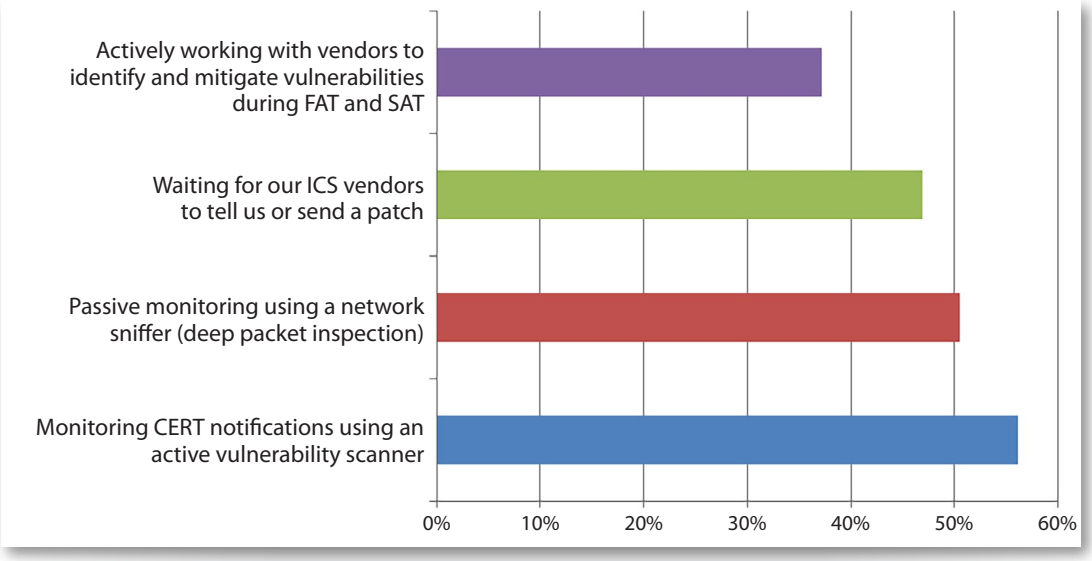


Figure 15. Vulnerability Detection Processes

Disappointingly, the highest growth is in the group waiting for vendors to provide a patch or direct some other action, which increased to 47% from 37% in 2015. Vendors of multimillion dollar (US$) industrial equipment increasingly maintain networked communications with their installed products, and contracts generally include specific language limiting changes clients may make to those devices, but that does not preclude self-protective activities such as any of the options listed here. Even working with vendors to find and solve security problems during the factory acceptance test (FAT)[17] and site acceptance test (SAT)[18] phases lost adherents this year, from 49% in 2015 to 37% in 2016. The only positive here is that more organizations are using passive network monitoring to help alert them to anomalies. Monitoring is essential both to maintaining the security of an ICS network and to detecting infiltrations when they do occur.

[17] FAT, which tests the system or equipment against specifications provided and/or approved of by that client to ensure it is ready to be installed on the client's site, is generally performed by the vendor before delivery to the end client.

[18] SAT takes place post-delivery in collaboration with the client to ensure the system or equipment matches client-approved specifications and is installed properly in its working environment.

Threat Detection

While the methods used to detect vulnerabilities have not changed much in the past year, the burden of finding these issues did shift more onto internal resources. Over half of respondents (54%) rely on trained staff to know when to search out security events, as illustrated in Figure 16.

Monitoring is essential both to maintaining the security of an ICS network and to detecting infiltrations when they do occur.

What sources of intelligence do you rely on to detect threats aimed at your control systems? *Select all that apply.*

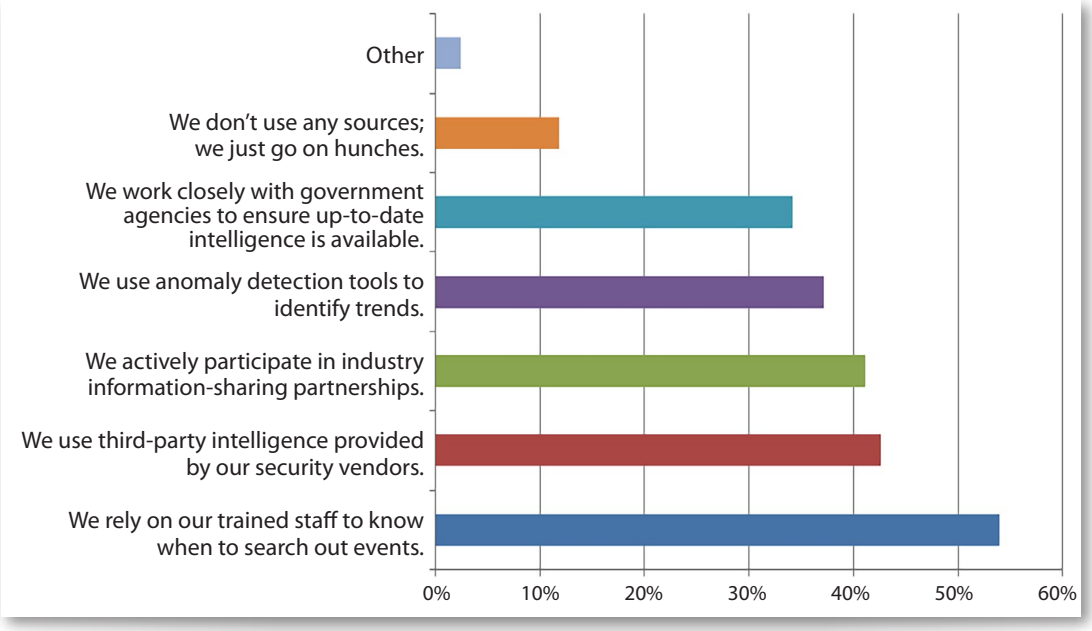


Figure 16. Sources of Intelligence

The widely reported shortage[19] of trained and experienced resources[20] in this field argues against the possibility that companies have successfully strengthened their cyber security staff by hiring.[21]

[19] www.networkworld.com/article/3068177/security/high-demand-cybersecurity-skill-sets.html

[20] www.rsaconference.com/blogs/11-strategies-to-consider-in-addressing-the-cybersecurity-skill-shortage

[21] www.secureworldexpo.com/how-raise-your-cybersecurity-salary-heres-how

This shift of responsibility onto internal resources includes an overall drop in the number of companies working with outside entities to detect threats, whether those entities are governmental, industry partnerships or security vendors. This also correlates with other indicators, such as an unwillingness to share their breach history, that companies may be growing more secretive about their security. Table 1 provides a snapshot of the decrease in use of external sources of intelligence.

Table 1. Changes in Use of External Sources of Intelligence

Source	2015	2016	Change
Trained staff knowing when to search out events	49.2%	54.0%	+4.8%
Third-party intelligence from security vendors	45.3%	42.6%	-2.7%
Industry information-sharing partnerships	44.7%	41.1%	-3.6%
Government agencies	44.1%	34.2%	-9.9%

A security policy establishes an organization's objectives, identifying what assets will be protected and, often, who is responsible for protecting them. The document provides and is extended by the mandate for standards or controls that detail specific rules, resources and measures to use in protecting those assets. Regardless of who authors these governance tools, it is important that they are actively supported at the highest possible organizational level to ensure their effectiveness.

Responsibility for Control System Security

The chief information security officer, chosen by 32%, is the role most frequently cited as setting control system security, followed by the "Other" category, at 18%, and the chief security officer at 12%. Roles listed in the "Other" category include IT or security director; compliance officer or manager; SCADA manager, department or staff; and network engineer or administrator, to name just a few. Figure 17 shows the breakdown of responsibility.

Who in your organization sets policy for security of controls systems?

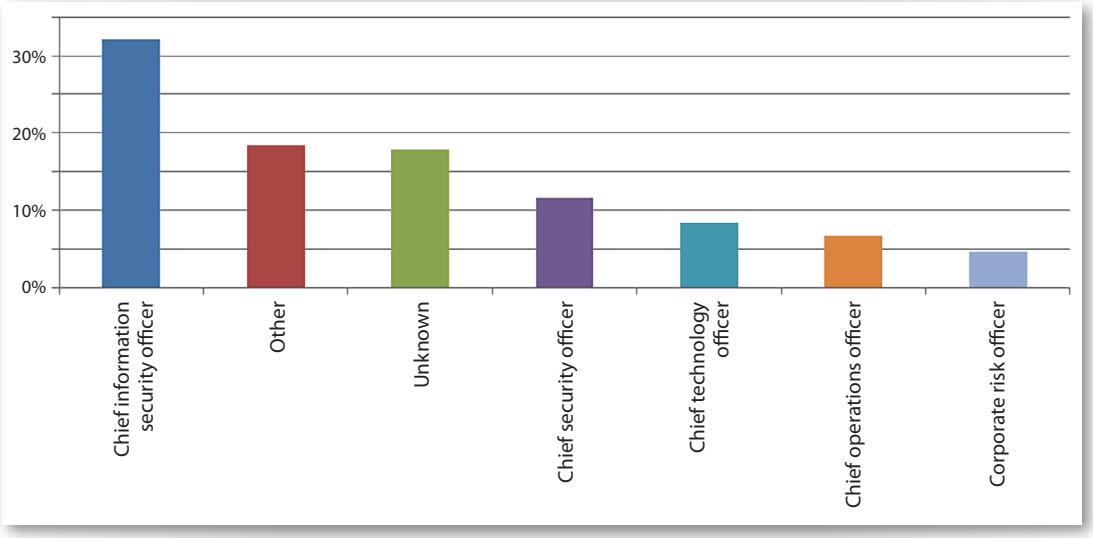


Figure 17. Responsibility for Control System Security Policy

It's clear that setting ICS security policy appears in the portfolio of many different parties across the enterprise landscape, at least 15% of which are not C-level positions and appear in write-in responses. Moreover, about a third (34%) of "other" respondents stated that policies were determined not by an individual, but by a group which, in the opinion of the authors, often works well for the granularity needed at the implementation level (controls and standards) and less so at the strategic level (policies).

Considering that corporate officers are ultimately responsible for company fortunes and that the impacts of control system security incidents are potentially enormous in scale, we recommend that all organizations align these responsibilities accordingly. The role of operations- and implementation-focused resources in properly informing leadership is essential, but policy needs to be established at the highest levels, both to address liability considerations and to provide those policies with sufficient authority to overcome organizational obstacles and enact change in the enterprise. Regardless of who is responsible for the implementation and management of security controls and their effectiveness, their authority needs to derive from the policy level and should map to a regulatory framework. Consistent risk-rating measures are also required to determine the effectiveness of controls.

Security controls exist at multiple locations in an ICS environment, so multiple parties are responsible for their implementation. This includes owner/operators in 51% of organizations, with engineering managers and system integrators, chosen by 41% and 32%, respectively, also carrying implementation responsibility (see Figure 18).

Who in your organization is responsible for implementation of security controls around control systems? ***Select all that apply.***

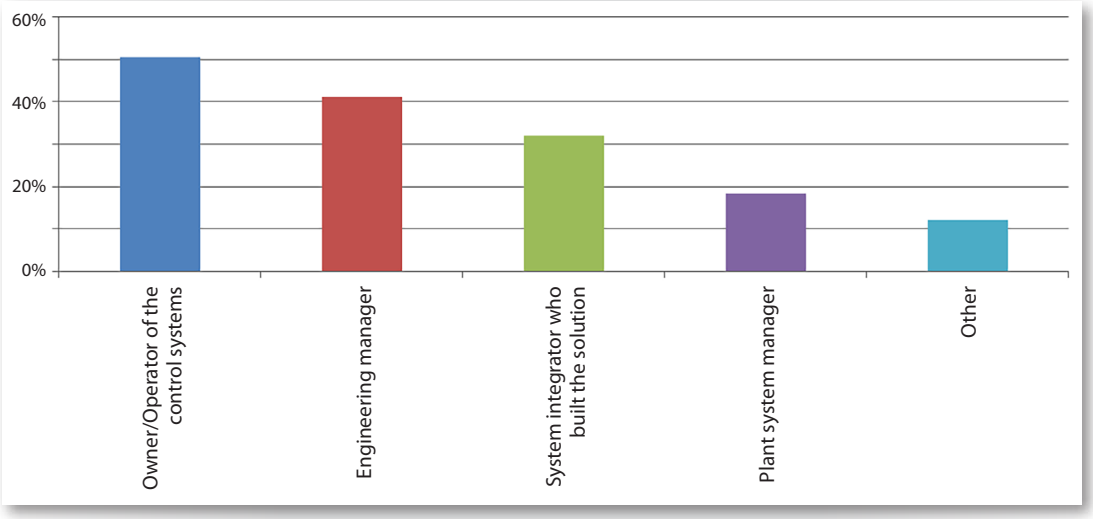


Figure 18. Responsibility for Implementation of Controls

One of the strongest recommendations of the 2015 SANS State of ICS Security report[22] was the inclusion of cyber security considerations in the control system procurement process. We are encouraged to see even a slight shift in this direction, with 40% indicating they have a clear and reasonable set of requirements in the procurement process, as illustrated in Figure 19, an increase of 5% over 2015.

Do you normally consider cyber security in your control systems procurement process?

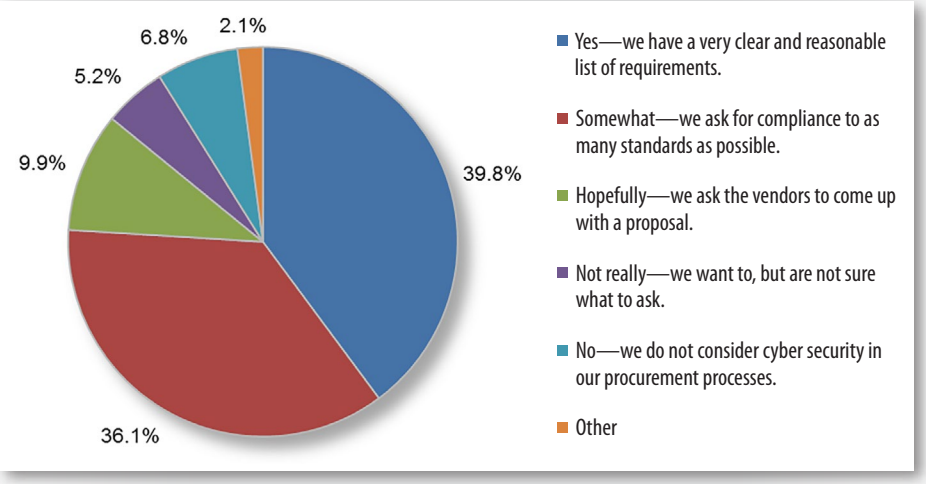


Figure 19. Cyber Security and the Procurement Process

TAKEAWAY:

Efforts to improve supply chain security concerns must address two distinct issues: security of procured assets and security of connections to those assets.

We must, however, reiterate and emphasize the importance of this guideline: Get security resources engaged with the procurement processes. Recall that 23% of respondents identified suppliers as one of the top threat vectors. This recognition clearly argues for action on the matter.

Control system-dependent organizations need to understand that the examination and testing of new equipment and software for vulnerabilities is not a given. These activities increase asset design, development and production costs and are generally performed only by suppliers who perceive that sufficient value would be added in the marketplace. Companies need procurement agents (supported with sufficient technical expertise to properly define security requirements) working with vendors to incentivize the delivery of more secure products. Because alternative products and vendors are not always available, purchasers may have to pay some of the costs associated with that improved level of security in the form of increased prices. Organizations must weigh those costs against the risks of continuing to accept less-secure assets.

[22] "The State of Security in Control Systems Today," www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042

The procurement process has a role in establishing the security of assets after acquisition as well. FAT and SAT procedures are separate and given requirements, but the agreements for maintenance of ongoing security are essential both after installation and during implementation. These agreements include defining responsibilities for asset monitoring and updates, scheduling and implementation of security patches, and other such tasks. Additionally, as connections between ICS equipment and external parties (vendors, manufacturers and contracted support entities) continue to proliferate, the responsibility for maintaining the security of these conduits and networked devices must be clearly delineated. Numerous high-profile breaches have been carried out by attackers infiltrating suppliers or servicers and pivoting from there into customer networks.[23]

Tools

The tools in use to protect control systems are those we would expect, with anti-malware/antivirus used by 80%, physical access controls used by 73% and zones or network segmentation used by 71%. Table 2 illustrates the top five tools in use and the top five tools respondents planned to have in use in the coming months.

Table 2. Tools and Technologies in Use and Planned for Implementation

In Use	
Tool	**Used By**
Anti-malware/ Antivirus	80.0%
Physical controls for access to control systems and networks	72.8%
Use of zones or network segmentation	71.1%
Monitoring and log analysis	64.7%
Technical access controls	63.4%

Planned	
Tool	**Planned By**
Anomaly detection tools	34.5%
Control system enhancements/ Upgrade services	32.3%
Application whitelisting	31.5%
Vulnerability scanning	31.1%
Intrusion prevention tools on control systems and networks	28.9%

We found little change over 2015 on the security technologies or solutions actually in use. The largest increases in usage are for monitoring and log analysis (up 10% to 65% in 2016), application whitelisting (up 8% to 40%) and communications whitelisting (up 10% to 37%). Use of technical access controls decreased from 83% to 63% in 2016.

[23] www.forbes.com/sites/paulmartyn/2015/06/23/risky-business-cyber-security-and-supply-chain-management/#782e467a723b

Looking at what is in use today compared with what last year's respondents had *intended* to be using, however, we noticed significant differences. We expected to see an additional 20% over the noted growth in use of monitoring and log analysis, vulnerability scanning, and application whitelisting. In addition, security awareness training was projected for a 25% increase that did not materialize, and anomaly detection tools were expected to see a 30% increase. What happened to planned initiatives?

We can only theorize why security plans appear to have been delayed or canceled because neither this survey nor other sources of data provide insights. This survey was not designed to check whether individual organizations made their planned changes year over year. Possible causes for any single organization to put off an initiative are plentiful, but impacts across a range of somewhat diverse organizations are harder to explain. Budgets are at the top of the list of usual suspects, of course, and economic events have affected some industries negatively in the past year. The small but notable upward trend in security allocations over this same time period suggests looking elsewhere, however.

New initiatives to conduct security assessments and audits of control systems and networks are fewer this year (down 13% from 2015), as are plans to train staff responsible for the security of those systems and networks (down 8%). More organizations intend to implement controls on mobile and wireless communications (up 10%) and roll out anomaly detection tools (up over 8%) but if there is no training, we must ask who will implement those technologies. Table 3 details the top initiatives on which organizations plan to invest budget dollars in the coming 18 months.

Table 3. Top Planned Initiatives

Planned Initiative	Percentage
Security awareness training for staff, contractors and vendors with access to control systems and networks	39.8%
Security assessment/audit of control systems and control system networks	36.4%
Staff training and certification for current staff responsible for implementing and maintaining security of control systems and networks	34.2%
Implementation of anomaly detection tools on control systems and networks	31.6%
Implementation of intrusion detection tools on control systems and networks	28.1%
Implementation of greater controls over mobile devices/wireless communications	21.6%
Acquisition of additional skilled staff responsible for implementing and maintaining security of control systems and control system networks	21.6%

Budgets

It is inevitable that finances influence the choices organizations make in acquiring and developing tools and resources. The picture here is complicated by multiple factors, including: 1) responsibility for security is often spread across many business divisions, as are budgets; 2) the value of security investments is largely seen as cost- or risk-avoidance and ROI can be difficult to quantify; 3) the perception of that value is heavily influenced by experience with successful breaches, making it much greater in hindsight than in anticipation; and 4) comparing the likely effectiveness of specific allocations within the overall security umbrella is hampered by a continually shifting threat landscape and limited data on breaches, exacerbated by limited information sharing.

Control system security budgets can be controlled in a variety of ways. For our sample, 26% are controlled by the IT department, 31% by the operations department, and 34% by a mix of the two (see Figure 20).

Who controls the control systems security budget for your company?

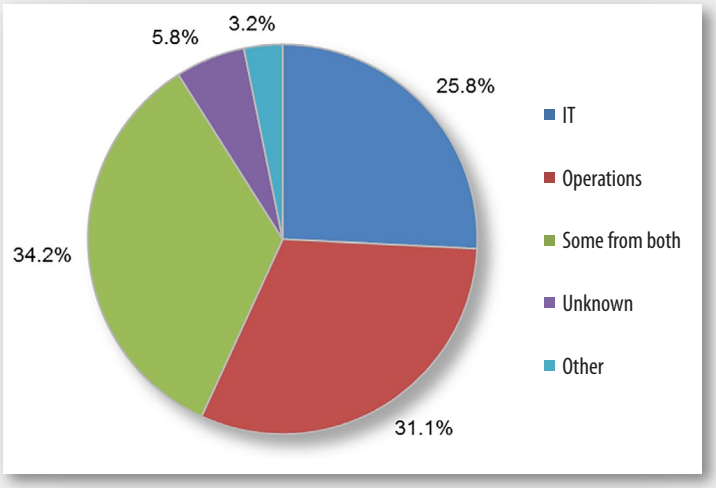


Figure 20. Budgetary Control

This year respondents indicated that control system security budgets are less often shared across IT and OT, down 11% from 45% in 2015, with a nearly equal shift of funding responsibility and control to each group. While it could be argued that this simplifies the situation, real security improvements must include organizational changes that enable security practitioners to carry out their mission effectively throughout the enterprise, as well as engaging nonpractitioners in security activities.

At several points in this report we have raised questions regarding the sufficiency of funds allocated to the mission of protecting control systems and their networks. We would be remiss if we did not point out that many organizations are giving greater financial support to security. Discounting those respondents who lack knowledge of finances in this area (36%), more than half of those who provided data (54%) stated that their control system security budgets had grown in the past year (see Figure 21), a very positive sign that companies are starting to respond to changing risks.

Does this represent a change from your control system security budget for FY2015?

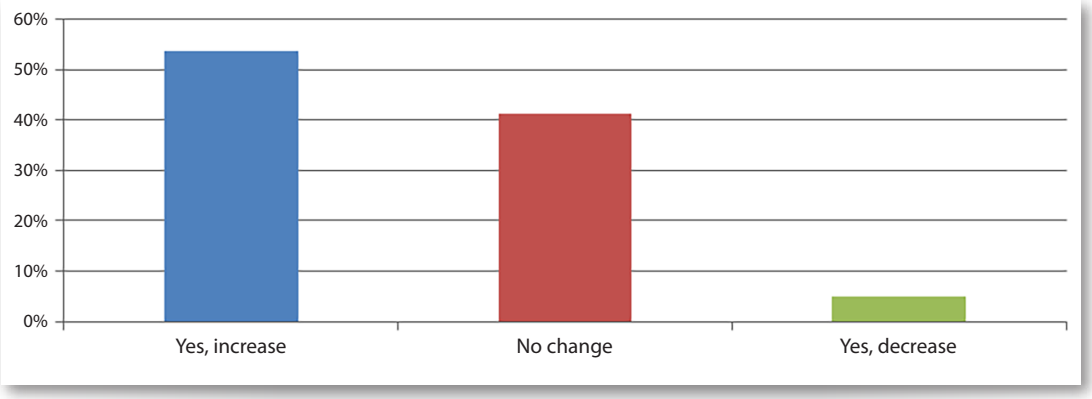


Figure 21. Changes in Security Budgets

IT/OT Convergence

Cyber security is a relatively new consideration for many businesses. For most of their history, numerous mature industries that grew up on and contributed to the development of control systems, such as manufacturing, oil and gas, and electric power, were able to protect themselves and their customers by managing physical security risks. Network-based threats to their assets and operations largely began to appear in the past two decades, initially introduced to many with vendor support of installed equipment and expanding with increasing speed as the benefits of connectivity with business systems came to be recognized, and as IT and operational technologies started to converge.

The incorporation of IT-developed technologies into control system devices and networks introduces risks previously unknown in this environment. Many of the tools and techniques developed to address those risks in IT networks are problematic in ICS, with its extremely low tolerances for traffic delays and service disruptions. Organizations running control systems are experiencing demands to address security concerns that derive from this convergence despite a shortage of resources and knowledge with which to do so.

So, are organizations ready? A surprising 20% have no plans to address the security issues surrounding convergence of IT and control systems, nor do they plan to develop any. However, 37% do have such strategies and are implementing them, as illustrated in Figure 22.

Does your company have a security strategy to address the convergence of enterprise IT and operations?

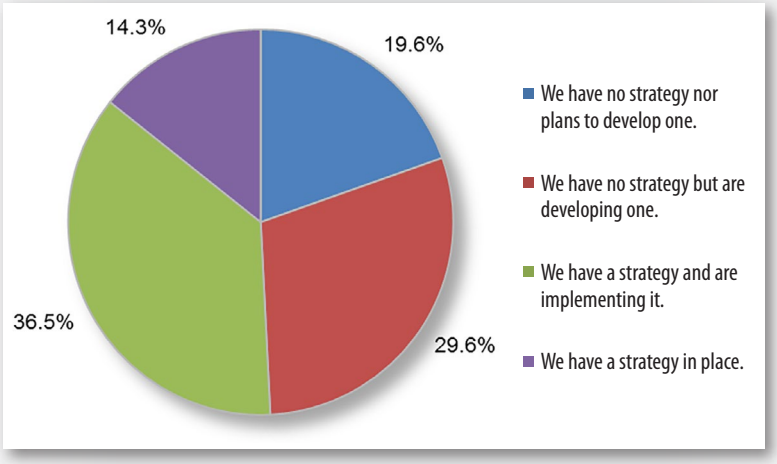


Figure 22. IT/OT Convergence Strategies

A small (4%) increase in the percentage of companies with security strategies addressing the convergence of IT and control system networks in place or implementing such strategies brings those with strategies to just over 51%. That so few entities have such a policy remains a red flag of concern. The conversion of facilities and entire industries from electromechanical, analog controls managing devices operating largely in isolation to software-driven, highly networked digital systems is driven by the pursuit (or at least acceptance) of many business factors. The accompanying reality is that this change is opening control systems—and by extension those dependent on their smooth operation—to new vulnerabilities. Organizations responsible for that operation must establish, implement and adhere to a plan to manage this transition and its inherent risks.

TAKEAWAY:

Develop and implement an IT/OT convergence security strategy[24] to protect your organization from new vulnerabilities arising from convergence changes. Creating a successful strategy will require engagement of skilled security practitioners with detailed information regarding the ICS environment and relevant project management experience.

Developing a Convergence Security Strategy

Planning and implementation teams need empowered stakeholders not only from IT and OT but also from business operations. Plans are living documents that need to be updated and expanded over the course of transition activities and must include:

- Comprehensive, detailed documentation of current IT and OT assets
- Comprehensive, detailed analysis of operations (with impact analysis of planned convergence changes)
- Road map to the future state of the converged technological environment
- Identification of skillset/resource shortages (gap analysis) and plans to address them
- Overarching governance model establishing responsibilities, authority and top-level mandate for implementation of the strategy
- Change-management plan
- Coordination plan with existing asset management processes

[24] www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005249

Conclusion

A singularly important message from the data gathered in this survey is that little has changed for the better in the past year. Even though organizations perceive increasing risk levels, they have done less to secure control systems and their networks than they had planned. Despite larger security budgets, companies do not seem to have used those funds toward increasing the skills and capabilities of the security practitioners charged with protecting these critical assets. Instead, they used funds for catch-up measures such as acquiring technology to address mobile security issues.

In the industrial IoT world, security is a requirement everywhere. Security perimeters are increasingly porous, and internal assets are being suborned and used by malicious external actors to gain greater access and carry out further attacks. However, responsibility for security is distributed across the enterprise and its supply chains. Policies defining how organizations will manage through this ongoing evolution of the threat landscape, established by senior leaders and backed with their full support, are required to fulfill organizational responsibilities to stakeholders at all levels. Prompt and sustained action is needed to protect lives and livelihoods alike.

Organizations built on the dependency and reliability of their control systems must recognize the rising level of risk and focus resources on addressing the serious threats to their continued operations. The stakes are nothing less than existential, regardless of whether we consider reputations, finances or human lives.

About the Authoring Team

Derek Harp is currently the director for ICS Global Programs at SANS and chair of the GICSP Steering Committee. He is responsible for organizing events, resources and initiatives that educate and enable increased collaboration within the entire ICS security community. Derek has served as a founder, CEO or advisor of early-stage companies for the past 18 years with a focus on cyber security. He is a former U.S. Navy officer with experience in combat information management, communications security and intelligence.

Bengt Gregory-Brown is a consultant to the SANS ICS program and the principal analyst at Sable Lion Ventures, LLC, a virtual accelerator focused on emerging cyber security solutions. He brings 20 years of experience to bear in his writing about the management of IT and infrastructure projects, enterprise security governance, information security risk analysis, regulatory compliance and policy conformance for high-profile companies. Bengt has managed multiple patents from ideation through the development and issuing phases.

Sponsor

SANS would like to thank this survey's sponsor:

BELDEN