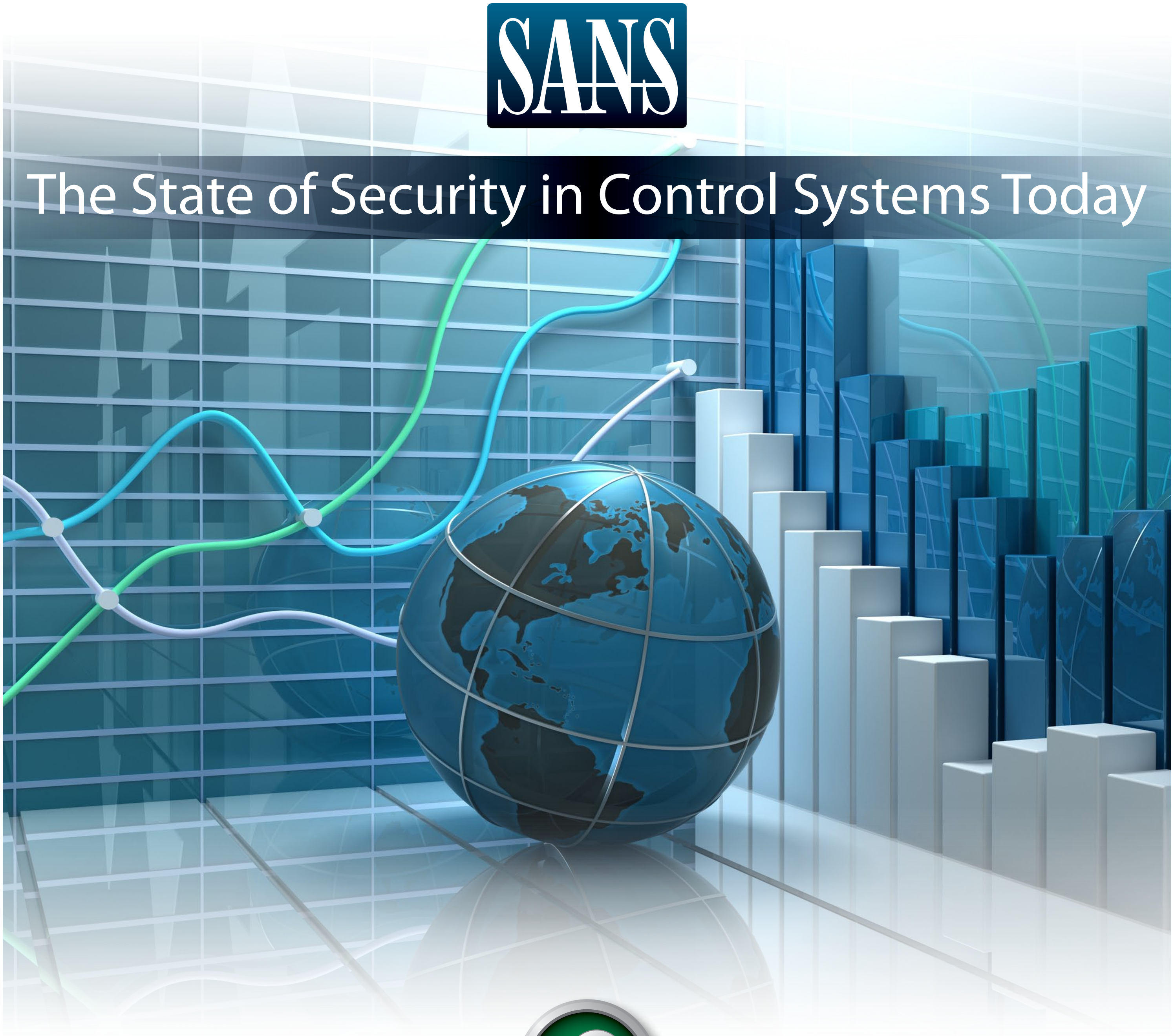
The State of Security in Control Systems Today

By reading this report, ICS professionals will gain insight into the challenges facing peers, as well the approaches being employed to reduce the risk of cyberattack.

The State of Security in Control Systems Today



A SANS Survey

Written by Derek Harp and Bengt Gregory-Brown

June 2015

Sponsored by
SurfWatch Labs and Tenable Network Security

Executive Summary

Industrial control systems (ICS), or the hardware and software that monitor and control physical equipment and processes for critical infrastructure, such as water, oil, gas, energy and utilities, as well as automated manufacturing, pharmaceutical processing and defense networks, present a wildly attractive target for those who seek to cause disruption or to threaten infrastructure for their own purposes. Because of the significant costs of designing, developing and optimizing control systems, those seeking to gain technical data for their own use also target them.

Industrial Control Systems (ICS)

Monitor and control industrial and infrastructure processes; referred to in different industries as supervisory control and data acquisition (SCADA) systems, process control systems (PCS), process control domains (PCD), or building automation and control systems (BACS)

SANS recognized the growing concerns about attacks on this sector with the appearance of Stuxnet and began developing an ICS security-specific practice, including a growing selection of educational offerings and an annual survey of professionals working or active in industrial control systems.[1] Since our first ICS security survey, we have seen such disturbing events as the 2014 German steel mill incident[2] and ICS-targeting malware such as Havex and Dragonfly.[3]

In 2015, we conducted our third survey on ICS security, which was taken by 314 respondents. Their answers indicate their organizations are concerned about keeping their most basic ICS operations running reliably and safely. They also show an increasing uncertainty over whether their systems had been infiltrated without their knowledge.

The results also echo other industry data indicating more frequent targeting of industrial control systems, particularly energy-generation systems. Data also shows that those targeted attacks have resulted in a rising number of breaches.[4]

32% indicated their control system assets or networks had been infiltrated or infected at some point

34% believe their systems have been breached more than twice in the past 12 months

15% reported needing more than a month to detect a breach

44% were unable to identify the source of the infiltration

[1] "SANS SCADA and Process Control Security Survey," www.sans.org/reading-room/analysts-program/sans-survey-scada-2013;
"Breaches on the Rise in Control Systems: A SANS Survey," www.sans.org/reading-room/whitepapers/analyst/breaches-rise-control-systems-survey-34665

[2] www.bbc.com/news/technology-30575104

[3] https://securityledger.com/2014/07/industrial-control-vendors-identified-in-dragonfly-attack

[4] http://thirdcertainty.com/news-analysis/targeted-attacks-industrial-control-systems-surge

Executive Summary (CONTINUED)

While control system networks are not necessarily more opaque than IT systems, the available tools to map and monitor their traffic and attached devices have been less robust than their IT counterparts. It is essential that industry leaders provide their security practitioners with the tools, training and resources to gain the insight needed to protect these critical assets.

42% see external actors as the No. 1 threat vector

19% see integration of IT into control system networks as the top threat vector

11% see insider threats as the No. 1 threat vector

Threat vectors do vary, but the top vector consists of external actors (hacktivists or nation states). Threats from these sources were chosen by 73% as one of the top three threat vectors. Although 25% of respondents' breaches were attributed to current employees (insiders), 48% cited insider threat as being among the top vectors.

By reading this report, ICS professionals will gain insight into the challenges facing peers, as well the approaches being employed to reduce the risk of cyberattack.

Survey Participants

The 314 respondents who actively maintain, operate or provide consulting services to facilities maintaining industrial control systems, energy and utilities (29%), together with related oil and gas production or delivery (5%), far outweigh other industry segments. The "Other" category accounted for 21% and consisted of a mix of respondents providing business and government services to this industry. And 13% of respondents came from business services. Only engineering services and control system equipment manufacturers accounted for 5% of our sample. All other sectors were represented by less than 4% of the respondents.

Of the respondents, 70% work in companies of more than 1,000 employees, and 28% work in companies with more than 15,000 employees. These numbers indicate that industrialized processes and their support services are typically provided by larger enterprises.

While respondents' organizations primarily operate or support control systems in the United States, we observed an increase in the number of respondents' employers outside the U.S., rising from 16% in 2014 to 22% in this survey, with increases fairly evenly distributed across all regions of the world. Table 1 provides a look at the international reach of respondents' organizations.

Table 1. International Representation

Country or Region	Representation
United States	77.7%
Europe	31.2%
Asia Pacific (APAC)	26.8%
Canada	22.9%
Middle East	19.1%
South America	17.2%
Australia/New Zealand	15.3%
Africa	15.0%
Latin America	14.3%
Antarctica region	3.8%
Other	3.5%

Roles

The majority of respondents fall into two categories: security administration/security analyst, chosen by 31% of respondents, and security manager/director or officer, selected by 15% of the sample. This result corresponds with the findings from 2014. Figure 1 shows the roles respondents play.

What is your primary role in the organization?

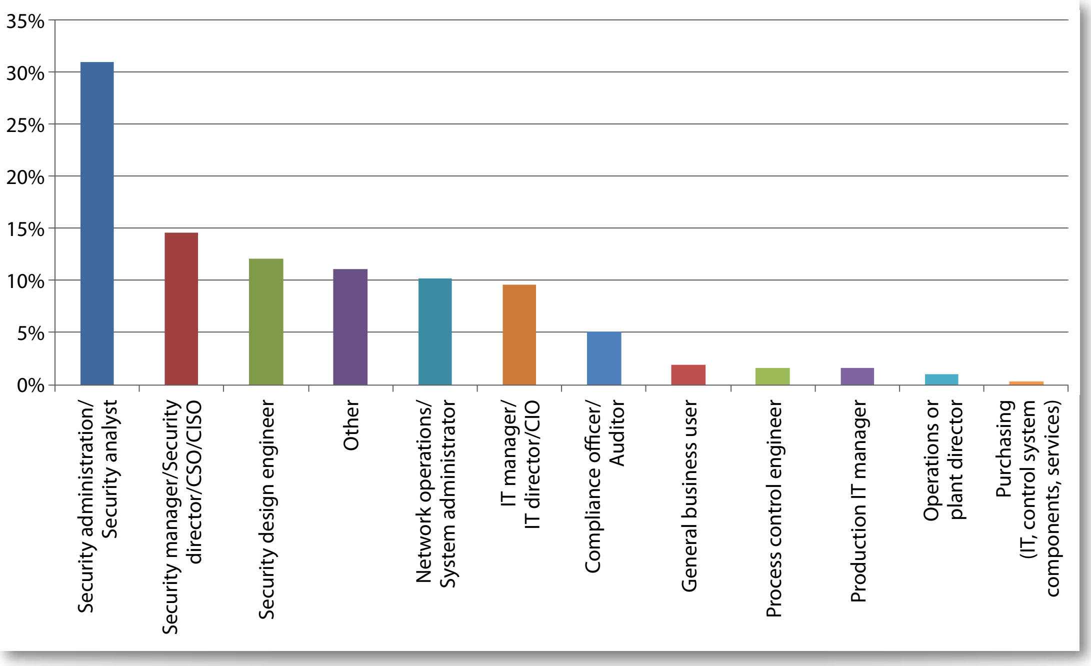


Figure 1. Respondent Roles

We saw a significant increase in security design engineers in 2015, nearly doubling from 2014 in overall percentage to 12%, as well as in ICS security specific consultants. This is a positive trend, given that these individuals have a perspective on operational concerns that generally differs from that of the administrative group.

Control System Security Training

It is clear from our results that most of our respondents hold security certifications, but the largest number of these (52%) is not specific to control systems, such as the CISSP,[5] CISA[6] or CompTIA. Less than half (43%) have completed the GICSP,[7] and even fewer the ISA99/IEC[8] (13%) or IACRB[9] (12%). IT security education is valuable, particularly with the converging technology trends, but it does not translate directly to ICS environments. We highly recommend that everyone working with the security of control systems and their networks be trained in ICS-specific considerations. See Appendix A, "ICS Security Training," for additional information.

[5] Certified Information Systems Security Professional

[6] Certified Information Systems Auditor

[7] Global Industrial Cyber Security Professional

[8] International Society of Automation's ISA99: Cybersecurity Expert

[9] Information Assurance Certification Review Board's SCADA Security Architect

Security Threats and Drivers

Survey respondents indicated that their primary business concern regarding the security of control systems was ensuring the reliability and availability of control systems (35%). This was followed by ensuring the health and safety of employees—a distant second at 15%. The third most-pressing concern was lowering of risk/improving security at 13%. These same concerns fall in the top four overall concerns:

- Ensuring reliability and availability: 68%
- Lowering risk/improving security: 40%
- Preventing damage: 28%
- Ensuring health and safety: 27%

Control system reliability and availability are often considered in conflict with efforts to secure those systems, and this issue has gained attention recently. The increasing utilization of IP-based technologies in control system environments has brought with it well-known security concerns. Unfortunately, the methods and tools long in use in IT can be highly disruptive in the ICS space. The need for nondisruptive methods to secure control systems, without awaiting the infrequent shutdowns of these systems, is leading to new products and solutions. See Figure 2 for a ranking 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.

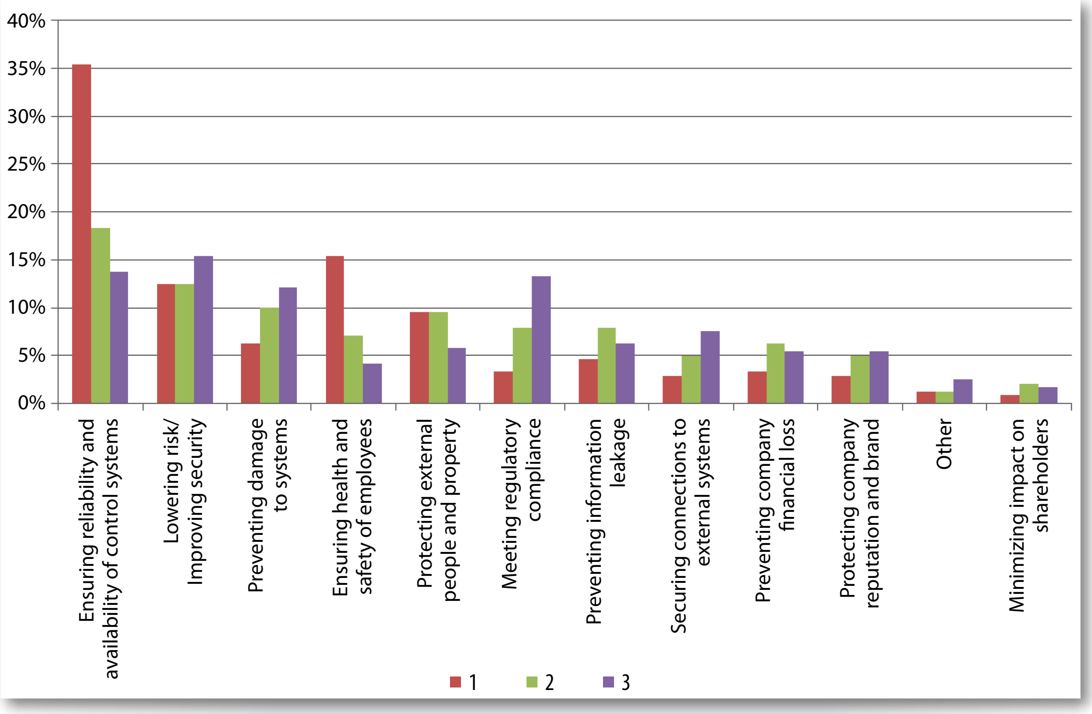


Figure 2. Business Concerns Related to Control System Security

The fifth most highly rated concern, protecting external people and property, fell from the top position (21%) in our previous survey to 10% in just one year. It is unclear what this means. There is clearly a shift in either the attitudes of our respondents or in their perceptions of the attitudes of their companies.

Risk Perception

General-purpose computing assets (human–machine interface [HMI], server, workstations) running commercial OSes are considered to be at greatest risk of compromise by 44% of respondents. Penetration and assessment teams often find routes into control system networks through corporate IT, so it is not surprising that the runner-up, chosen by 14% as their primary concern, is connection of office networks to the internal systems.

Although exploit kits targeting industrial control systems have begun to proliferate, penetration testers know their fastest route onto an ICS network is often through connected business systems. See Figure 3.

Which control system components do you consider at greatest risk for compromise?

Rank the top three, with "1" indicating the component at greatest risk.

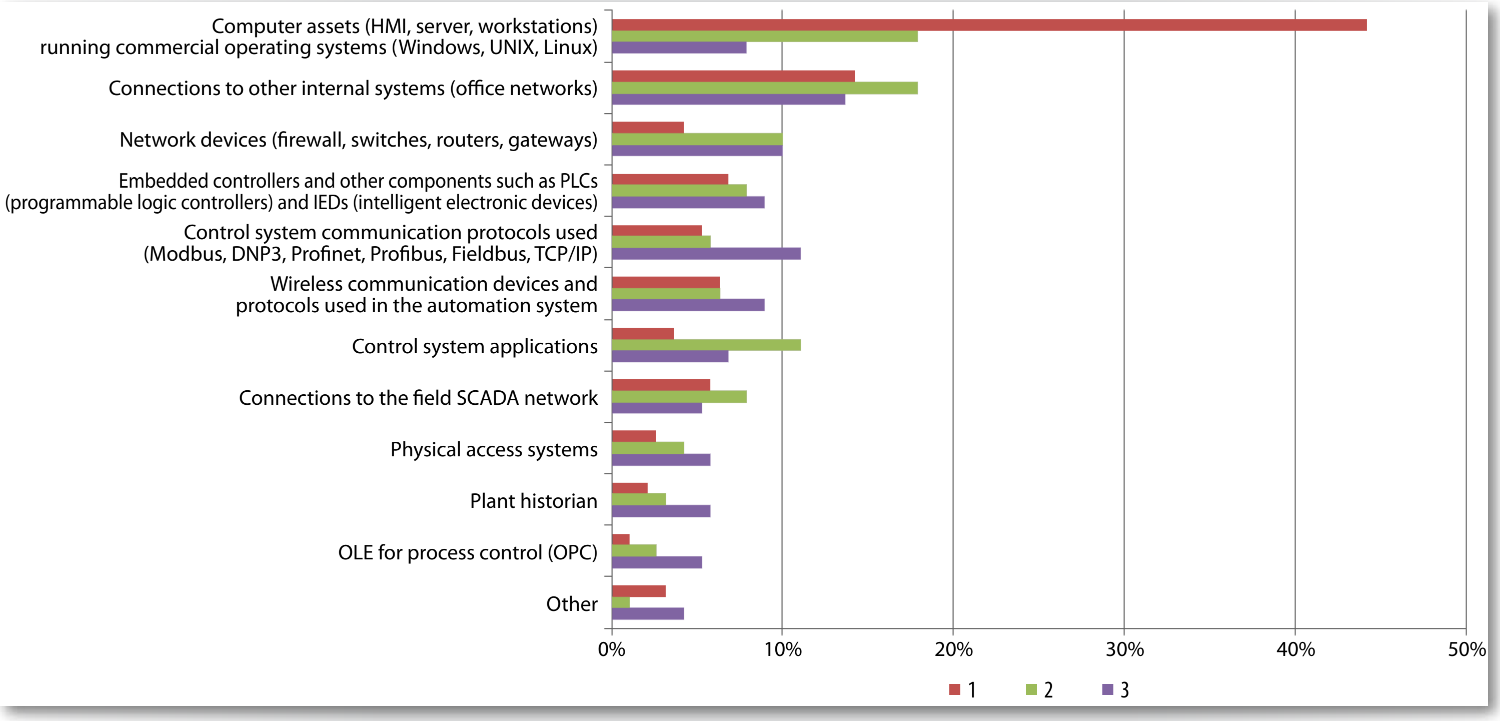


Figure 3. Components at Greatest Risk for Compromise

Survey respondents indicate that the focus remains on securing IT devices and applications, rather than on the industrial control system components themselves. The relative maturity of security tools and practices for general-purpose computers and commercial operating systems may be contributing to the greater attention they receive. Options for securing ICS systems and networks are newer and less tested. Still, technologies such as security information and event management (SIEM) solutions and passive network anomaly detection systems, enabling greater insight into control system networks with decreased risk of operational disruptions, have begun to grow in number and establish their safety and reliability.

Threat Perception

Recognizing that decision influencers often deal more closely with the details of operations, we refined our survey from last year. In addition to asking for the respondents' perceptions, we added a question to learn how decision makers and decision influencers perceived the threat. Figure 4 compares these two groups' perceptions.

TAKEAWAY:

Don't Forget the Data!

Protect data as well as devices. Make multiple levels of backups, verify all current configuration settings and firmware, and limit access to configuration and firmware privileges. Follow strict change-control procedures when you do need to make changes.

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

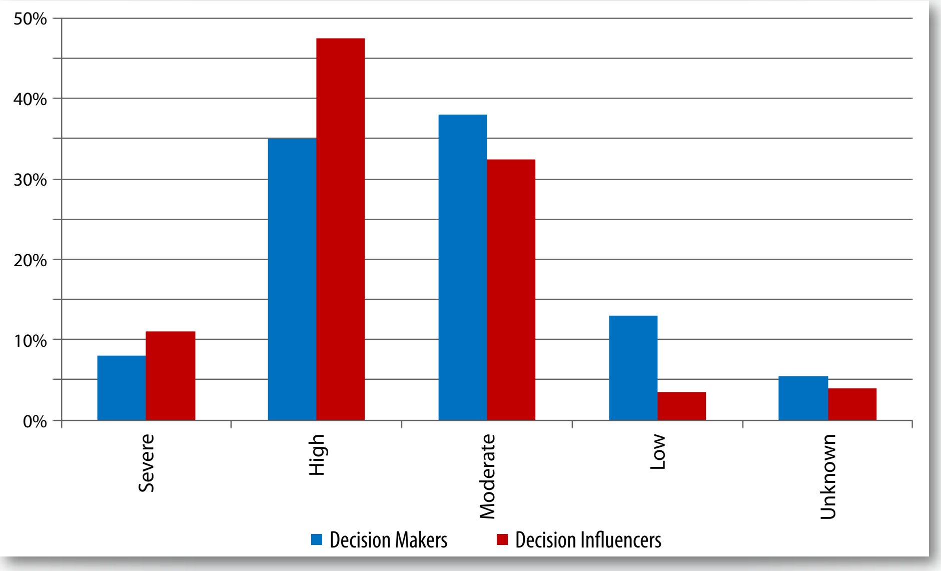


Figure 4. Threat Perceptions

Our respondents believe decision *makers'* concern with cybersecurity threats has decreased over the past year, with significant percentages moving from the highest to more moderate levels of concern. This change may be due to advances in organizational security programs providing better situational awareness and protection. Respondents' answers, however, indicate decision *influencers* are notably more concerned than decision makers, with relatively higher numbers rating their perception of threat as High or Severe, perhaps attesting to their being closer to the problem and playing a more hands-on role in threat mitigation.

Incident Detection

A clear year-over-year trend emerged in respondents' answers to our question about recent control system infiltration. It appears that more breaches are occurring, with 9% of respondents acknowledging six or more breaches in 2014, and 17% noting six or more breaches in 2015. More organizations also acknowledge the possibility of breaches taking place without their knowledge.

Interestingly, due to company policy, 24% were unable to answer whether they'd been attacked—a testament to the tradition of keeping information about potential breaches close to the vest. Figure 5 removes those respondents and shows that 32% of the remaining respondents have experienced a recognized attack.

TAKEAWAY:

Know what is normal.

Lack of visibility into control system devices and networks is one of the greatest barriers to securing these resources.[10] Without awareness of normal communications and activity, it's impossible to properly evaluate or improve security of assets. Operations and security staff must be able to visualize and verify normal network operations to detect and assess possible abnormalities and respond to potential breaches.

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

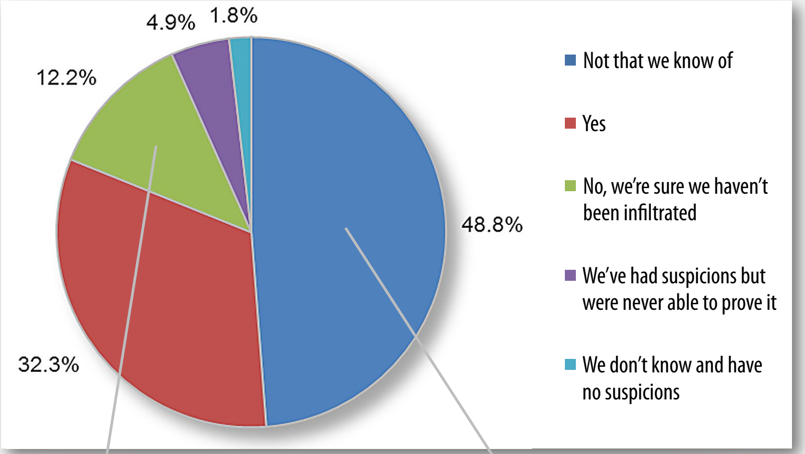
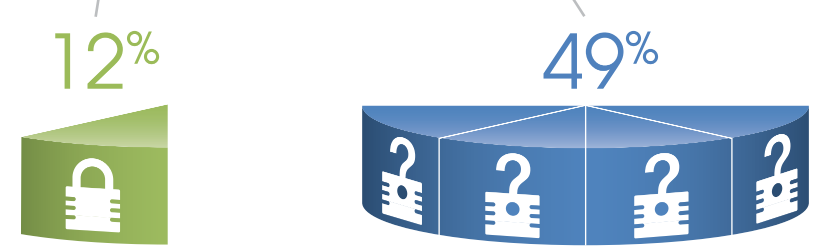


Figure 5. Have your control systems been breached?



Percentage of respondents sure their systems have not been breached

Percentage of respondents not aware of any infiltration or infection of their control systems

[10] www.sans.org/press/sans-releases-results-of-2014-analytics-and-intelligence-survey.php

TAKEAWAY:

Gain visibility into control system networks.

Map all devices, physical interconnections, logical data channels and implemented ICS protocols among devices, including read coils, write registers, scans and time stamps. Establish a fingerprint of normal control network activity and communication, including communication patterns, schedules and protocols. Then, enable device logging, strict change management and automated log analysis based on your baseline data.

Of those who acknowledge a breach, 32% could not put a number on how many incidents had occurred. This reinforces the lack of visibility respondents have into the security of their assets. See Figure 6.

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

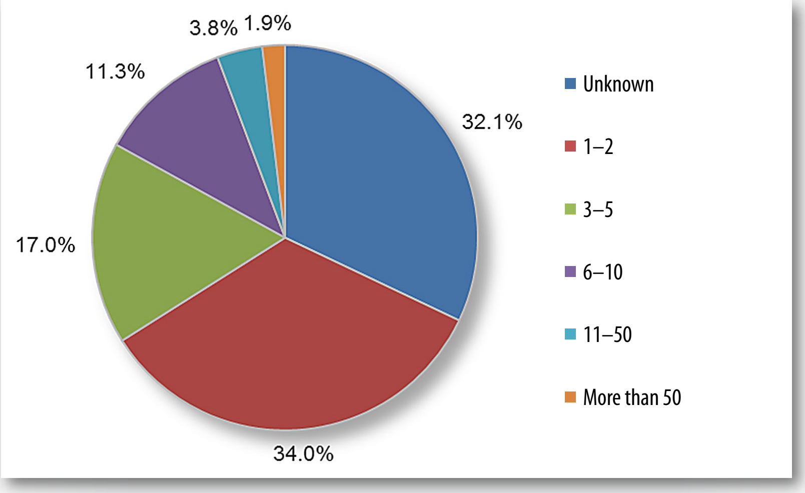


Figure 6. Number of Breaches

Another third reported experiencing more than two breaches within the past year, and the group who believed their systems had been infiltrated six to 10 times in that period more than tripled, increasing from 3% in 2014 to 11% in 2015. This is a dramatic increase and supports the widely reported increasing frequency of attacks on control systems.[11]

Both the degree of uncertainty and the rising number of known incidents are red flags calling for the dedication of greater resources to monitoring, detecting and analyzing anomalous activity in control system networks. Breaches of security that do not disrupt normal operations may still be detected, if trained and knowledgeable personnel armed with the requisite tools look for such breaches. The success of advanced persistent threats (APTs) depends on their operating at a sufficiently slow pace or below a level of network or system noise so as not to be noticed.

Rapid detection is key because the longer breaches remain unknown, the greater the potential impact. Due to the critical nature of many control systems, the documented rise in attacks on these systems[12] and the potential impact of even brief operational disruptions, we investigated the time to detection.

[11] www.dell.com/learn/us/en/uscorp1/press-releases/2015-04-13-dell-annual-threat-report

[12] www.govtech.com/blogs/lohrmann-on-cybersecurity/Hacking-Critical-Infrastructure-is-Accelerating-and-More-Destructive.html

For 39% of respondents, systems were breached for at least 24 hours before security staff became aware of the breach, and 20% reported that they could not determine how long the infiltration had been going on. For an additional 20%, breaches were not detected for more than a week, and 15% reported not knowing about the infiltration for more than a month, as illustrated in Figure 7.

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

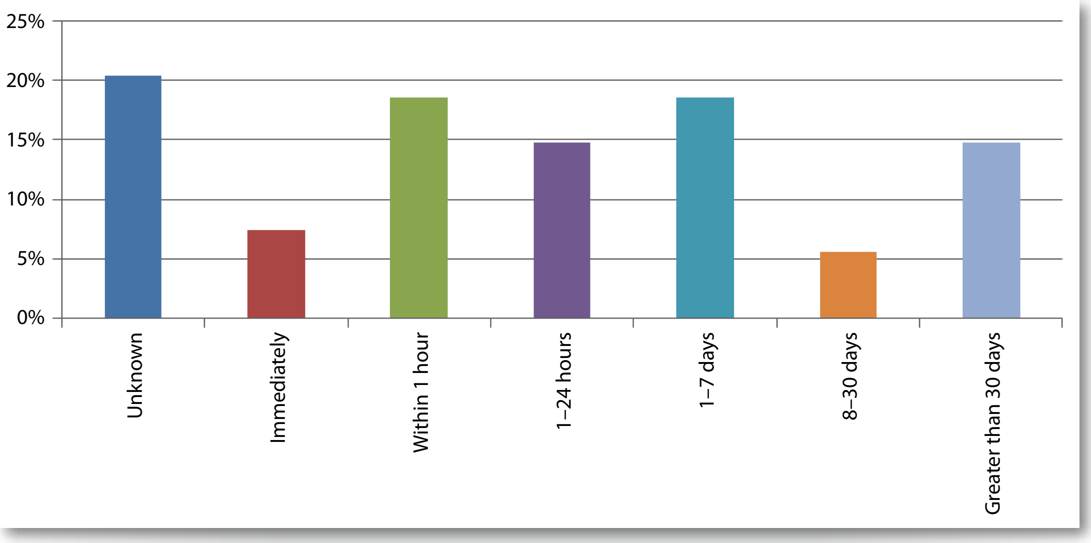


Figure 7. Time to Detection

Various industry reports show that security breaches often go undetected for great lengths of time, even exceeding our greatest answer option by multiples. Such lengthy times to detection provide more than enough time for attackers to complete their reconnaissance and install any illicit monitoring, reporting or disrupting malware. Greater amounts of time also allow attackers to remove the traces that would otherwise provide forensic investigators with the clues necessary to identify them, their actions and purposes. So it comes as no surprise that 44% never identified where the infiltrations or infections took place. Either attackers covered their tracks or the investigations carried out were not sufficient to find them.

Insider threats are recognized as a security problem in all industries. And, current employees were found to be responsible for at least one of their breaches by 25% of respondents (see Figure 8).

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

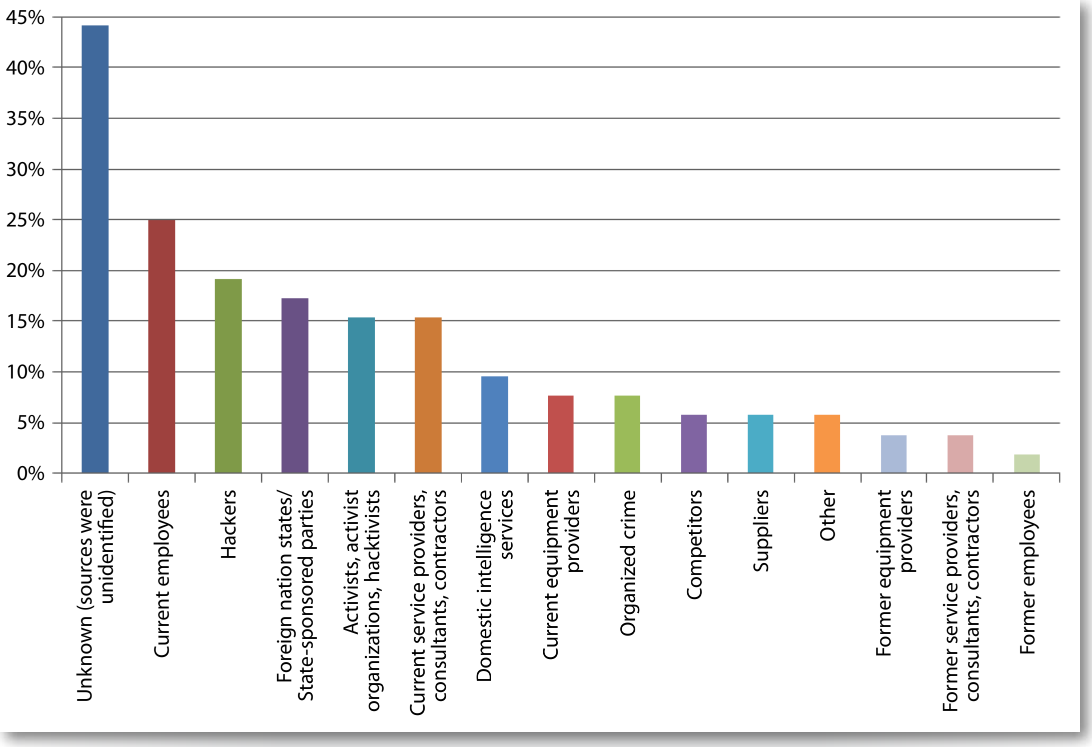
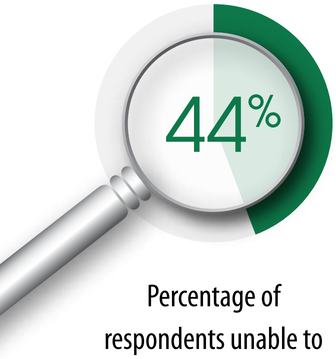


Figure 8. Identified Sources of Breaches



Percentage of respondents unable to identify the source of at least one breach

Threat Vectors

Despite the attacks attributed to internal sources, external actors represent the most concerning threat vectors, chosen by 42% as the top threat and by 73% as one of the top three threats. In 2014, 25% chose external actors as the top threat, and 60% included that category in the top three threats. See Table 2.

Table 2. Top Threat Vectors[13]

	2015				2014			
Vector	1	2	3	Total	1	2	3	Total
External Threat	42%	14%	17%	73%	25%	14%	21%	60%
Internal Threat	11%	14%	24%	49%	14%	9%	14%	37%
Attacks from Within the Internal Network	N/A	N/A	N/A	N/A	10%	12%	12%	34%
Integration of IT into Control System Networks	19%	15%	12%	46%	N/A	N/A	N/A	N/A
Malware	7%	18%	16%	41%	16%	21%	16%	53%
Phishing Scams	6%	11%	13%	30%	12%	14%	9%	35%
Industrial Espionage	7%	15%	7%	29%	8%	12%	5%	25%
Extortion	6%	8%	5%	19%	1%	3%	5%	9%
Cybersecurity Policy Violations	N/A	N/A	N/A	N/A	10%	10%	13%	33%
Other	3%	2%	3%	8%	3%	1%	2%	6%

Nearly every other category shrank, with the exception of industrial espionage and extortion. Extortion ranked in the top three threats by 19% in 2015, up from 10% in 2014. This supports the impression that the Sony attack[14] has had a significant impact on the public mind, given that it was generally characterized as an extortive situation.

The integration of IT into control system networks, a new option chosen by 19% of respondents as the single greatest threat vector, was ranked in the top three by 46%. Those working in this field have long been aware of risks inherent to the introduction of IP-based technology and general-purpose computing devices into control systems. Acceleration of the trend in recent years has increased levels of concern. Awareness of the issues continues to grow, as does IT's level of penetration.

Phishing Scams

A note of concern: Phishing scams fell even lower this year as a concern of respondents despite a growing body of evidence that this key weakness is frequently exploited by attackers.[15] Underestimating the importance of protecting against phishing is the equivalent of not requiring background checks on security personnel. "For two years, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing. The user interaction is not about eliciting information, but for attackers to establish persistence on user devices, set up camp, and continue their stealthy march inside the network."[16]

[13] Results in this table are rounded to the nearest integer for clarity in presentation. This might result in variation of 1 to 2% in total ranking.

[14] www.schneier.com/blog/archives/2014/12/lessons_from_th_4.html

[15] www.industryweek.com/technology/phones-phishing-and-practical-cybersecurity-lessons-2015-data-breach-investigation-report

[16] "2015 Data Breach Investigations Report," www.verizonenterprise.com/DBIR/2015/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2015, p. 12.

Security Controls and Methodologies

Access controls and anti-malware/antivirus continue to be the most commonly used security items in practitioners' toolboxes, both being used by 83% of respondents. Both unidirectional (30%) and bidirectional gaps (66%) are implemented in more than twice as many environments as in 2014 (15% and 25%, respectively). Such results can be interpreted to mean an increasing number of asset owners and operators are segregating their control systems from their business counterparts, a highly important step to securing any networked system. Figure 9 provides a picture of the technologies in use and planned for implementation.

TAKEAWAY:

Training is essential.

Develop cross-functional teams and provide cross-training for all those involved in defending assets. Educate personnel about the new norm for asset protection. All companies, and especially those with critical infrastructure assets, are potential targets. Increasing the default level of asset protection raises the difficulty of mounting a successful attack and reduces the attractiveness of a target. Design security into the environment with appropriate choke points, active defense capabilities and written procedures to enact during an active incident.

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

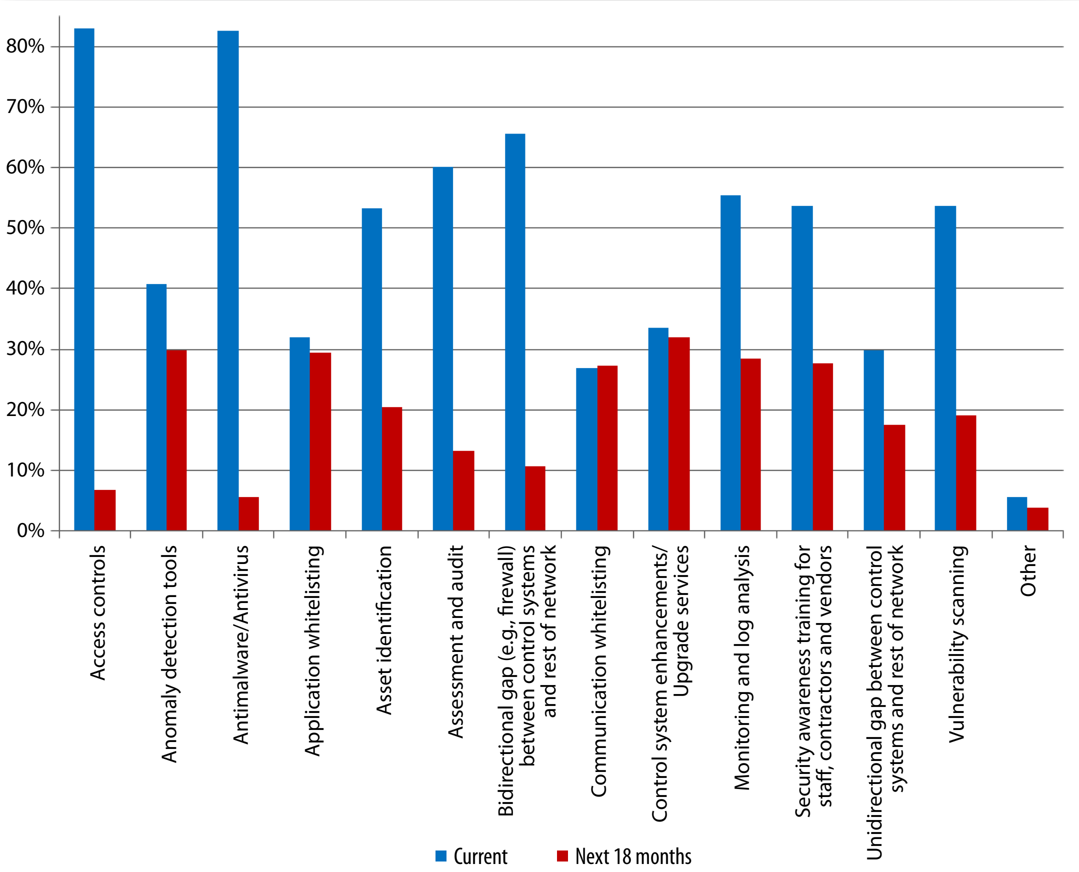


Figure 9. Technologies in Use to Protect Control Systems

Despite economic challenges in some industrial sectors, it is notable that security awareness training has maintained both its current and forecast numbers (54% and 28%, respectively) and has not fallen to budget reductions.

Despite the relatively short period that anomaly detection tools have been available, 41% of respondents report using these technologies, and 30% intend to roll these capabilities out within the next 18 months. Communication whitelisting, another newer technique, is in 27% of our respondents' environments, with another 27% planning to implement it by the end of 2016.

Looking specifically at initiatives intended to increase ICS security, the clear leaders are performing security assessment/audit of control systems and control system networks, chosen by 49%, and security awareness training (41%). They are followed closely by increasing physical security to control access (27%). It is possible that incidents such as the PG&E substation attack continue to keep perception of risks in this area elevated.[17] See Figure 10.

What are the top three most important initiatives for increasing the security of control systems and control systems networks that your organization has planned for the next 18 months? ***Rank the top three, with "1" indicating the most important.***

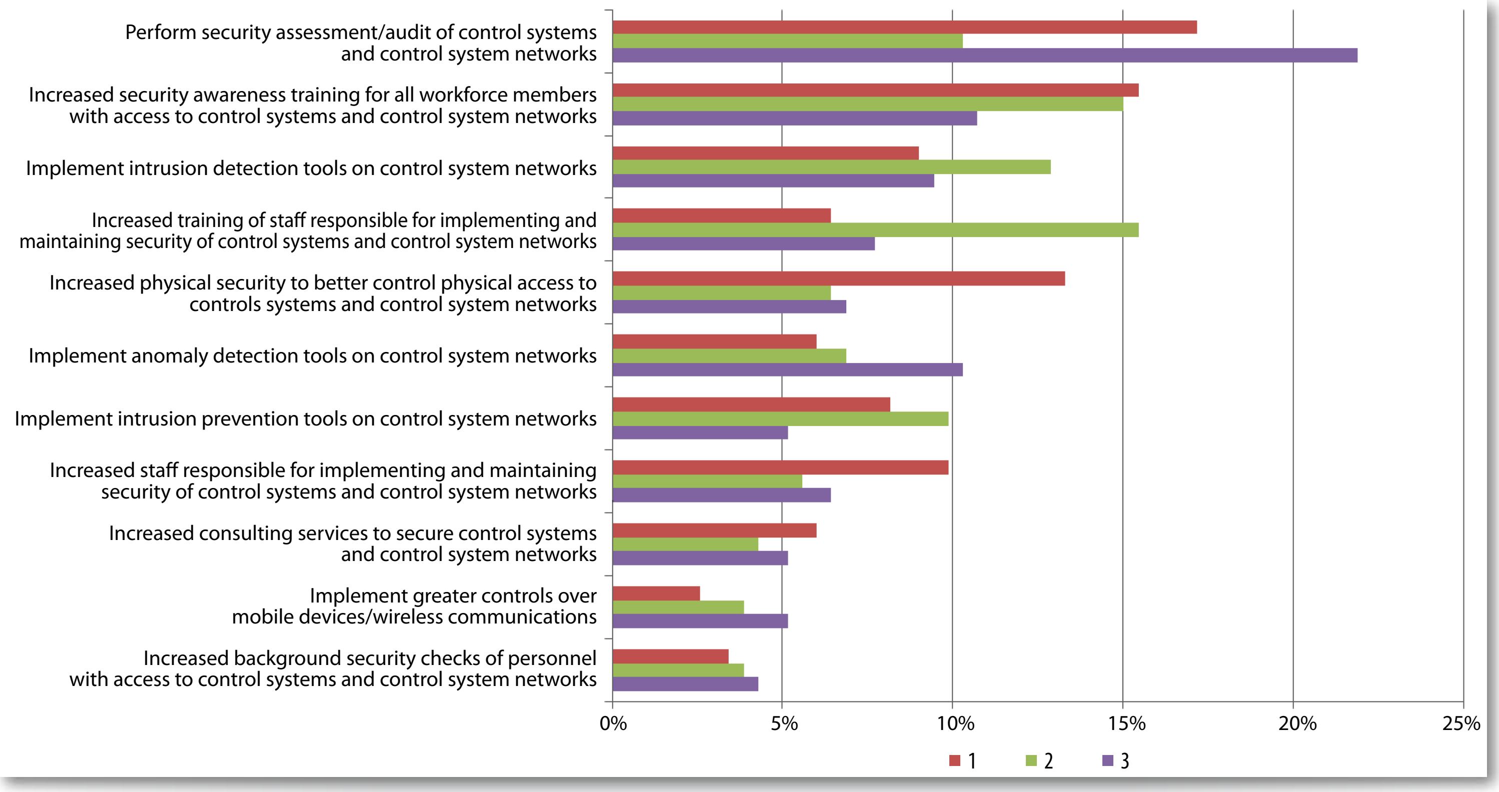


Figure 10. Top Initiatives for Increasing Security

[17] www.wsj.com/articles/SB10001424052702304851104579359141941621778

Vendor Qualification

Considering the critical nature of Site Acceptance Testing (SAT) of industrial control system components, it is concerning that only 20% of respondents stated that qualification of security technologies by their ICS equipment vendors is mandatory, and even more concerning that 25% said it is only moderately important or not important. And 10% didn't know how important it is to validate new security tools before introducing them into control systems. Most respondents (65%) consider vendor qualification of security technologies and solutions to be either highly important or mandatory.

Patch Management

The installation of vendor-validated patches on a regular schedule was the primary method used to handle patching in both 2014 and 2015. Results for 2015 are shown in Figure 11.

TAKEAWAY:

Use Vendor Qualification.

Because many IT security technologies can disrupt normal operations in industrial environments, we recommend that all companies establish qualification plans with vendors to reduce potential risks.

How are patches and updates handled on your critical control system assets?

Select the most applicable method.

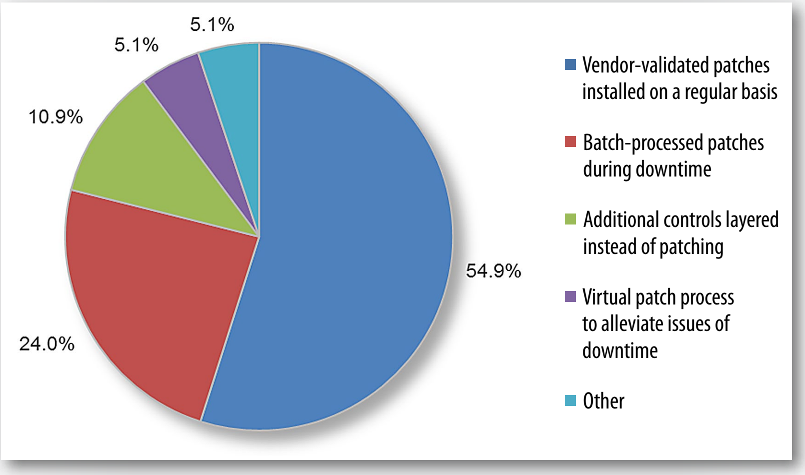


Figure 11. Patching and Updating Assets

We must stress here that failure to conduct regular and frequent patching is a tremendously risky posture. Numerous industry reports identify outdated patches as one of the largest and most commonly exploited points of vulnerability in both IT and control systems. A minimal patch management program must at least provide security practitioners an awareness of what software and systems are out of date so they can monitor for and protect against relevant exploits. For additional information, read information provided by the European Union Agency for Network and Information Security (ENISA)[18] and SANS.[19]

[18] "Risks of using discontinued software," www.enisa.europa.eu/publications/flash-notes/flash-note-risks-of-using-discontinued-software/at_download/fullReport

[19] "Framework for building a Comprehensive Enterprise Security Patch Management Program," www.sans.org/reading-room/whitepapers/threats/framework-building-comprehensive-enterprise-security-patch-management-program-34450

Data Collection

The great majority of our respondents collect and correlate log data from the devices they consider most at risk: network devices and general-purpose computing devices (see Figure 12).

Of the following system components, select those that you are collecting and correlating log data from.

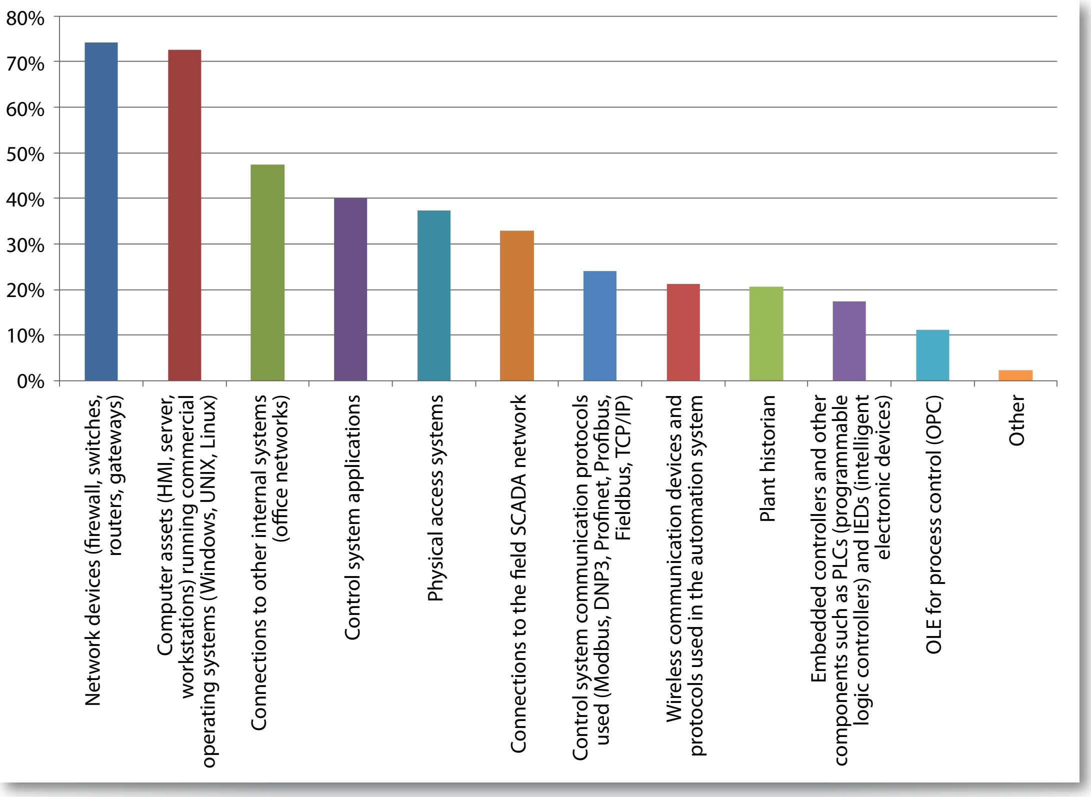
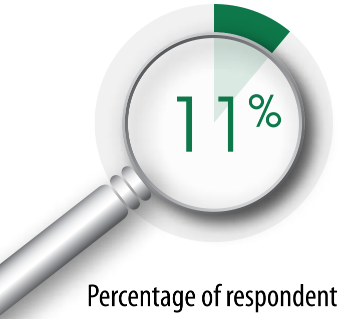


Figure 12. Log Data Collection Points

Once again, OLE for Process Control (OPC) was rated as the least frequently monitored asset—even though it often provides communications between control systems and corporate networks. We noted last year that this role and lack of oversight makes OPC a highly attractive target for attackers seeking a point to pivot from business to operations networks—and it appears this remains true.



Percentage of respondents collecting logs from OLE for process control (OPC) systems that provide communications between control systems and corporate networks

TAKEAWAY:

Protect the weakest points first. ICS protocols (e.g., Modbus/TCP, DNP3 without authentication, Ethernet/IP, ProfiNet, BACnet, ISO-TSAP, S7, ICCP without certificates, and similar) are inherently vulnerable. Use uni- and bidirectional firewalls and strict operational procedures to control access to communication channels. Investigate latency and scan rate challenges using SSL or IPSEC for communication to field devices and ICCP links. Also protect vulnerable OPC systems and database servers, which attackers can use to initiate attacks internally and infiltrate other systems.

Network Documentation

TAKEAWAY:

Document connections. Incorporate a network traffic analyzer designed for use with control systems to document existing connections and monitor for new ones.

Identifying and detailing connections and attached devices in a network is a key step in securing it, yet most (74%) of respondents believe their external connections are not fully documented. Whether external connections are opened by third parties, internal operators or others, many of these connections use the Internet as a conduit, exposing critical infrastructure to direct attack. The Internet of Things[20] and Industrial Internet of Things[21] trends will continue to drive proliferation of inter-network linkages and threat exposures for the foreseeable future.

Without specialized tools, tracing connections can be very time-intensive. Active scanning of control system environments can cause operational disruptions, and most active scanners are designed for identifying commercial OS vulnerabilities. ICS-specific passive traffic monitoring applications such as passive network anomaly detection systems can aid in scanning operations.

Assessing Security

TAKEAWAY:

Find people with adequate skills and experience. Consulting firms and service providers with experts in ICS security are few, but they are growing in number and capacity. Utilize these resources whenever possible or provide the essential ICS security training and tools your organization needs.

As valuable as security assessments are, they are snapshots, and their accuracy and value diminish with age. The fact that 40% of respondents last performed an assessment more than six months ago and 9% have never done a security assessment of their control systems or control networks means many organizations are working with obsolete information. Although there is no one-size-fits-all frequency to performing security assessments,[22] the risks of unknown exposures and vulnerabilities in critical infrastructure argue for minimal delays between assessments.

Most (69%) of the assessments carried out in respondents' companies are performed by internal teams. However, people with the required skills and experience are in short supply and high demand, and very few operating companies have them on staff, which calls the value of the efforts of these internal teams into question.

[20] www.csoonline.com/article/2687653/data-protection/new-toolkit-seeks-routers-internet-of-things-for-ddos-botnet.html

[21] www.techradar.com/news/world-of-tech/forget-smart-fridges-the-industrial-internet-of-things-is-the-real-revolution-1287276

[22] www.supplychainbrain.com/content/general-scm/sc-security-risk-mgmt/single-article-page/article/key-steps-to-minimize-unplanned-downtime-and-protect-your-organization

Establishing a Secure ICS Program

- Develop and implement a security policy aligned with relevant standard(s). (See "The Security Policy" section later in this paper). Use policies and standards to guide the security program.
- Engage device and application vendors as partners in establishing and improving security. Communicate the expectation that secure systems are the foundational requirement for continued business relations.
- Require third-party security evaluations of software and devices. Where vulnerabilities are found, require remediation plans and progress reporting.
- Maximize security of operating systems through restrictive configuration settings and use of hardened systems whenever possible. Although Windows has a limited number of options from which to choose, Linux provides many secure distributions. Provide security training for staff to enable their implementation of these directives.
- Implement passive ICS network mapping and communications monitoring, configuration analysis tools and, where feasible without operational disruption, deep packet inspection of ICS protocols.
- Establish incident-handling procedures to return to a secure state. Once an intrusion is detected, assume all systems are compromised.
- Secure operating protocols (such as OPC), networks and devices capable of serving as pivot points.

WARNING

Active scanning and control networks. Never use an active scanner within an operational control network. It can disrupt operations. Most active scanners are tuned to identify vulnerabilities on commercial operating systems, not control system-embedded devices and applications. As a result, they do not identify weaknesses in control system cyber assets—the signatures they look for aren't there.

Vulnerability Detection

No single tool can cover all exposures in control system networks, and security practitioners are well-served to use a variety. The largest number of respondents (59%) monitors CERT notifications. Evaluation and implementation of guidance from organizations like this and industry information-sharing groups should be continual and ongoing.

More of our participants have engaged with their equipment vendors in identifying and mitigating vulnerabilities (49%, up from 41% in 2014). This is a positive indication of the growing awareness of their own essential active and continuing role in protecting organization assets. See Figure 13.

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

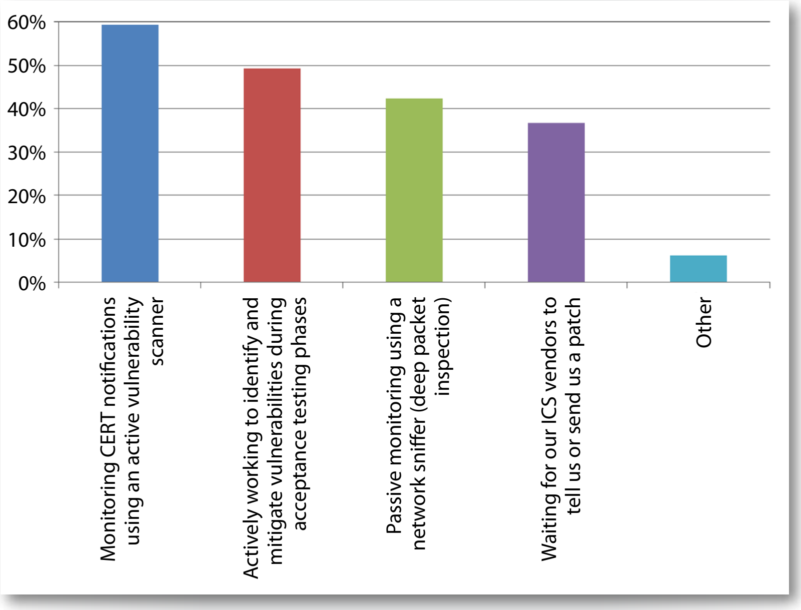


Figure 13. Vulnerability Detection Processes

We would like to see greater use of nondisruptive tools (passive monitoring designed specifically for the particular considerations of control systems and their networks) than the 42% represented in this survey.

TAKEAWAY:

Establish documented procedures. Create well-defined incident response procedures that identify roles and responsibilities, as well as provide authorizations for actions that affect operations. Develop or adopt cradle-to-grave procedures for managing each type of cyber asset used by the organization from requisition through decommission and redeployment. Most importantly, communicate and implement these procedures.

Threat Intelligence

Many respondents are following some recommended practices to detect threats aimed at their control systems: 49% have trained security staff, 45% use third-party intelligence from security vendors, 44% work with governmental agencies and 45% participate in industry information-sharing groups. Although all of these methods are valuable and complementary, they are not all in use by the same companies. As noted previously, a combination of intelligence tools is the best way to ensure asset protection.

We also observed a reduction in the number of respondents who rely on their own staff for their threat intelligence needs. Monitoring and tracking the flow of information regarding threats, threat actors and active attacks—as well as analyzing that data and producing targeted intelligence relevant to the specific considerations of each company—call for a specialized set of skills not commonly found in security practitioners.

Incident Reporting

When encountering signs of infection or infiltration, survey participants turn first to the same four groups: internal resources, government organizations, control system vendors and security consultants. A greater number of respondents consult with vendors (45%) and security consultants (38%) than in the past (37% and 33%, respectively in 2014). And they are significantly more likely to contact a cybersecurity solution provider than before (32% in 2015 compared with 21% in 2014). Figure 14 provides a complete breakdown.

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

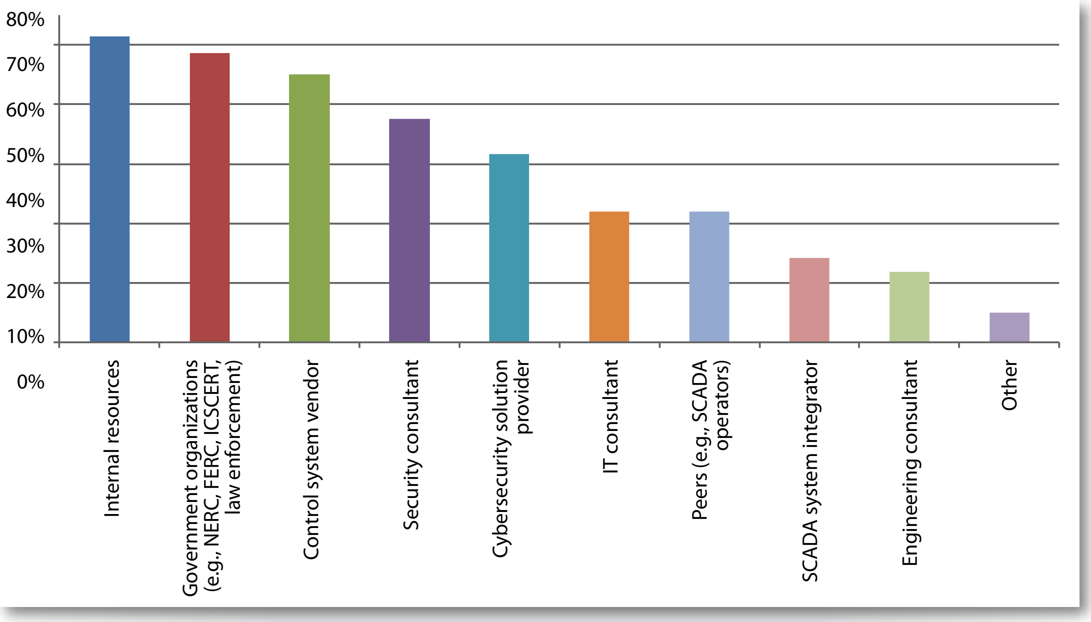


Figure 14. Incident Response Support

Security Policy

Most (86%) respondents identified the individuals with responsibility for control system security policy as titled officers, including chief security officer, CIO, chief information security officer, information security officer and CEO. For 8% of respondents, no single individual set policy; rather, policy was set by committees, teams and boards. The evolving nature of the control system security landscape and the unique characteristics of each operation certainly appear to contribute to the diversity of models in use.

IT and control system networks are still very different environments,[23] and a strong working knowledge of both is required to set and implement successful policies. We consider the involvement of cross-functional teams a positive indication that organizations are working to ensure inclusion of all aspects of the systems and networks involved.

Security Controls

To gain deeper insight into security responsibility, we also studied who implements the subsequent controls. It is no surprise to see that for 56% of respondents the asset owners/operators are chiefly responsible, with 40% tapping engineering management (see Figure 15).

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

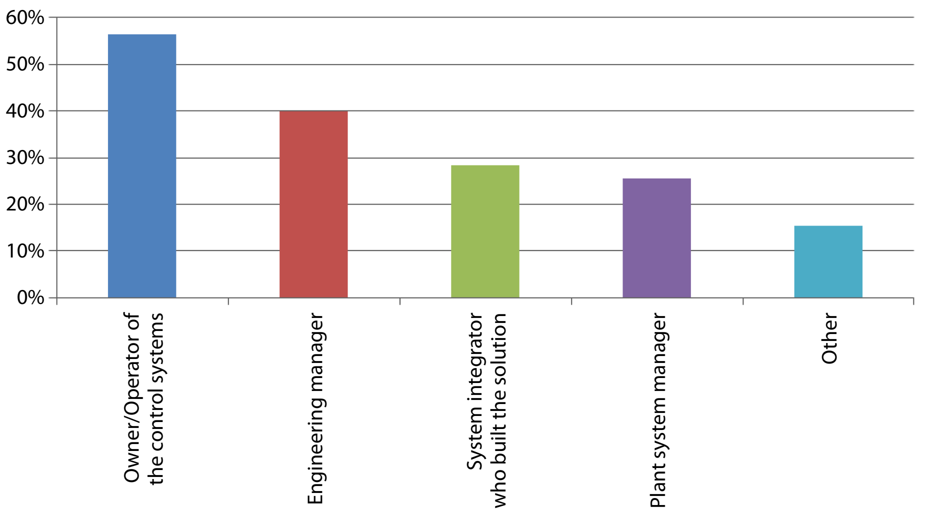


Figure 15. Control Implementation Responsibility

Investigation of responses in the "Other" category revealed that 6% assign implementation of security controls to IT personnel. If such personnel are involved, it is essential that their IT-derived experience is sufficiently supplemented with ICS training. See Appendix A, "ICS Security Training," for a selection of available options.

[23] www.smartgridtoday.com/public/SECURITY-EXPERTS-Utility-IT-OT-still-miles-apart.cfm

Security Standards

Data from our 2014 survey indicated that the United States NIST Guide to SCADA and Industrial Control Systems Security was the primary standard in use, with 32% of respondents mapping to it and another 22% intending to follow suit. It appears that many moved forward with those plans, as 49% of respondents this year indicated they were mapping to NIST. NERC CIP was used by more respondents, moving from use by 20% in 2014 to 37% in this year's survey. The Critical Security Controls (34%) and ISA99 (29%) are also used more frequently than in the past, as shown in Figure 16.

Which cybersecurity standards do you map your control systems to?
Select all that apply.

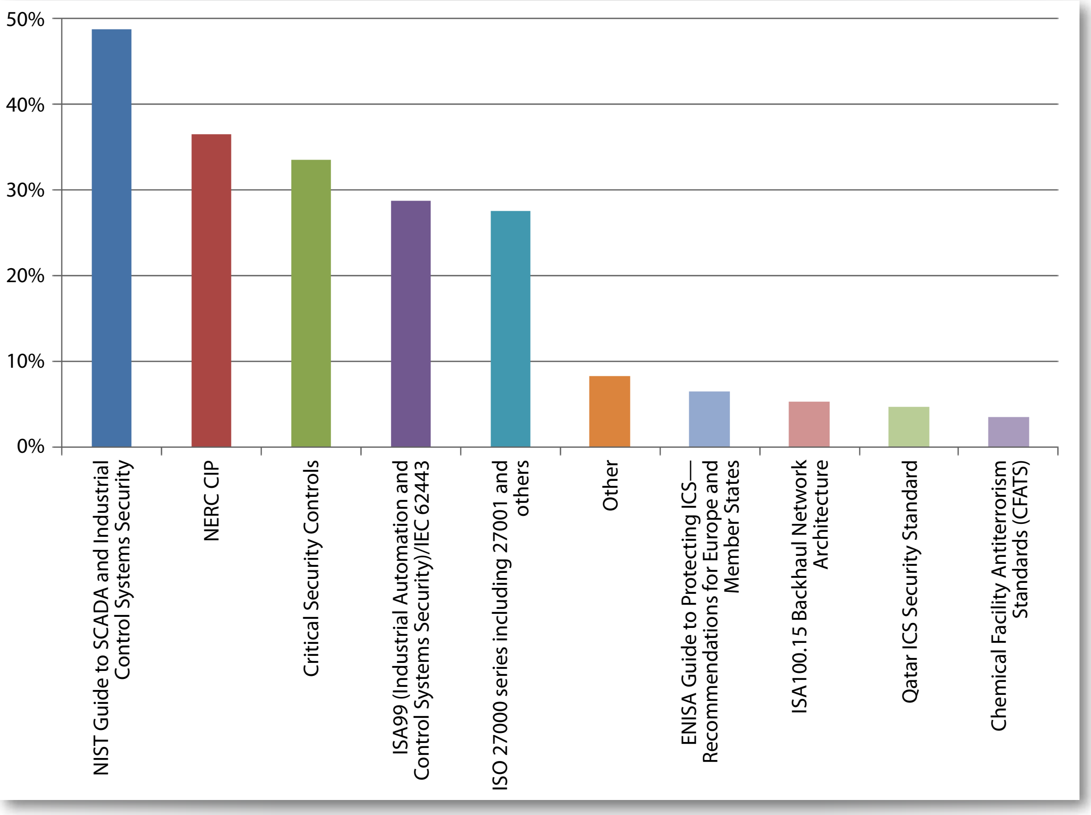


Figure 16. Standards Mapping

Systems Procurement

Securing existing assets and systems is inescapably important, but a full life-cycle approach includes security in procurement. We find this year's results encouraging in that more respondents consider cybersecurity in their automation systems procurement process. The group indicating it does not consider cybersecurity in automation systems procurement process decreased, from 9% in 2014 to 6%. Those confirming they do consider cybersecurity grew to 35% (from 32% in 2014), while those who "somewhat" do also grew to 37% (from 35% in 2014). See Figure 17.

TAKEAWAY:

Integrate security into procurement and decommissioning processes. Establishing the security of software or devices is cheaper, easier and more effective prior to deployment. The burden of maintaining security is lighter when you start from a secure state. And, security should be included in the decommissioning and removal of devices to avoid opening serious vulnerabilities.

Do you normally consider cybersecurity in your automation systems procurement process?

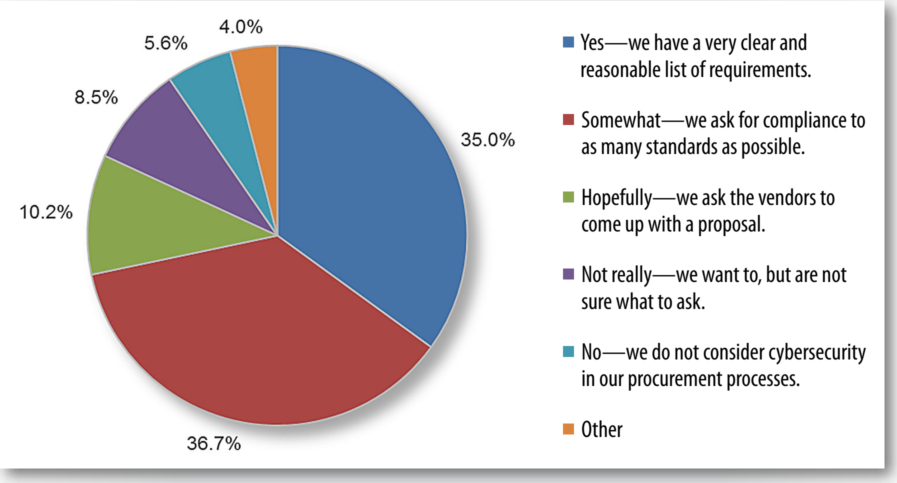


Figure 17. Consideration of Cybersecurity in the Procurement Process

This growth, however small, is a positive trend. The question of who should bear the cost of increased security can be a contentious one, with both vendors and customers presenting business cases placing the burden on the opposite party. Whether operations or market share is at risk, everyone has a stake in preventing security breaches. We hope to see increasing consideration of cybersecurity in procurement processes drive greater efforts to include security from initial product design through disposal.

IT-ICS Convergence

Ongoing issues arising from the continuing integration of commercial operating systems (Windows, Linux, UNIX) and open communication protocols into control system networks encouraged us to study how participants are dealing with this convergence of technologies.

Considering the magnitude of the changes that drive the trend,[24] we wondered if participants have a plan as general-purpose devices and IP-based technologies continue to grow within control and automation system environments. The majority (83%) recognize the importance of having a security strategy to address the convergence of information and operational technologies. Unfortunately, only 47% actually have a strategy, as shown in Figure 18.

Does your company have a security strategy to address the convergence of information and operational technologies?

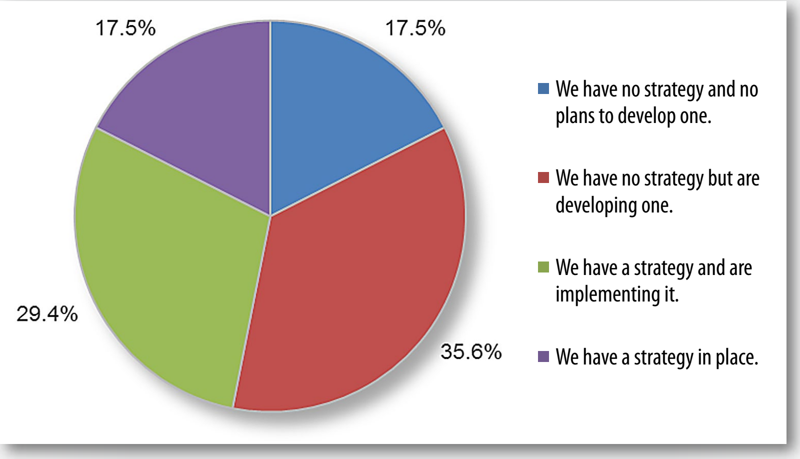


Figure 18. Strategies for IT-ICS Convergence

The changes associated with IT-ICS convergence have been ongoing,[25] and many are both fundamental and far-reaching in effect.[26] Although the unique considerations of each enterprise prevent the creation of a universal road map to deal with these changes, much guidance does exist on approaches to the problem. A simple Google search identifies many sources on the subject. It is clear the most serious mistake an organization could make would be not taking on the challenge of managing this convergence with a plan.

The survey also examined the collaboration between IT and control systems operations groups. The majority (70%) of our respondents noted a moderate level of such collaboration. We hope that the remaining 30% have acquired or developed the requisite knowledge and skills within their operations environments. On the positive side, 73% of respondents indicate a trend toward increased collaboration.

[24] www.intelligentutility.com/article/13/09/fusion-it-and-ot-utilities-0

[25] www.gartner.com/newsroom/id/1590814

[26] www.wirelessdesignmag.com/articles/2014/09/how-it-and-ot-are-converging-avoid-pitfalls-reap-benefits

Security Budgets

Another positive trend is that in 45% of the respondent companies, IT and operations jointly control the control systems security budget, as shown in Figure 19. This should promote recognition of common goals and further collaboration.

Who controls the control systems security budget for your company?

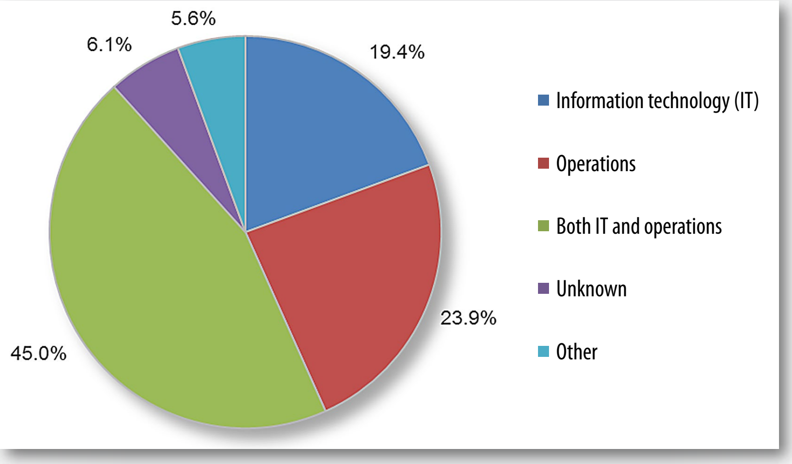


Figure 19. Control of the Control Systems Security Budget

It is encouraging that 47% of respondents noted they had some insight into the budget. We consider that positive because it indicates that those in the trenches are at least partially involved in the budgeting process, likely including participation in setting priorities. Unfortunately, that leaves another 53% of respondents with no knowledge of the budgets. Figure 20 illustrates what we know about the control system security budgets after removing the responses of those with no knowledge.

What is your organization's total control system security budget for 2015?

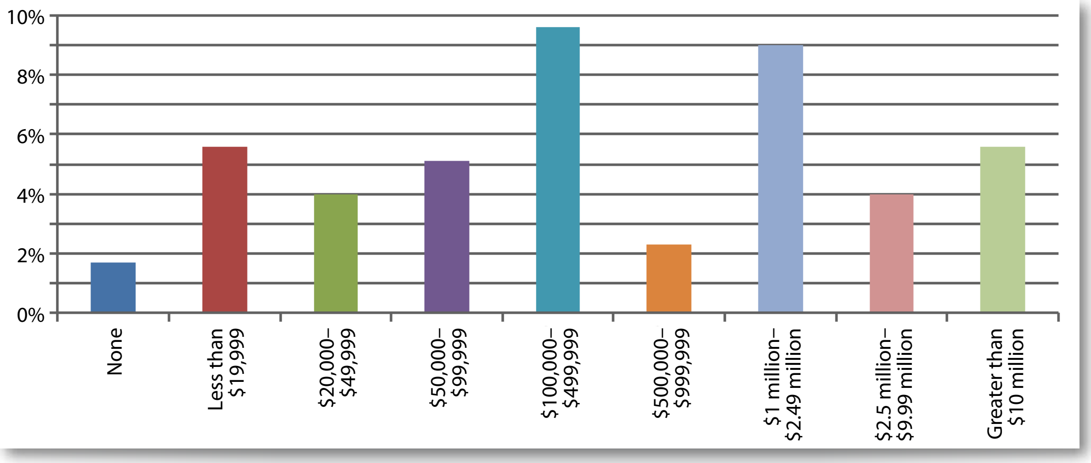


Figure 20. Control System Security Budgets

Almost as many indicated a control system security budget of less than $100,000 (16%) as did a budget of $1M or more (19%), and exactly the same number (6%) have less than $20,000 for security (not counting those with no budget at all) as have more than $10M.

Conclusions

Multiple factors drive the increased targeting of control systems. Connections within and across network boundaries continue to grow at an accelerating rate, opening new points of exposure. The introduction of IP-based technology and general-purpose computing devices into operational environments is introducing new vulnerabilities along with their benefits. At the same time, the sophistication, capabilities, motivations and numbers of threat actors are also increasing.

To succeed at protecting these environments, control system and information security professionals need sufficient training, tools and support—not only so they can respond to ongoing attacks, but also so they can proactively identify and implement safeguards to prevent future ones. Yet, the survey suggests necessary resources may be lacking in many organizations. Rectifying this problem requires increasing cybersecurity budgets. We believe it essential that business leaders provide security practitioners with the tools, training and resources to gain the knowledge and insight needed to protect these critical assets.

Another challenge highlighted in the survey, a lack of visibility into control system equipment and network activity, continues to inhibit progress in securing assets and decreases confidence in the accuracy of self-evaluations of vulnerability levels and the number of breaches experienced.

The results are not all negative. On the positive side, we see collaboration between IT and control systems personnel on the rise, although there is much room for additional improvement. Similarly, products and services to improve insight are increasing in response to the need. We consider this crucial because vendors must also take an active role in developing solutions. No single party can solve all the problems that have grown in and around this space.

It is SANS' hope that the entities with the most to lose, particularly the organizations built on the dependency and reliability of their control systems, will recognize the rising level of risk and focus their resources on addressing the serious threats to their continued operations. For our part, we will continue our mission to support them in their efforts.

Appendix A: ICS Security Training

A variety of ICS certifications and training resources are available.

ICS Certifications

Global Industrial Cyber Security Professional (GICSP). This certification combines the perspectives of IT, engineering and cybersecurity to provide vendor-neutral training to secure industrial control systems from design through retirement. See www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

Information Assurance Certification Review Board (IACRB) Certified SCADA Security Architect. This certification provides documentation that the individual has the knowledge to be able to secure a power transmission, oil and gas, or water treatment industrial control system. See www.iacertification.org/cssa_certified_scada_security_architect.html

International Society of Automation (ISA). This organization provides ICS-specific training and subsequent certification for successful applicants. The most applicable certification is ISA99: Cybersecurity Expert. See www.isa.org/templates/two-column.aspx?pageid=121797

Training Programs

We have listed just two nonprofit organization training programs. There are, however, numerous commercial opportunities. For a more exhaustive listing, search using "ICS Security Training" to guide your efforts.

The U.S. Department of Homeland Security offers both virtual and instructor-led industrial control system security training through the Industrial Control System–Computer Emergency Response Team (ICS-CERT). Course descriptions and a calendar of planned courses are available at https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

The SANS Institute offers self-paced online training as well as remote- and classroom-based instructor-led industrial control system security training through the SANS ICS curriculum. Course descriptions, instructors and a calendar of planned courses are available at http://ics.sans.org

About the Authoring Team

Derek Harp is currently the business operations lead for the Industrial Control System (ICS) programs at SANS. He has served as a founder, CEO and advisor of startup companies for the past 16 years with a focus on cybersecurity. Derek is also a co-founder and board member of a company focused on the security technology needs of ICS asset owners. Derek is a former naval 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 cybersecurity solutions. He brings 20 years of experience in management of IT and infrastructure projects, enterprise security governance, information security risk analysis, regulatory compliance and policy conformance for high profile companies to bear in his writing. Bengt has managed multiple patents from ideation through the development and issuing phases.

Sponsors

SANS would like to thank this survey's sponsors:

SURFWATCH CYBER IN SIGHT

tenable® network security

Last Updated: January 4th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Miami 2019	Miami, FLUS	Jan 21, 2019 - Jan 26, 2019	Live Event
Cyber Threat Intelligence Summit & Training 2019	Arlington, VAUS	Jan 21, 2019 - Jan 28, 2019	Live Event
SANS Dubai January 2019	Dubai, AE	Jan 26, 2019 - Jan 31, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NVUS	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LAUS	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS SEC504 Stuttgart February 2019	Stuttgart, DE	Feb 04, 2019 - Feb 09, 2019	Live Event
SANS FOR610 Madrid February 2019 (in Spanish)	Madrid, ES	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, GB	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Anaheim 2019	Anaheim, CAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Vienna, VAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Zurich February 2019	Zurich, CH	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TXUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, JP	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Riyadh February 2019	Riyadh, SA	Feb 23, 2019 - Feb 28, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VAUS	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MDUS	Mar 02, 2019 - Mar 09, 2019	Live Event
SANS Training at RSA Conference 2019	San Francisco, CAUS	Mar 03, 2019 - Mar 04, 2019	Live Event
SANS Secure India 2019	Bangalore, IN	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MOUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CAUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS London March 2019	London, GB	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 23, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Bangalore January 2019	OnlineIN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced