Securing Industrial Control Systems-2017

Bengt Gregory-Brown

Securing Industrial Control Systems—2017

A SANS Survey

Written by Bengt Gregory-Brown

Advisor: Doug Wylie

June 2017

Sponsored by
Great Bay Software, Nozomi Networks, PAS Global,
Tempered Networks, and Tripwire

Prologue

Ensuring the cyber security of our industrial plants and infrastructure is a critical concern for everyone. Fortunately, industrial managers recognize these risks, and many have launched programs based on popular standards, including IEC-62443 and NERC CIP. While they hoped that this would solve their problems, many are frustrated with the never-ending stream of requests for new technology and resources. They don't want to become cyber security experts, but they need to be sure that their organization has an appropriate, cost-effective plan for managing cyber threats.

Understanding what others are doing is essential guidance for these managers and their cyber security teams. This includes information on critical topics like standards, responsibilities, best practices and technology. Charting one's own course through today's complex cyber environment is simply too slow and inefficient, given the growing risks. Information in this SANS Institute report should be useful for companies just starting their cyber security journeys, as well as those facing the challenges of sustaining effective programs.

The findings of this SANS research are quite interesting. Despite some significant differences in the survey groups, the results align quite well with ARC's ICS cyber security surveys of plant operators, process control engineers and manufacturing IT specialists. Everyone considers budgetary constraints and the introduction of potentially insecure Industrial Internet of Things (IIoT) devices as major challenges. Plant personnel are also concerned that investments in technology have given managers a false sense of security, while lack of resources and security management tools are undermining the effectiveness of these defenses. Lack of cyber security expertise is another critical issue, and plant personnel recognize the need for convergence of IT and operational technology (OT) cyber security efforts. But plant personnel still lack trust in IT groups. Seeing that this concern is appreciated by all the groups who participated in the SANS survey is very encouraging. Cultural roadblocks have been jeopardizing the security of our critical infrastructure for far too long. We hope that a shared understanding of the challenges will help us overcome this major obstacle.

—Sid Snitkin, PhD, Vice President and General Manager,
Enterprise Advisory Services, ARC Advisory Group

Executive Summary

We annually gather and analyze raw data from hundreds of IT and industrial control systems (ICS) security practitioners across a variety of industries, people whose work places them in positions of responsibility to identify risks and safeguard control systems and networks from malicious and accidental actions. It is our mission to turn these inputs into actionable intelligence that can be used to support new developments and address ongoing trends in the field, to inform the crucial business decisions that determine allocation of resources, prioritization of protective measures on critical assets and systems, and planning of new initiatives.

Key Results

- **46%** of responders who are privy to budgetary information report their ICS Security budgets increased from their fiscal year 2016
- **44%** consider the top threat vector to their ICS to be adding devices to the network that can't protect themselves
- **35%** rate extortion (including ransomware) as a top threat vector, almost doubled from 2016
- **36%** have budgetary priorities to perform security assessments and audits of ICS networks
- **24%** consider embedded controllers to be at greatest risk, and **32%** consider the impact of this risk to be greatest in event of a compromise
- **48%** map their security internal standards, policies and practices to NIST's Cyber Security Framework
- **69%** consider the threat to ICS systems to be high or severe/critical

The importance of this information grows with each iteration of this report because reliance on control systems continues to expand across not only industrial settings, but also the operation and maintenance of our cities, our buildings and all kinds of modern smart applications. The convergence of IT and operational technology (OT) has now come into popular awareness as the lines between the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) have blurred and the media have given increased coverage to security breaches and their impacts.

ICS systems control and monitor industrial and infrastructure processes that produce products and deliver services and are referred to in various settings as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), process control systems (PCS), process control domains (PCN), programmable logic controller and programmable automation controller systems (PLC/PAC), and building automation and control systems (BACS). Related terms include IIoT, the Industrial Internet, Industry 4.0 and the Connected Enterprise.

ICS and OT are used interchangeably in this paper because ICS is the enabler for operational technology systems used in industrial applications. OT is used primarily to distinguish cyber-physical systems that produce and deliver products and services, in contrast to IT systems that serve and support data-driven business operations.

With greater awareness comes greater attention. ICS security budgets, despite the fact that many businesses face ongoing budgetary challenges, are largely stable or growing, for respondents who are privy to such information. Recognition that even dedicated, special-purpose ICS components, such as intelligent embedded devices and programmable devices that are used for command and control, can carry vulnerabilities exploitable by malefactors is increasing among ICS security practitioners and the broader security community, as is concern about ransomware, which has started to invade the corners of almost any digital system. Awareness has led some corporate leaders and IT to be proactive and take action, such as providing new and expanded investments to offset related risks and better ensure safe, reliable and available operations. This report discusses these trends and other changes across companies that make active use of ICS as a core enabler for business imperatives and provides actionable advice for today's security practitioners.

Security Roles and Responsibilities

As in years past, respondents to this survey came from all sizes of organizations, from very small (fewer than 100 employees) to very large (more than 100,000). The sample is fairly evenly distributed, with almost 32% having more than 10,000 employees, 34% having between 1,001 and 10,000 employees, and 34% having fewer than 1,000 employees. Individuals came from a variety of industries, including energy/utilities, business services, oil and gas (production or delivery), engineering services and control system equipment manufacturers, transportation, control system services, healthcare and chemical production, among many others. Forty-nine percent (49%) of the sample came from industries that are easily recognizable as using control systems as critical enablers of company operations.

Many respondents (34%) have earned one or more ICS-related professional certifications. This is a positive trend, growing by 7% over 2016 results. Because the bulk of the sample is from the SANS audience, it is not surprising that 56% have earned the Global Industrial Cyber Security Professional Certification (GICSP). Other certifications or certificates reported include the ISA99/IEC 62443 Cybersecurity Fundamentals Specialist Certificate (19%) and IACRB's Certified SCADA Security Architect (10%).

Focus of Role

Survey respondents largely were consistent with the SANS audience demographic; 26% of respondents listed their role as security administrator or security analyst. Few (6%) have roles strictly related to ICS activities such as process control engineer, control system operator, operations or plant director, or production engineering manager. With that said, though, 27% indicated that their primary emphasis is on ICS operations. Another 31% split their time between IT/business operations and ICS operations equally, while the remainder do not consider ICS security to be their primary emphasis.

More than one-third (37%) of responders who hold an ICS-related certification or certificate spend at least half their time on ICS cyber security, and most of those (25%) appear to be almost exclusively focused on this area (see Figure 1 on the next page).

TAKEAWAY

Considered in combination with the high-impact risks of operational disruption, we recommend that organizations protect their own interests with staff wholly focused on ICS security rather than requiring staff to split time and attention across multiple missions.

In your current role, indicate approximately how much of your time is spent on ICS cyber security.

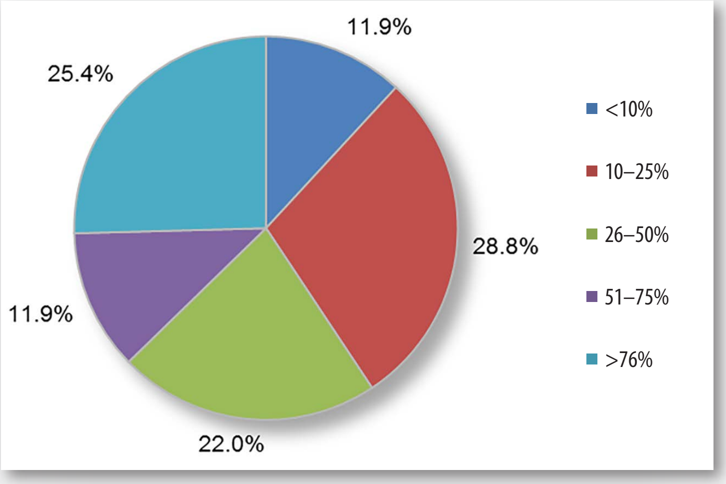

Figure 1. Security Practitioners Focus on ICS Cyber Security

Size does play some role in the amount of time staffers devote to ICS security. For the largest organizations, the highest percentage spend more than 76% of their time focused on ICS security. Respondents in moderately sized organizations chose the 10–25% timeframe most frequently. And, respondents from the smallest organizations chose the more than 76% category most frequently.

As positive as these results are for helping safeguard systems, a large number of respondents must balance their ICS security duties with a significant proportion of secondary responsibilities. Given that the field of control system cyber security is detail-oriented, complex and evolving rapidly, some specialization may be warranted.

Roles Related to Risk Management Frameworks

A risk management framework provides a means to associate relevant activities by their phases within the risk management life cycle. To understand where respondents focus their efforts, we asked them to relate their roles to the stages of a security risk framework: identify, detect, protect, respond and recover. Most (62%) are highly involved in protection activities—the ones that prevent breaches, disruption or damage from taking place, for example, ensuring patch currency, identifying and remediating vulnerabilities, and identifying and addressing misconfigurations. Almost half (48%) are highly engaged in identifying ICS security risks to understand and assess level of risk and potential impact, with nearly equal numbers working in detection (41%) and response (43%) to execute action plans. Only 30% were highly involved in recovery activities.

The narrow range of responses to our question on involvement with security incident response phases (with almost every phase having 30–48% claiming high levels of participation) suggests that those engaged in recovery are there for much of the process, which is optimal for knowledge-sharing considerations (see Figure 2).

TAKEAWAY

Protection/prevention functions receive the most attention, but we cannot overstate the importance of clearly documented and validated recovery/restoration plans, including task responsibilities and communications. These are the final bulwark against a business disaster.

For your current role, indicate your current level of involvement in the following security incident response phases as low, medium, high or not applicable.

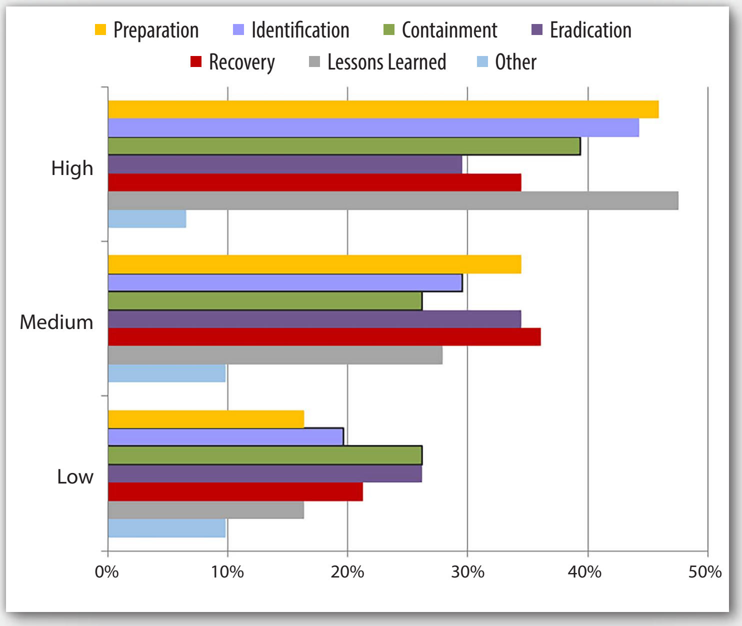

Figure 2. Incident Response Phase Involvement

Multiple disciplines, including project, process and risk management, stress the importance of engaging key stakeholders throughout this life cycle to ensure knowledge transfer and awareness of salient business and operational details, as well as to inform the lessons-learned phase and contribute to process improvement. Simply put, security incident response activities are more effective when the response team is involved across multiple phases of the process, rather than just a few.

TAKEAWAY

Security responders place the highest priority on keeping OT systems reliable and available. Their next priority is to ensure employees are safe, followed by decreasing security risks and improving security.

Business Concerns: Reliability and Availability Dominate

The single largest group of respondents (24%) continues to be primarily concerned with ensuring the reliability and availability of control systems. Overall, 52% ranked reliability and availability a top concern, as illustrated in Figure 3.

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

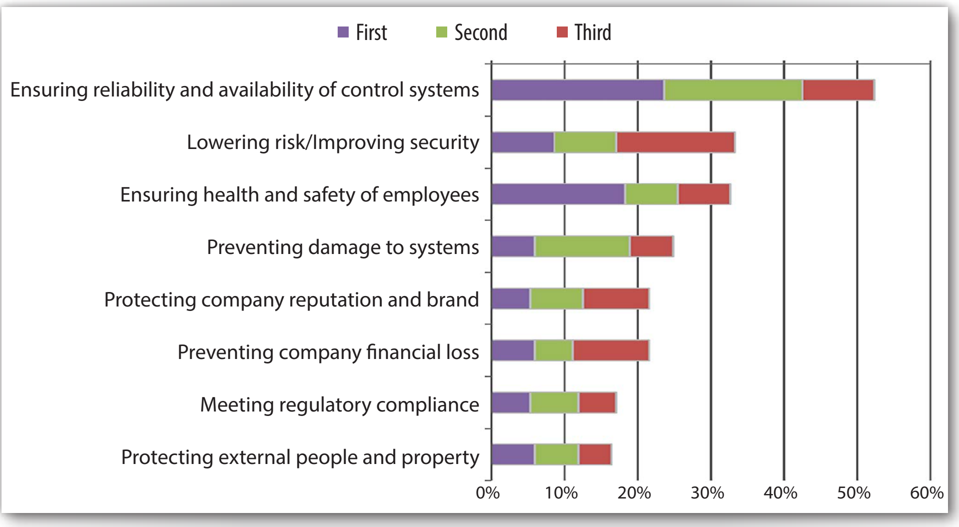

Figure 3. Top Eight Primary Business Concerns

Lowering of risk/improving security was selected as in being in the top three only slightly more frequently than ensuring the health and safety of employees. However, health and safety received the second-most marks (18%) as the No. 1 concern.

Threats and ICS Security Controls

Sources of and threats to ICS environments continue to evolve, and respondents continue to consider the risks high. As the quantity and technical details of threats have advanced, so have new types of security solutions. Innovations to address the unique challenges of ICS security include real-time asset discovery, real-time monitoring, network traffic anomaly detection or intrusion prevention systems, and others. Companies need to keep on the lookout for new technologies that make achieving ICS cyber resiliency easier or better amid an ever-shifting threat landscape.

Perceived Level of Threat

Despite greater publicity of ICS security incidents,[1, 2] the perceived level of threat to organizations rose only slightly over the past year, with 67% perceiving severe or high levels of threat in 2016 and 69% with the same evaluation in 2017. Figure 4 illustrates the change.

How serious does your organization consider the current threats to control system cyber security to be?

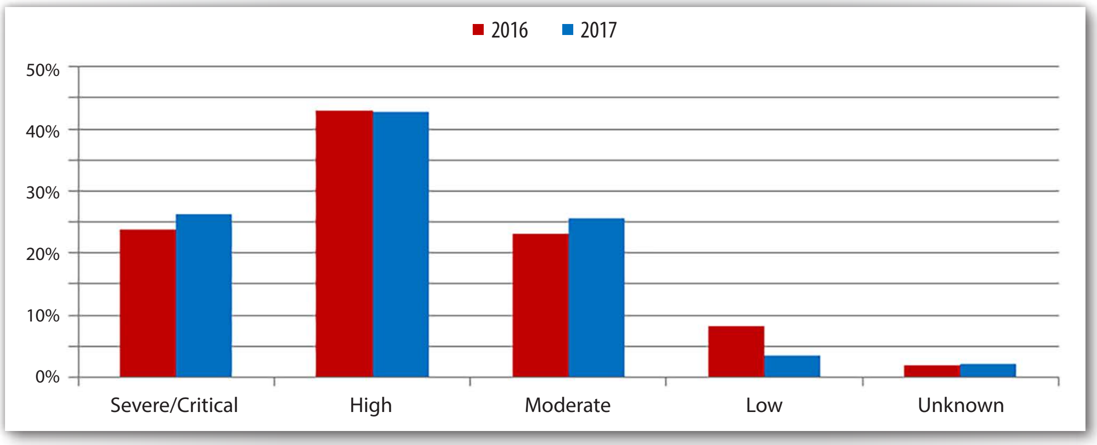

Figure 4. Perceived Threat Levels in 2016 and 2017

This suggests that responders who previously saw threats as low have changed their views. The decrease in the low responses since 2016 correlates with increases in moderate and severe/critical in 2017.

[1] www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html

[2] www.securityweek.com/critical-infrastructure-security-risks-posed-it-network-breaches

Threat Vectors

While ransomware and other external threats have news media attention, the respondents' top overall concern was for devices and "things" that cannot protect themselves, at 44%, followed by internal threats (accidental) at 43%. External threats from hacktivists or nation-states came in third at 40%. This is recognition that although external threats are a top concern (22% rank them as the top individual concern), the overall concerns are the internal threat (accidental) and the increasing presence of connected devices, many insecure by design, in and around ICS environments. This is also an indication of the movement toward what is broadly called the Industrial Internet of Things (IIoT).

It is worth noting that extortion, including ransomware, was the fourth top concern overall in 2017, at 35%, almost twice that in 2016 (18%). See Figure 5.

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

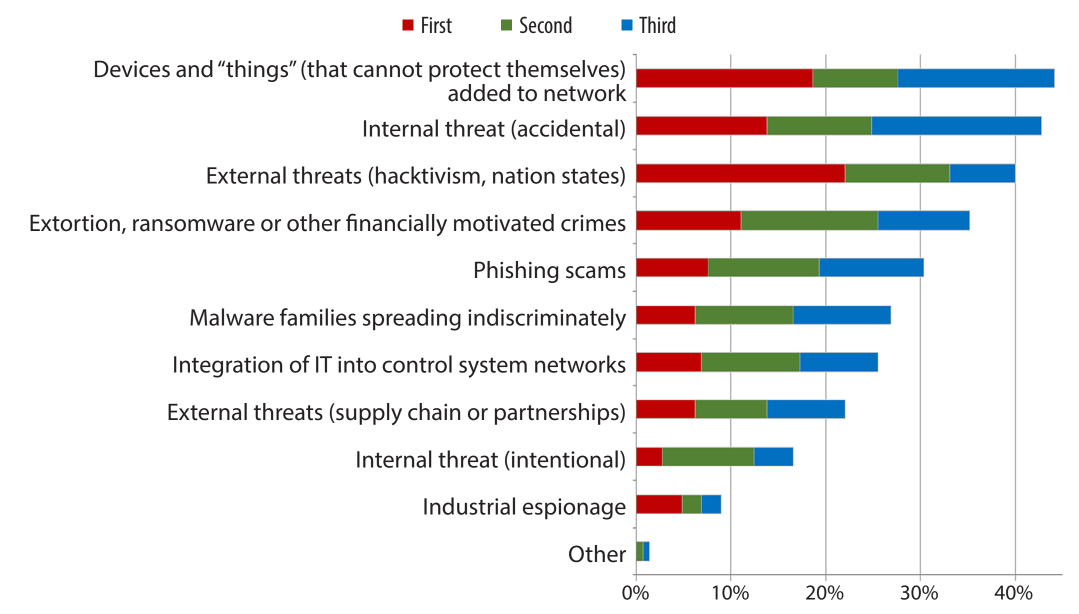

Figure 5. Top Threat Vectors

Ransomware has grown in the past two years from an occasional threat reaping fairly nominal economic payback for attackers to a sizable and lucrative industry, with estimates of greater than $1B payouts by victims annually.[3] Although ransomware primarily infects commercial OS-based systems (e.g., Windows, Linux), the integration of these into ICS environments and the dependence of ICS on devices running these operating systems has extended ransomware's effectiveness and reach. Publicly known operational impacts remain few to date[4] but, we expect more to follow, especially given public demonstrations of ransomware targeting ICS/SCADA.[5]

Network Segmentation and Traffic Monitoring

The threat from nearly every vector identified by ICS security practitioners can be reduced by detailed monitoring of ICS network traffic[6] in a manner that provides visibility into both process anomalies and security anomalies on the control network, in some cases establishing control points limiting access to different zones of your network.[7] However, integration of IT-based tools into ICS and connecting OT systems to corporate networks requires that precautions be taken to prevent the capabilities of—and intended security controls from—a single component becoming a vulnerability of the entire networked system.

TAKEAWAY

Many valid sources of guides exist that explain how to create limited-access zones, plan and implement network segmentation,[8] and safely monitor your ICS network segments for anomalous traffic.[9] Many vendors and consultants that can also provide these services. To protect your systems, we recommend you follow good security design practices complemented with relevant and proven ICS-ready security controls and maintained by security-aware, trained personnel.

[3] www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

[4] http://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml

[5] www.securityweek.com/new-scada-flaws-allow-ransomware-other-attacks

[6] https://files.sans.org/summit/ics2015/PDFs/Missing_the_Obvious_Network_Security_Monitoring_for_ICS_Rob_Caldwell_and_Chris_Sistrunk_Mandiant.pdf

[7] "Secure Architecture for Industrial Control Systems," September 2015, www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

[8] https://ics-cert.us-cert.gov/Standards-and-References

[9] https://ics.sans.org/blog/2016/03/29/collecting-serial-data-for-ics-network-security-monitoring

ICS Controls

Respondents use a variety of protective controls to secure their environments. Anti-malware/Antivirus (81%) and access controls (71%) continue to be the most common. The top 11 controls, when sorted by technologies currently in use, are illustrated in Figure 6.

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 only those that apply.***

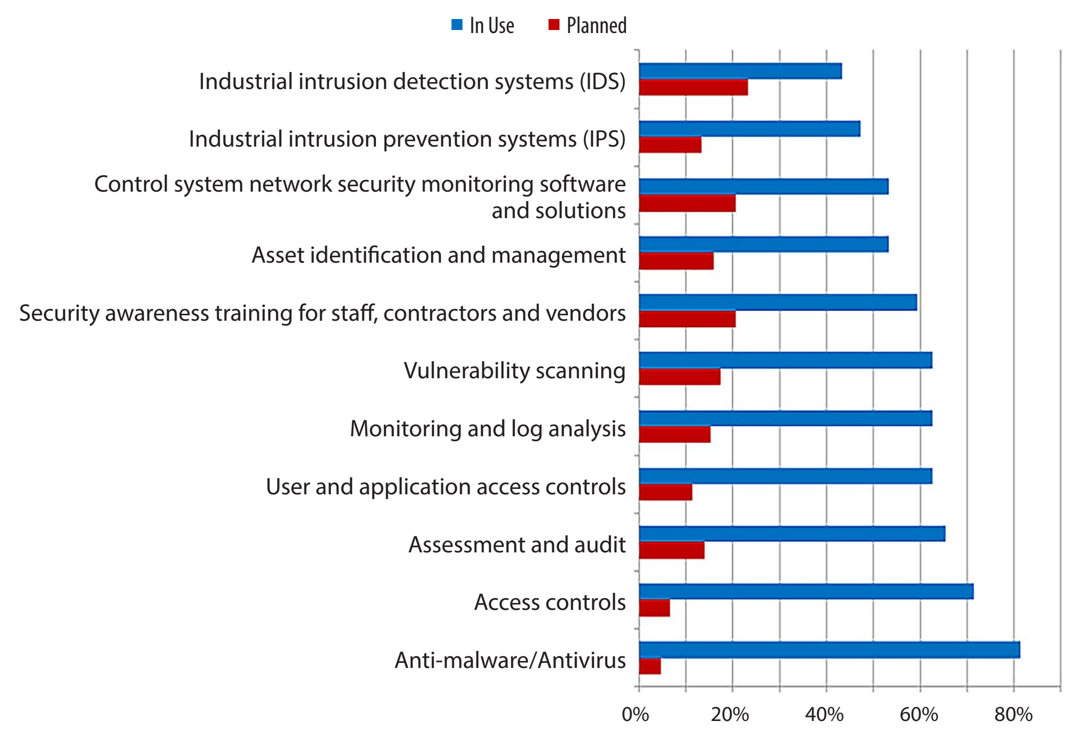

Figure 6. Top 11 Security Technologies in Use/Planned

Year-over-year analysis indicates that more organizations have implemented vulnerability scanning (63%, up from 53% in 2016), security awareness training (59%, up from 55%), and industrial intrusion prevention systems (47% up from 43%). Industrial intrusion detection systems (IIDS) are used less frequently this year, falling from 57% in 2016 to 47% this year, while communication whitelisting (not among the top 11 technologies) fell from 37% use to just 30%.

ICS/OT configuration management is the most frequently named new initiative being planned, selected by 24%. If all organizations that plan such initiatives actually follow through, this would represent a 65% growth over the 37% currently using such technology. Interestingly, industrial IDS and application whitelisting follow closely, with 23% identifying them as planned solutions.

ICS Security Budgets

IT and OT share control of ICS security budgets for 39% of respondents (OT independently controls budgets for 31%; IT independently controls 17%). Both groups provide valuable budgetary insights since vulnerabilities and attack vectors to OT originate in both IT and OT systems, and a shared budget solution engaging both areas encourages collaboration.

Organization's Control System Security Budget for FY 2017 by Size

	<1K	1K to 10K	>10K
We don't have one	9.4%	3.4%	2.6%
Less than $100,000	3.4%	2.6%	0.0%
$100,000–$499,999	6.0%	3.4%	3.4%
$500,000–$999,999	0.0%	1.7%	4.3%
$1 million–$2.49 million	0.9%	6.8%	4.3%
$2.5 million–$9.99 million	0.0%	4.3%	1.7%
Greater than $10 million	0.0%	0.9%	2.6%

Among those who provided budget information, more indicate security allocations in the $100,000–$499,999 (21%, up from 14% in 2016) and $1M–$2.49M (19%, up from 12% in 2016) ranges, with fewer budgets below $100K. As we would expect, larger organizations do report larger budgets, with significantly more organizations under 1,000 employees reporting that they have no budget.

And, 46% of respondents with funding knowledge report stable ICS security budgets and another 46% report increases. Just 8% reported decreases.

Overall, the number of respondents planning new initiatives in the near future is low which, in combination with the stable or rising ICS security budgets, suggests that planned spending allocations aim at strengthening current programs rather than investing in new technologies. The planned configuration management initiatives, however, may indicate that organizations are starting to shift their investment attention toward protecting ICS/OT proprietary cyber assets.

Where budgets are available, organizations are making security assessments/audits and gaining greater visibility into control system assets and configurations top priorities in their budgets. For a more in-depth discussion, see the "Security Assessments" section later in this paper.

Respondents' top six budgeted initiatives for the next 18 months, all cited by more than 20% of the sample, include the following:

- Perform security assessment or audit of control systems and control system networks (36%)
- Increased visibility into control system cyber assets and configurations (36%)
- Increased security awareness training for all personnel with access to control systems and control system networks (28%)
- Implement visibility and control tools for monitoring ICS devices connected to the network (27%)
- Increased training and certification of staff responsible for implementing and maintaining security of control systems and control system networks (26%)
- Implement anomaly and intrusion detection tools on control system networks (22%)

Budgets for training and certification of staff responsible for implementing and maintaining security of control systems and control fell considerably, from 34% in 2016 to 26% in 2017. Rather than balancing this with increases in trained staff or outside consultants, budgets for these initiatives decreased, dropping, at 14%, below the top 10 budgetary initiatives. At a time of increasing exposures and risk factors, this is counterintuitive. Rising threat levels and expanding attack surfaces require skilled professionals to address these risks.

ICS Assets at Risk

Recognizing that threats to ICS systems continue to increase, it is important to determine whether breaches are occurring, the frequency of such incidents, and how organizations are assessing and addressing the threats facing them. Understanding these elements provides more useful information to enhance risk management processes.

Breach History

Respondents continue to indicate that they don't think their control systems have been infected or infiltrated. The most common response, "not that we know of," was selected by 40%. Note that this doesn't necessarily mean they haven't been breached; it's just that they don't know it, or don't know it yet. Such a response isn't surprising, however, given the case studies of persistent threats that support this as the safest answer, since dwell time (the period between the onset of an infiltration and its discovery) is often counted in months.[10] Figure 7 provides a snapshot of respondents' knowledge of their breach history.

Have your control systems been infected or infiltrated in the past 12 months?

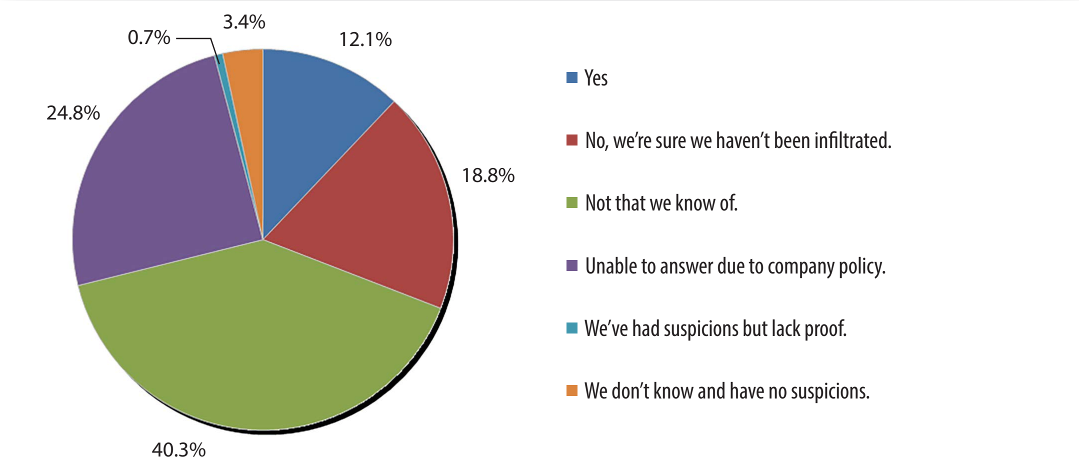

Figure 7. Infections/Infiltrations in the Past 12 Months

Unfortunately, this means that 4 out of 10 ICS security practitioners lack visibility or sufficient supporting intelligence into their ICS networks, which is one of the primary impediments to securing these systems.[11] Without full knowledge of interconnected assets, their configurations (including control logic) and the integrity of communications taking place, defenders are effectively working blindly, unable to make adequately informed decisions regarding which controls to implement, or how to prioritize security plans and spending.

[10] www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing

[11] www.securityweek.com/three-questions-every-ics-security-team-should-ask

In a positive change with this year's survey, those knowledgeable about security events grew by 10 percentage points, with those lacking information ("Unknown") decreasing from 28% in 2016 to 18% in 2017. Of those knowledgeable about security events, the number reporting one to two incidents increased by a similar amount, from 37% in 2016 to 47% in 2017. Those reporting three to five incidents also increased, from 19% in 2016 to 24% in 2017. Figure 8 illustrates the breach experiences of this year's respondents.

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

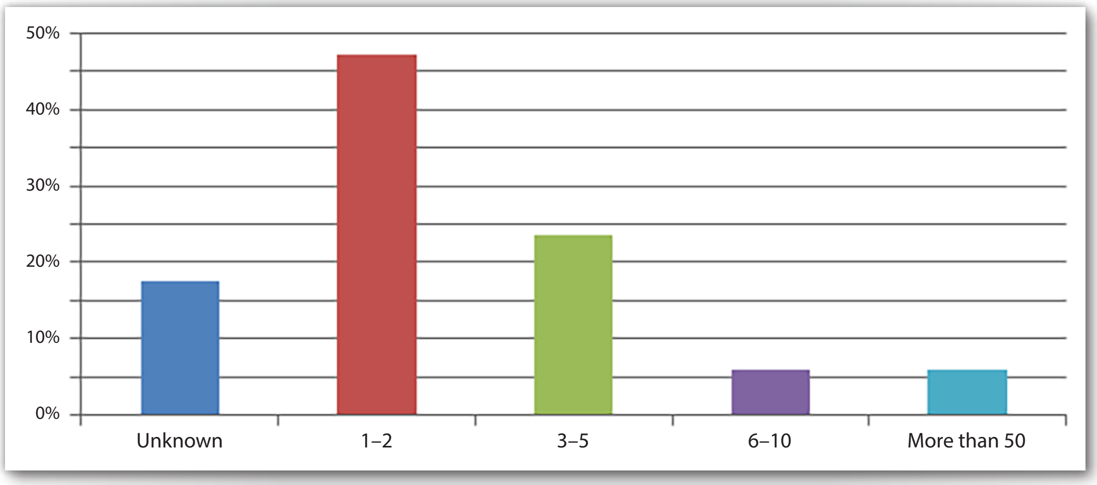

Figure 8. Infiltrations/Infections in the Past 12 Months

These results suggest that breach recognition is increasing, yet the discovery of the breach may not necessarily come early in the detection or protection phases of the risk management process.

Following on the increasing insight into security events, survey responses regarding dwell time shifted away from "unknown" toward longer dwell times before discovery than in previous years. We take this as an indication that breach intelligence is increasing and long-dwelling persistent threats are being uncovered before operational impacts reveal their presence. This reduction in those answering unknown (from 12% in 2016 to 6% in 2017) suggests incident responders and forensic teams are making headway trapping and tracking down information on when and how initial breaches had occurred. Respondents were also more frequently able to identify the sources of control system network infections/infiltrations, attributing the compromises to hackers as opposed to unintentional causes significantly more often, up from 36% in 2016 to 56% in 2017.

Detection of Infections

Companies continue to rely on internal resources (55%) more than any other source when they detect an infection or infiltration of control system environments. In light of the lack of budgeted plans to increase staffing, training or consulting, one possible interpretation is that those organizations believe their current internal resources, in concert with external resources, are sufficient to protect their systems. See Figure 9.

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

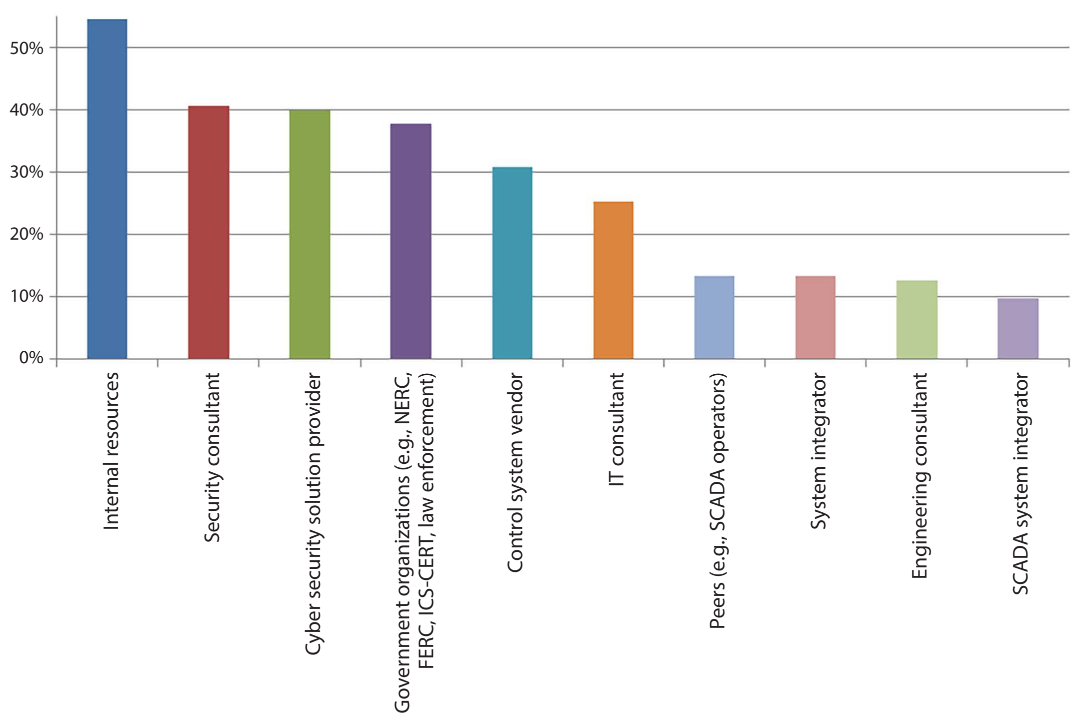

Figure 9. Contacts When an Infection or Infiltration Is Detected

Fewer respondents look to government and related organizations (38%), control system vendors (31%) or peers (13%) for aid than in the past. There, however, is an increased risk from greater reliance on internal personnel without more training of those resources. Additionally, the absence of involvement of the government or industry peers may lead to other organizations being subsequently affected, whereas shared knowledge may enable these firms to defend themselves.

Asset Data and Vulnerability

IT devices such as computer assets running commercial OSes continue to be considered most at risk (70%) and having the greatest impact (46%). We are seeing an increasing awareness that embedded controllers and control system applications are also vulnerable (see Figure 10). The well-publicized demonstrations of ICS component hacking may be contributing to the latter.[12, 13, 14]

Which control system components do you consider at greatest risk for compromise, and which would have the greatest impact if compromised and exploited?

Select your top three in each category in no particular order.

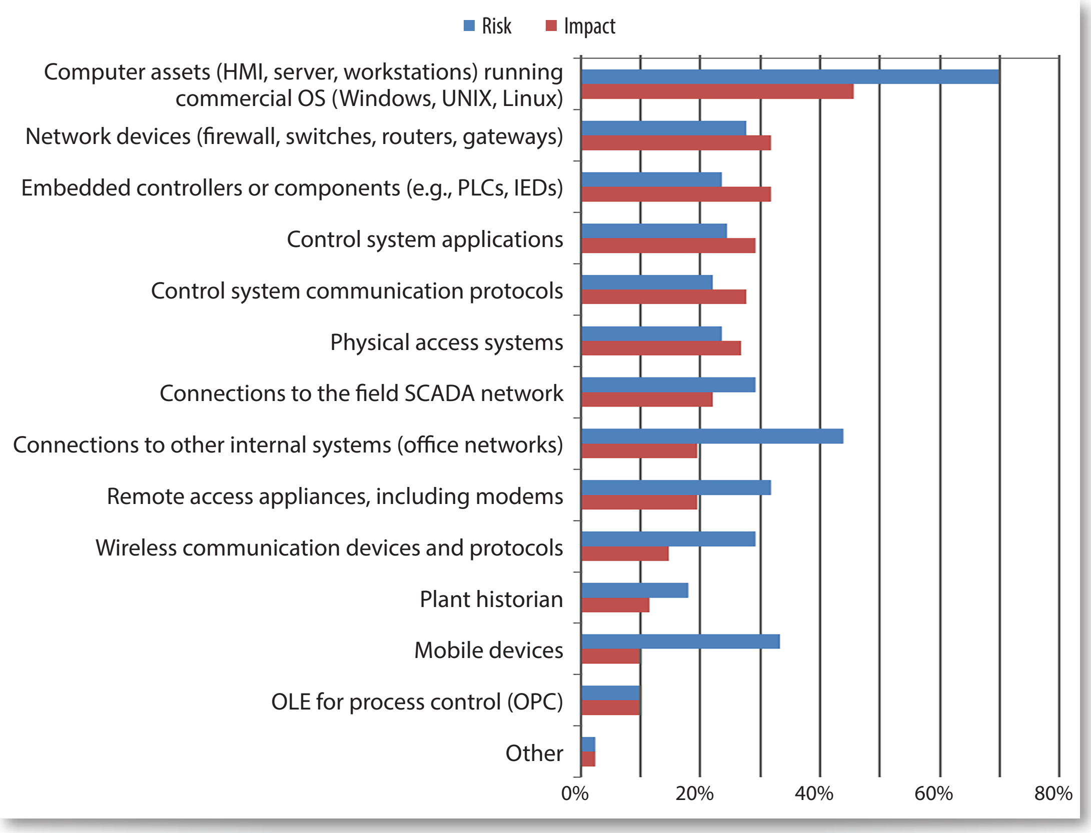

Figure 10. ICS Components at Greatest Risk

[12] http://thehackernews.com/2017/02/scary-scada-ransomware.html

[13] www.csoonline.com/article/3135244/security/workstation-software-flaw-exposes-industrial-control-systems-to-hacking.html

[14] www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

With computer assets and networking devices of greatest concern, it follows that data is most frequently collected and correlated on these components (78% and 77%, respectively). These are also the easiest components to collect data from, as they are presumably compatible with mature IT security tools. See Figure 11.

From which control system components are you collecting and correlating data?
Select all that apply.

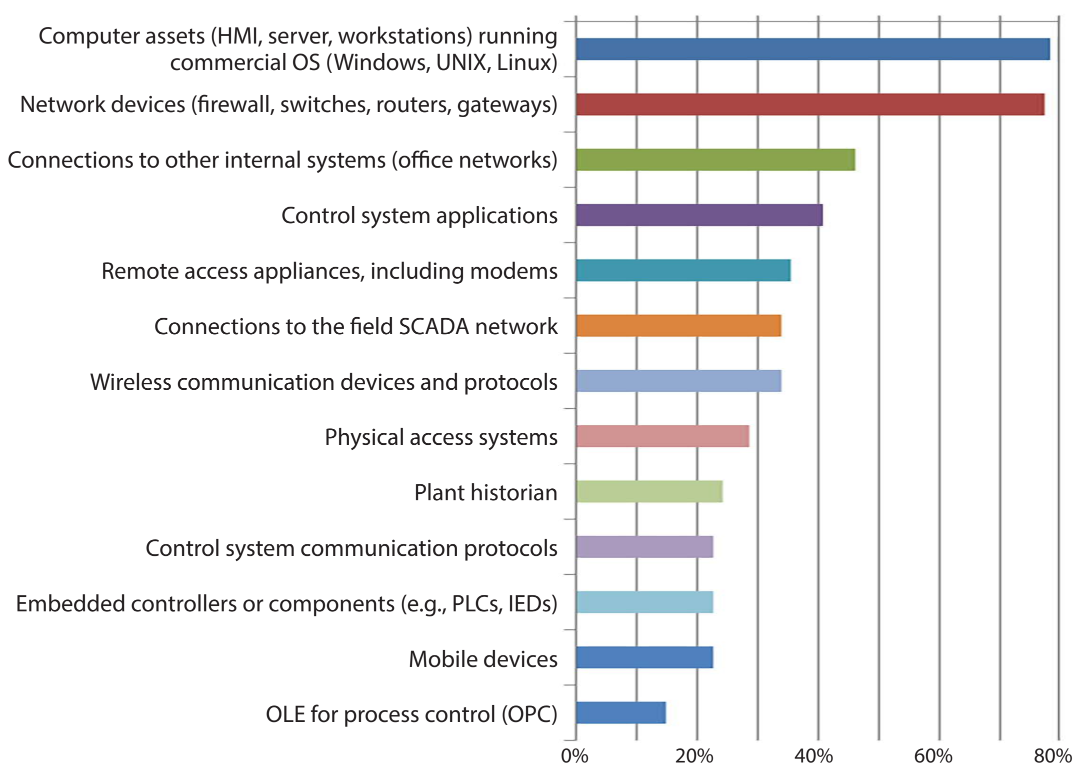

Figure 11. Data Collection from Control System Components

Only 46% of respondents gather data from connections between ICS and other internal systems such as office networks. Due to the prevalence of remote access architectures, attacks on ICS systems frequently begin with penetrations of business systems and pivot to the less-exposed, but interconnected ICS networks from there.[15]

It is also important to note that embedded controllers represent one of the highest impact systems, represented in Figure 5 on page 9 as devices and things that cannot protect themselves, yet they rank as one of the lowest in terms of data collection, at just 23%. This is a gap that organizations must look to close in the future.

[15] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, Page 6

Discussions with industry security experts routinely indicate that "as-designed" documentation of ICS environments seldom matches actual installed equipment, software and network connections. Best practices call for programmatic confirmation and improvement of asset documentation, including configuration data, such as control logic with periodic audits backed up by change management and automated discovery processes. Tracking at this level allows security personnel to detect breaches or inadvertent, unauthorized changes.

Asset Management

Taking an inventory of ICS assets is only one step in the asset management process, which itself is only one link in the system security management chain. Thanks to the development of commercially available automated asset discovery and configuration software, much of the labor involved in this effort can now be handled by software.[16] Documentation must be kept up-to-date through complementary change management processes and continual use of a passive automated discovery tool (where possible), and then verified by periodic audits/assessments. However, it is critical to carefully consider, test and validate that such discovery tools are appropriate for an ICS environment, due to the potential for disruption or damage.

Security Assessments

Regular security assessments/audits by trained and experienced security practitioners are fundamental to identifying areas of greatest risk and optimally targeting resources. Effective assessments provide:

- **Breach detection.** Analysts often find long-dwelling advanced persistent threats (APTs) only during detailed analyses of security controls, logs and configurations.
- **Network traffic analysis.** The highly deterministic nature of ICS networks enables assessment and identification of normal OT events and activities, allowing detection of anomalous and potentially disruptive or damaging communications.
- **Asset and network inventory.** Audits should validate the accuracy of asset and network documentation, including configuration data, while also identifying potential risks with rogue devices that should not be connected to the ICS.
- **Vulnerability identification and evaluation.** Assessments confirm the presence of vulnerabilities discovered by internal and external parties, evaluate the accompanying risks and recommend responsive actions, such as patching, reconfiguration, and replacement or addition of compensating controls.
- **Risk remediation action plans.** Assessments include recommended actions to address identified risks and evaluate whether the recommendations of earlier assessments have been completed.

[16] www.securityweek.com/role-asset-management-ics-network

TAKEAWAY

While we recommend that organizations able to support the skilled staff required to carry out a quality assessment do so, it is also important to have external teams analyze your environments periodically. This both allows access to personnel with greater experience and training without the related staffing costs and ensures that a second and neutral set of eyes does the evaluations.

Encouragingly, 33% of respondents' organizations had performed security assessments of their control systems/networks in the three months prior to the survey, up from 26% in 2016. As recommended last year,[17] some level of security assessment should be performed no less than quarterly, and full audits at least annually. For the 12% that have never performed a security assessment, we urge action to mirror the growing trends of their industry peers. See Figure 12.

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

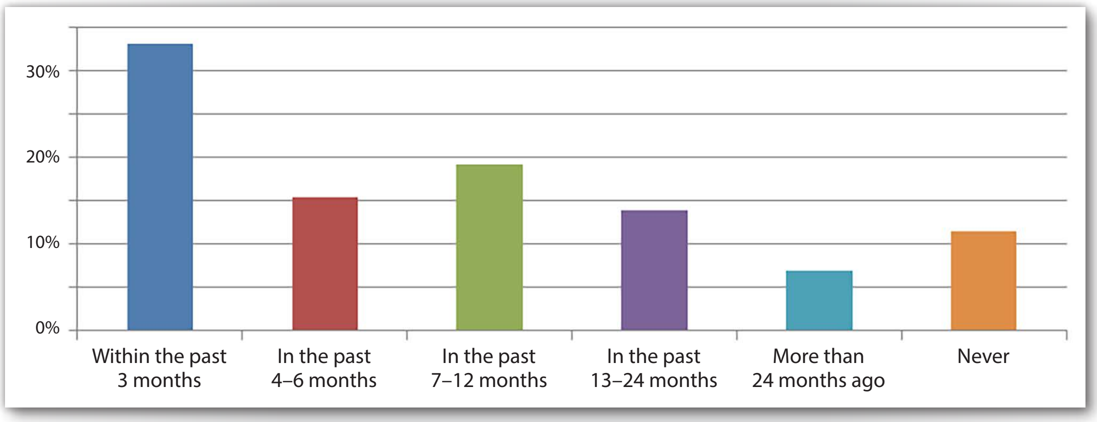

Figure 12. Frequency of ICS Security Assessments

Consistent with previous surveys, the largest group of respondents (45%) relied on internal resources to perform their most recent security assessment, with 22% using large consulting firms and 19% boutique consultancies.

[17] "SANS 2016 State of ICS Security Survey," June 2016, www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067

Patch Management

Only 46% of respondents regularly apply vendor-validated patches, and 23% batch process patches during scheduled downtime. Some (11%) layer additional compensating controls instead of patching, and 12% neither patch nor layer controls around critical control system assets. Figure 13 illustrates the ways organizations handle this important process.

How are patches and updates handled on your critical control system assets?
Select the most applicable method.

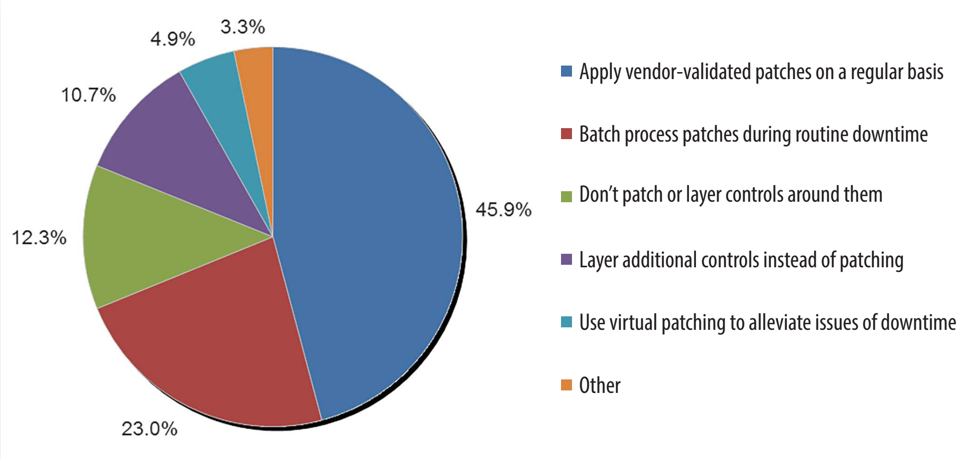

Figure 13. Patching Practices

Whether the root of the patching problem is technical (e.g., uptime requirements, uncertain asset compatibility, concerns about voiding manufacturer warranties), resources (e.g., insufficient staff) or a combination of factors, unpatched systems without carefully applied technical and nontechnical security controls are huge operational risks. With 12% not patching or layering controls and another 11% just layering controls instead of patching, organizations are facing a perfect storm of compromise. Growing lists of known vulnerabilities in control systems and of tools allowing even the unskilled to exploit those vulnerabilities make compromise of unprotected critical assets inevitable.

Patching security vulnerabilities and communication channels known to be exploited by ransomware and other malware is highly effective at mitigating risks when the patching actually takes place. However, the cadence and capability for rapidly patching business systems will likely always far exceed the speed at which ICS environments can and will be patched, if the ICS systems are patched at all. The result is that ransomware risks to ICS are more likely to linger well after patches and risk mitigation solutions are applied in IT. This weakness applies to other threats as well, and often accounts for why ICS systems still fall prey to very old, well-understood malware.

TAKEAWAY

We strongly recommend establishing a fully-staffed, closed-loop program to manage testing and implementation of patches and, where patching is not feasible, to design and implement additional compensating controls, such as machine authentication and authorization, microsegmentation, strong encryption and machine whitelisting, to minimize infection risks of ICS assets. A good resource to start with is the CIS Critical Security Controls.[18]

[18] www.cisecurity.org [Registration required]

Vulnerability Management

Respondents continue to primarily look to product and system vendors (53%) and CERT (49%) to inform them of ICS vulnerabilities. It is encouraging to note that many use multiple methods. However, risks identified by alerts and advisories must be considered by asset owners in the context of their systems. Many ICS solutions are customized to unique settings and collections of components from multiple vendors. We support monitoring all reliable information sources in this area, but we also strongly encourage each organization to work toward greater insight into its own ICS environment, particularly through ongoing network assessments, network monitoring and analysis for anomalies in access and operations. Figure 14 provides a look at the many avenues available to detect vulnerabilities.

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

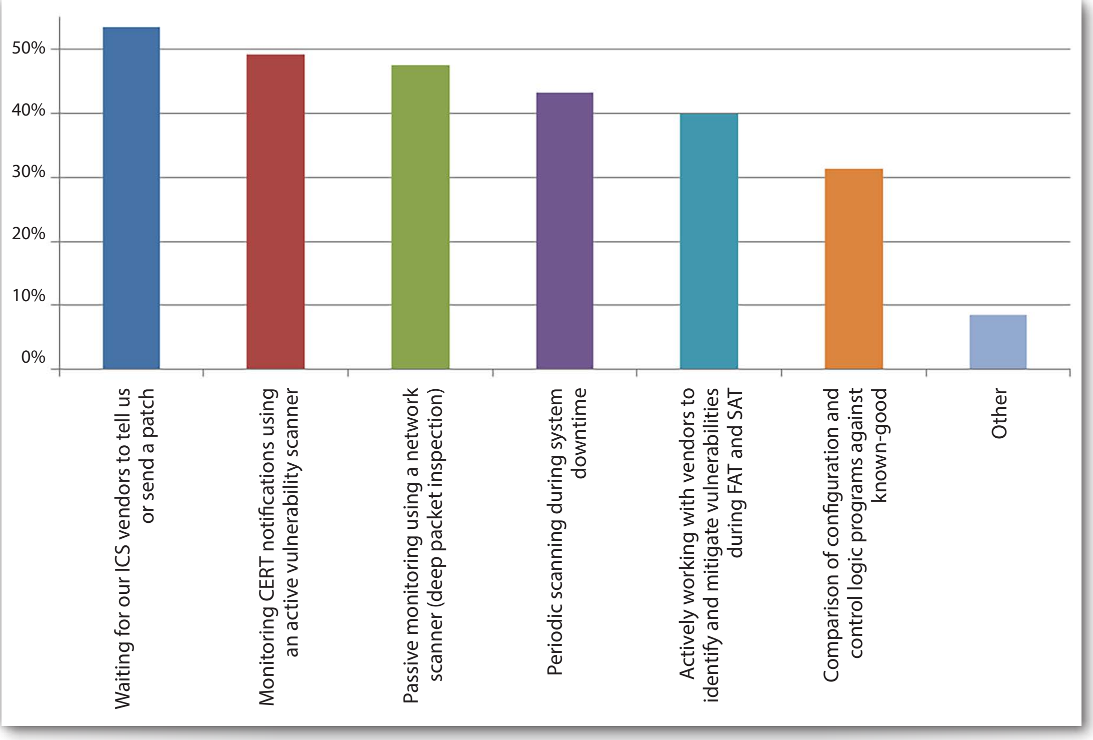

Figure 14. ICS Network Vulnerability Detection

Making use of threat intelligence is another way organizations can improve their ability to mitigate or prevent successful attacks on known vulnerabilities, targeted attacks or nontargeted campaigns affecting a broader community. Figure 15 illustrates where that threat intelligence often comes from.

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

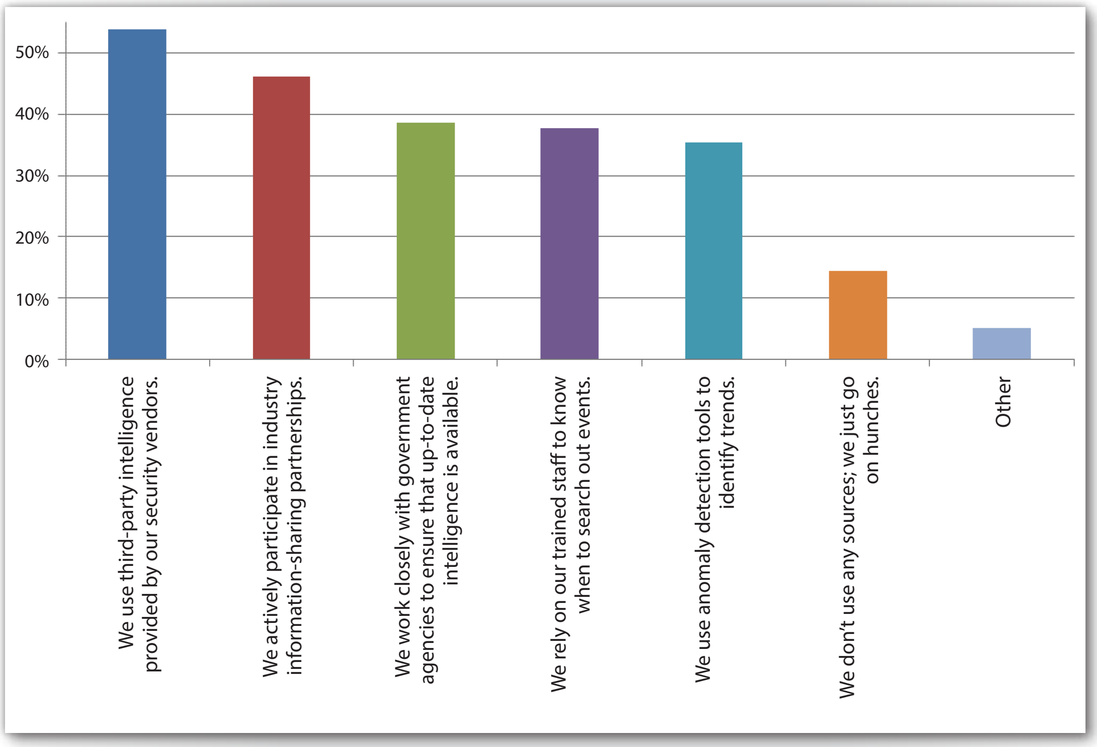

Figure 15. Intelligence Sources

More companies are using third-party intelligence from their security vendors (54%, up from 43% in 2016). This correlates with a drop in those relying on internal trained staff (down to 38% in 2017 from 54% in 2016). Decreased reliance on in-house staff may result from the tremendous shortage of adequately skilled and experienced resources in this area, a well-documented phenomenon. Analyzing responses by employee count also showed that companies in the 1,000–10,000 range are more likely than those smaller or larger to use third-party intelligence from their vendors, work closely with government agencies, and participate in industry information-sharing partnerships.

TAKEAWAY

Integration of the security function into procurement is absolutely necessary to manage the risks of introducing new assets. High capital costs and 10- to 20-year life cycles mean that today's ICS purchases remain in place for decades, and operating considerations may make modifications impossible. Qualifying security before acquisition is not only the least expensive option, it is often the only option. Because many ICS vendors lack qualification or interoperability/validation programs, they rely on standards such as NIST CSF and others mentioned later in this paper.

Another important source of risk mitigation and enhanced protection is making careful purchasing choices. Fewer participants (12%, down from 21% in 2016) mandated ICS equipment vendors to qualify security technologies/solutions. Figure 16 demonstrates that 55% find qualification highly important or mandatory.

How important is it to your organization for security technologies or solutions to be qualified by your ICS equipment vendors?

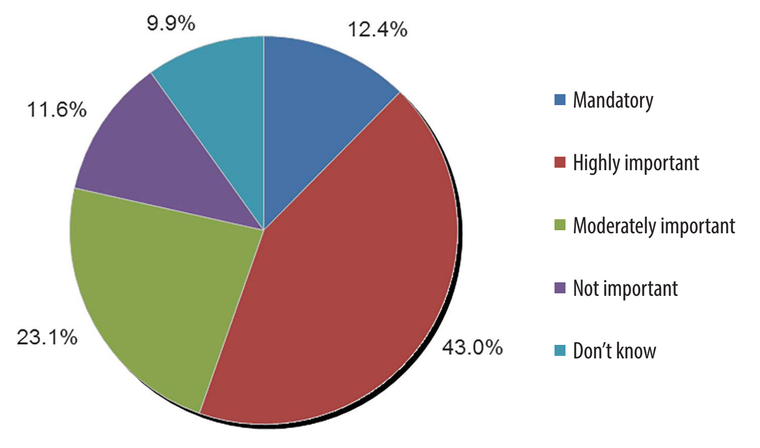

Figure 16. Importance of Technology Qualification by ICS Vendors

Security Policies, Standards and Controls

Security policies are only as powerful and enforceable as the governing processes and authority that direct them. Policies lay out a company's objectives, and organizations can measure progress toward those goals. Internal and industry standards can effectively expand on policies to define the specifics of security roles, tasks and responsibilities, dictating the risk management controls to be implemented.

ICS Security Responsibility

Although many different fiduciary roles at a senior level in a firm could set policy, 38% of respondents say the chief information security officer continues to be the role responsible for setting control system security policy, followed by the chief security officer, at 11%. Many respondents (19%) chose "Other," and many of them named a position below the executive level, which may reduce policy effectiveness. Interestingly, there seems to be little difference in who sets policy based on size, other than that fewer respondents from large organizations indicated that they didn't know who set the policy. See Figure 17.

TAKEAWAY

Organizational behaviors and overall security culture are driven from the top down. For security standards or guidelines to be enforceable, expectations and accompanying governance programs should also be set at the highest level.

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

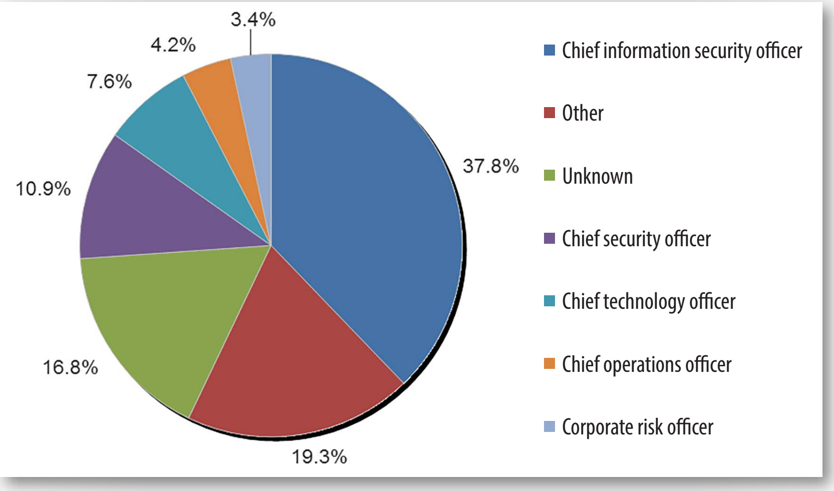

Figure 17. ICS Security Policy Authority

Organizations are largely resistant to change. Objectives and directives process downward through chains of command, defining performance goals and duties. The authority of C-level officers is generally recognized throughout an enterprise, but the same is not true for positions further down the ladder. As such, a widely accepted premise is that security leadership at the top of an organization leads to a stronger, more meaningful security culture throughout the organization.

What Standards?

The largest portion of respondents (48%) continue to map their cyber security standards to the NIST Cyber Security Framework (CSF) more formally known as the Guide to SCADA and Industrial Control Systems Security. Fewer (23%) adhere to NERC CIP, possibly due to the multiple version changes in the past year, but also reflective of the NERC-CIP standard being specific to the NERC Bulk Electric System. See Figure 18.

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

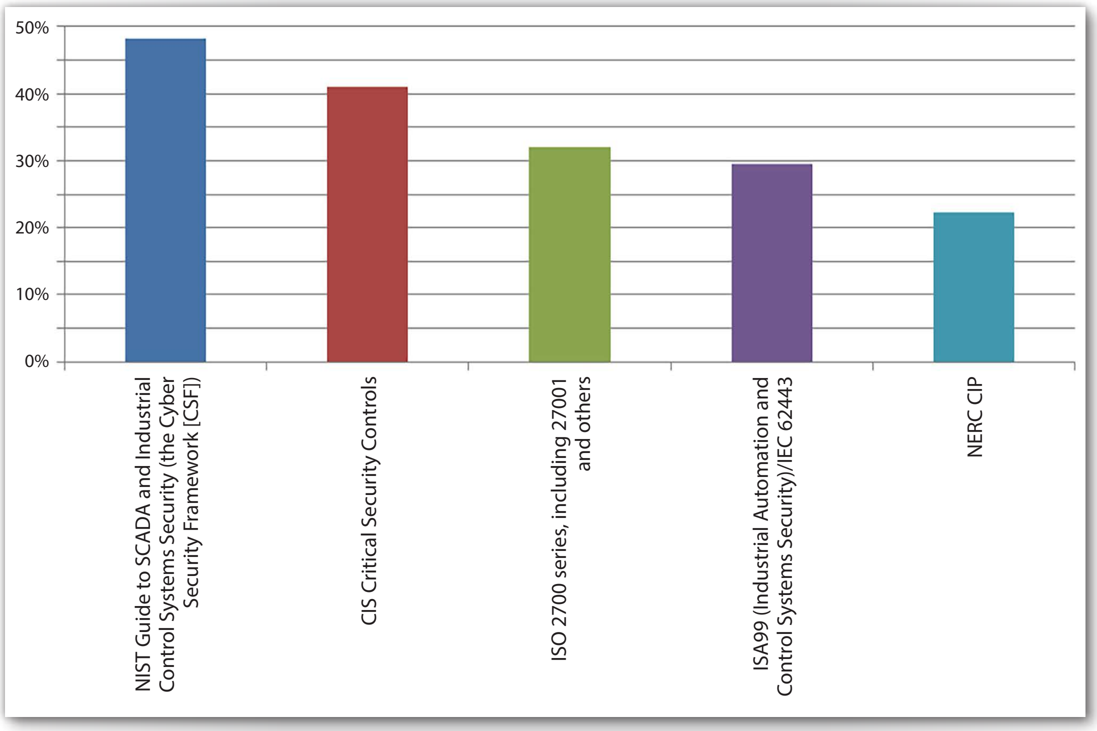

Figure 18. Mapping to the Top 5 ICS Security Standards

Although we do see more participants mapping to international standards, such as ISA/IEC 62443 and guidelines such as the ENISA Guide to Protecting ICS, which garnered support by 30% and 13%, respectively, these relatively lower numbers may be related to the demographics of our sample, which is predominantly North American, with 66% headquartered in North America and respondents providing strong evidence of organizations operating in multiple geographic areas. Regardless of the standard or guideline each organization chooses to follow, it is important that it guide the implementation of the ICS security controls.

Control Implementation Responsibility

Owner/operators of controls systems (59%) are in charge of implementing control system security controls, followed by engineering managers (43%).

It is clear, however, that numerous parties take part in this endeavor, as illustrated in Figure 19.

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

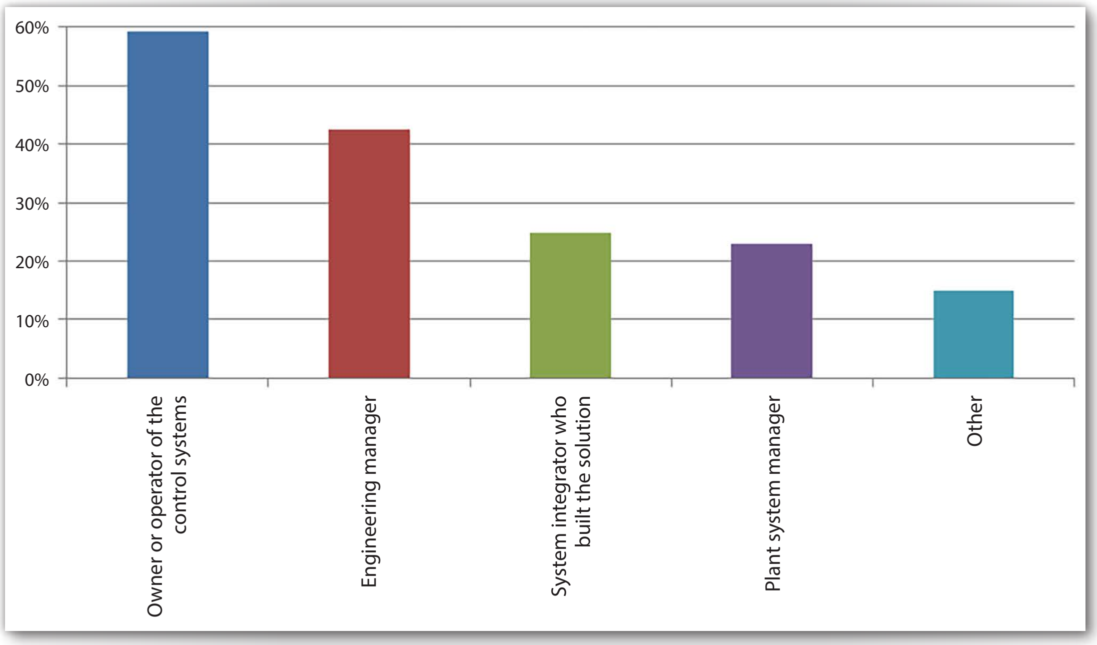

Figure 19. ICS Security Control Implementation Responsibility

Policies and Procurement Processes

Ensuring the security of new ICS assets and network devices is essential to the entire enterprise. Securing current assets is challenge enough. Yet only 34% of respondents have clear and reasonable requirements to consider cyber security in their procurement processes. Another 30% (grouping "Hopefully," "Not Really" and "No) do not even consider security (see Figure 20).

TAKEAWAY

Make use of the freely available resources on how to establish procurement security requirements and use them as you seek new or upgraded equipment and controls.[19]

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

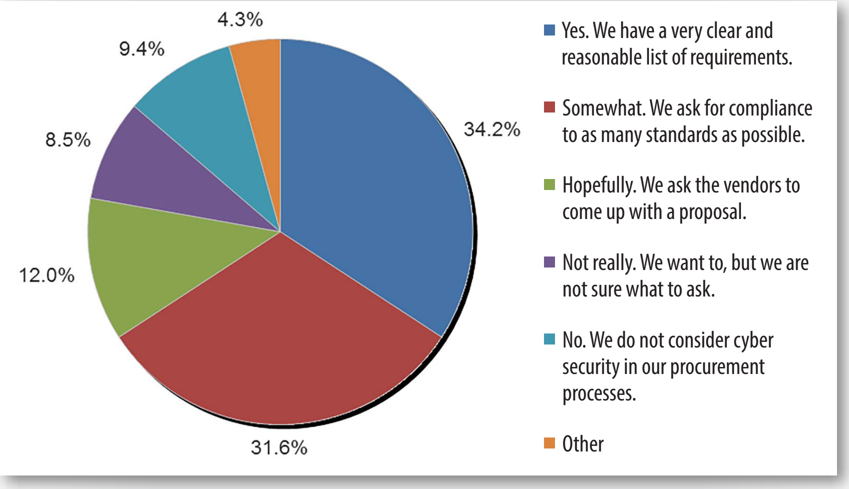

Figure 20. ICS Procurement Security Requirements

This combined 30% who lack concern for security during procurement is troubling, particularly because the lack of procurement processes is consistent across all sizes of companies. The risks of deploying systems without evaluating their security cannot be overstated.

[19] https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

The increasing connectivity and integration of traditional IT systems into ICS environments, often termed *IT/OT convergence*, brings large business benefits but also introduces risks that both IT and ICS personnel are often unaware of and unprepared to address. Where physical proximity was historically required to access ICS assets, these systems are increasingly accessible remotely.[20] Further, more devices within ICS environments run commercial operating systems than ever before, exposing the organizations to widespread vulnerabilities. These risks are compounded when systems are not maintained, such as by not having or not following a disciplined patch-management program.

Convergence Strategy?

Organizations must have a security strategy to address the risks that arise from this convergence. Fortunately, 38% indicate they have a strategy for implementation, and another 31% are developing one. The 18% of organizations that lack both strategy and plans for developing one put themselves at unconscionable risk. For those firms to proceed in such a way when there are many examples and guides widely and openly available[21] is baffling and arguably indefensible, especially given that nearly 82% of industry peers indicate they are following or developing some form of security strategy.

Very positively, most participants consider IT-OT collaboration to be moderate or better (67%), and 74% perceive increasing collaboration. Few individuals or business units have all the knowledge and skill sets needed to secure increasingly integrated environments. The interdependence of the technologies and connections requires working across organizational and cultural boundaries.

Respondents stressed two impediments to advancing IT and ICS technology integration. Figure 21 identifies hurdles organizations must overcome.

What are the biggest challenges your organization faces in integrating IT and ICS technologies?

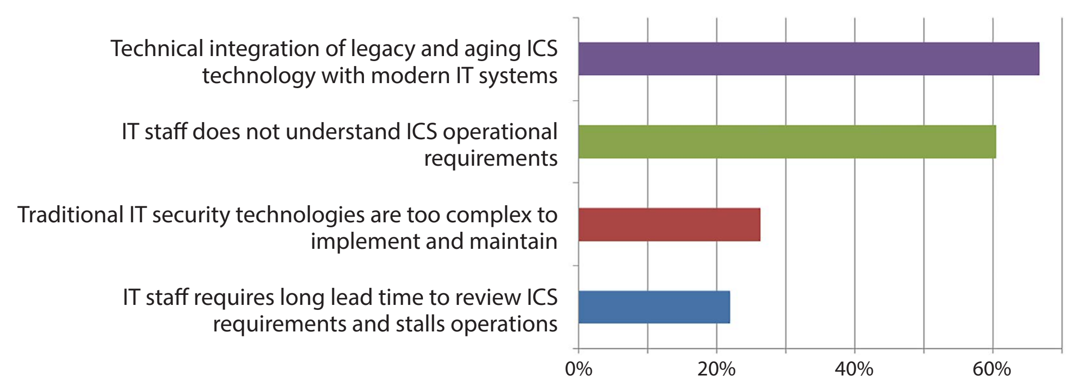

Figure 21. IT/ICS Integration Challenges

[20] www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014

[21] https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

TAKEAWAY

Implement a joint ongoing training program to increase each group's understanding of the other's requirements, approaches and considerations. NIST SP800-82r2 includes a section on how to do this. Consider reorganizing to bring IT and OT resources onto the same teams to support more balanced decisions and actions and to cross-pollinate skills. Successful collaboration between the two groups may require more cultural comprehension than technical learning, and the former is arguably harder to achieve.[22]

Lack of IT staff understanding of ICS operational requirements, chosen by 61%, is also a common sentiment among those with ICS backgrounds. And, IT staff charged with improving ICS security often make comparable statements, saying that ICS staff don't understand security risks or requirements.

To some degree, both groups are correct. Their backgrounds, priorities and training are unlikely to foster understanding of the other's roles and responsibilities, and developing a workforce that can successfully bridge this divide is one of the greatest challenges to improving ICS security. Tools and technologies are developing to help address the issues that can be dealt with in that way, but the human aspect of the equation is advancing more slowly. This pace can be accelerated through more focused training, especially where it bridges IT and OT boundaries.

One ICS organization has begun embedding an IT person in the OT operations team and an OT person in the IT team for six months to a year. Interestingly, the employees receive their reviews from the new manager they are working for. Management has found that the process improves understanding and communication between the groups.

[22] NIST Special Publication 800-82 Revision 2, "Guide to Industrial Control Systems (ICS) Security," http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Conclusions

Many organizations have not yet fully adapted to their changing technological realities. The implications of increased use of smart devices and ubiquitous connectivity are tremendous and far-reaching. They require a comprehensive strategy, informed by business, operations and security practitioners, with policies supported by top leadership. That strategy must guide companies through benefit realization without risking the entire enterprise. For many, these policies already call for increased budgets for staff, tools and training. For all, they should expand (or initiate) programs enabling cross-functional collaboration between IT and OT.

This age of expanding connectivity linking IT and OT with digital and cyber-physical systems means that there is no longer a singular perimeter. With malware capable of self-propagation among devices and malefactors surreptitiously traversing our networks, having gained entry through email phishing or exploiting unpatched vulnerabilities, it is clear that the media and channels across which our devices communicate need to be secured, safeguarded, monitored and maintained. ICS environments must be:

- Supported by educated, informed, well-equipped personnel that grow their skill sets over time
- Protected by network segregation and segmentation to establish multiple control points
- Architected on the assumption that any given part of the whole might be compromised at any time
- Able to allow traffic only as required for operations
- Monitored in real time for process and security anomalies to enhance visibility and improve asset control

However we measure things, the security risks to ICS are rising. The integration of IT with OT—and all this implies about remote access to once-isolated assets and systems—is moving forward and will continue for the foreseeable future. Undeniably, the amount of malicious activity (external threats) that is affecting vital, mission-critical systems, whether targeted or nontargeted, is growing annually, as are the tools and knowledge allowing malefactors to carry out their attacks. Internal threats and protecting devices and "things" are top overall concerns. Those dependent upon ICS systems, and those responsible for them, have clear and strong incentives to continuously focus on reducing risk to provide safe, reliable operations of systems that support business objectives to meet the wants and needs of society.

About the Authoring Team

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 more than 20 years of experience to bear in his writings about the management of IT and infrastructure projects, enterprise security governance, IT and ICS security risk analysis, regulatory compliance and policy conformance for high-profile companies. Bengt has managed multiple patents from ideation through issuance and has authored works for numerous corporate entities.

Doug Wylie (advisor) directs the SANS Industrials and Infrastructure business portfolio, helping companies fulfill business objectives to manage security risks and develop a more security-effective workforce. His career spans more than 22 years. He served as Rockwell Automation's director of product security risk management, where he established and led its industrial cyber security program. Doug works around the world with companies, industry groups, standards bodies and government entities to establish safer, more secure and reliable control solutions that integrate with business operations. He holds the CISSP certification and numerous patents, as well as being an accomplished writer, speaker and presenter.

Sponsors

SANS would like to thank this survey's sponsors:

GREATBAY SOFTWARE

NOZOMI NETWORKS

PAS®

TEMPERED™ NETWORKS

tripwire®

Special thanks to the ARC Advisory Group

ARC Advisory Group

Last Updated: February 19th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	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 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 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 Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 29, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Riyadh February 2019	OnlineSA	Feb 23, 2019 - Feb 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced