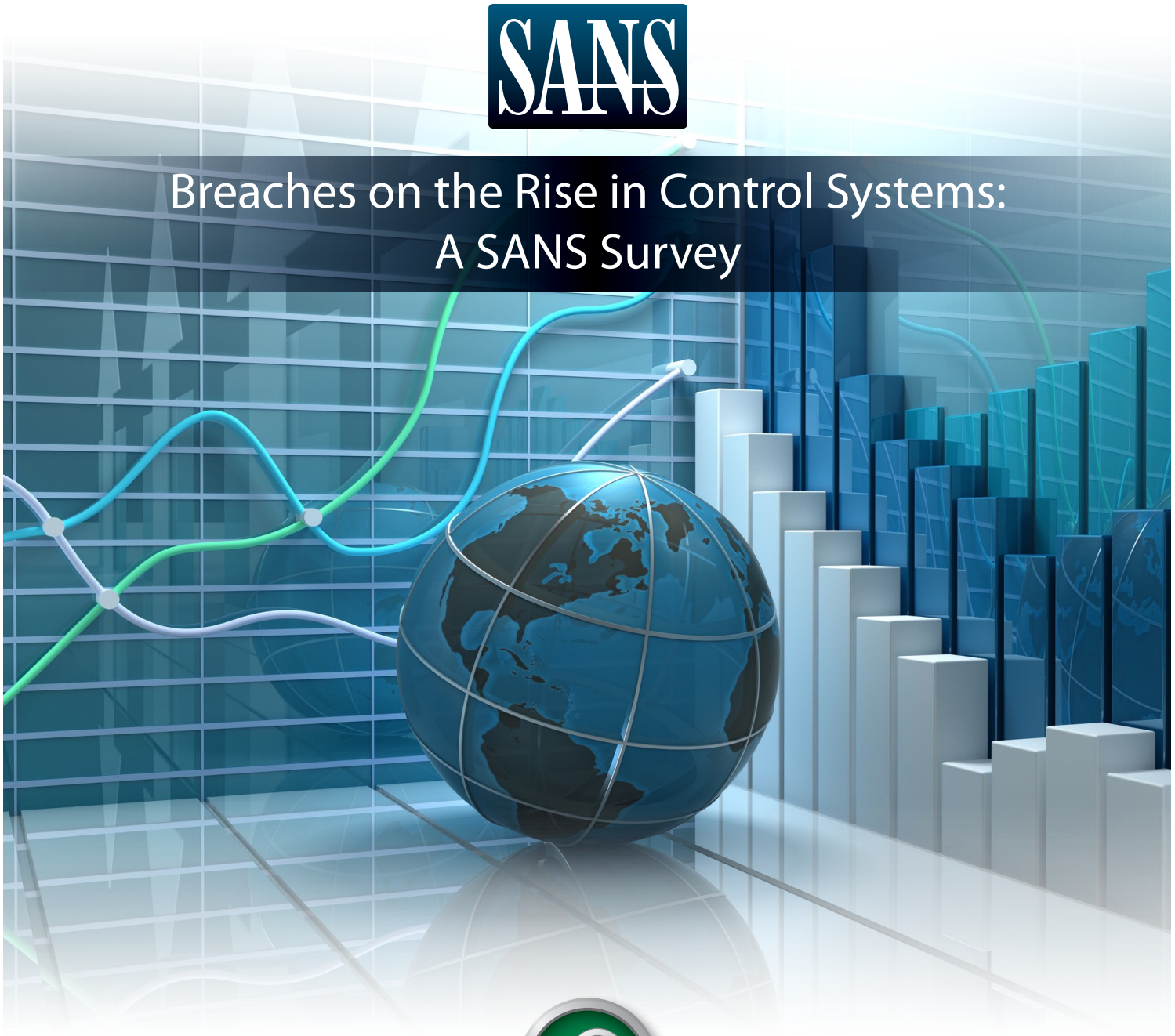


Breaches on the Rise in Control Systems: A SANS Survey

A SANS Analyst Survey

Written by Matthew Luallen
Advisor: Derek Harp

April 2014

Sponsored by
Qualys, Raytheon, Sourcefire and Tenable Network Security

Introduction

Industrial Control Systems (ICS), often referred to as Supervisory Control and Data Acquisition (SCADA) systems, monitor and control large industrial and infrastructure processes. Attacks against these systems, particularly energy-generation systems, are increasing and becoming more targeted against specific systems while also increasing in number.[1]

SANS began examining this trend of attacks against SCADA and other control systems, publishing its first survey on SCADA and ICS security in June 2013.[2] Results showed that respondents were having difficulty securing their control system environments and were beginning to experience breaches. Since then, the number of entities with identified or suspected security breaches increased from 28% in our 2013 survey to nearly 40%, based on this year's survey findings.

Taken online by 268 respondents, this nonscientific survey also indicates organizations are experiencing increased levels of concern over public safety and difficulties with visibility into their environments, including their vulnerabilities. It also points to the emergence of a new job definition that could bridge ICS and IT security roles.

These and more results will be discussed in further detail in the following pages.

Key Findings

- The number of entities with identified or suspected security breaches increased to nearly 40% from 28% in our 2013 survey. Only 9% say with surety that they haven't been breached.
- Respondents said the means to protect these systems has not improved, while the difficulty of detecting attacks and threats has not decreased.
- Many organizations do not or cannot collect data from some of the most critical SCADA and ICS assets, and many depend on trained staff, not tools, to detect issues. Almost 17% have no process in place to detect vulnerabilities.
- Embedded controllers, control system applications, object linking and embedding for process control (OPC) servers and historians are vulnerable, are being targeted and are not being protected.
- Respondents indicated widespread interest in protecting public safety; increasing leadership risk awareness; and expanding controls pertaining to asset identification, communication channels and centralized monitoring.
- Respondents noted interest in protecting a wide variety of assets, including computer systems (77%), network devices (56%), embedded controllers (53%), control system communication protocols (40%) and physical access systems (36%), among a long list.
- Respondents are facing an increasing number of international, regional or country-specific standards and regulations that will impact security handling and reporting.

[1] www.scmagazine.com//dhs-notes-rise-in-brute-force-attacks-against-natural-gas-companies/article/301339

[2] www.sans.org/reading-room/analysts-program/sans-survey-scada-2013

Survey Participants

Of the 268 survey respondents, more than 67% actively maintain, operate or provide consulting services within facilities maintaining industrial control systems, with most of the remaining ("Other" category) providing educational, legal and government services to this industry. The energy/utilities (23%) and oil and gas (11%) industries accounted for the largest number of participants. See Figure 1 for a complete industry breakdown.

What is your organization's primary industry?

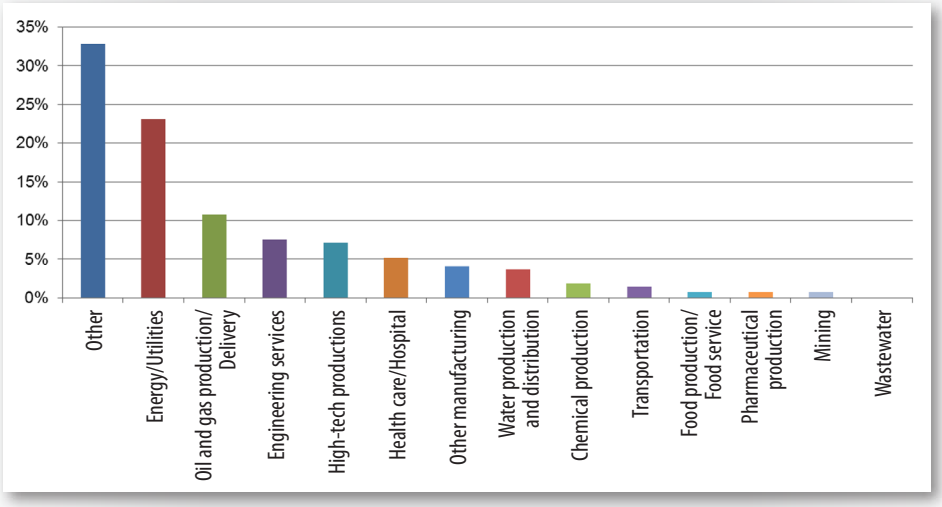


Figure 1. Survey Participants' Primary Industries

Percentage of respondents with more than 15,000 employees, contractors or consultants

Nearly 64% of the survey participants work in businesses with more than 1,000 employees, and 30% of the participants operate in businesses with more than 15,000 personnel, as illustrated in Figure 2.

How many people work at your company, either as employees, contractors or consultants?

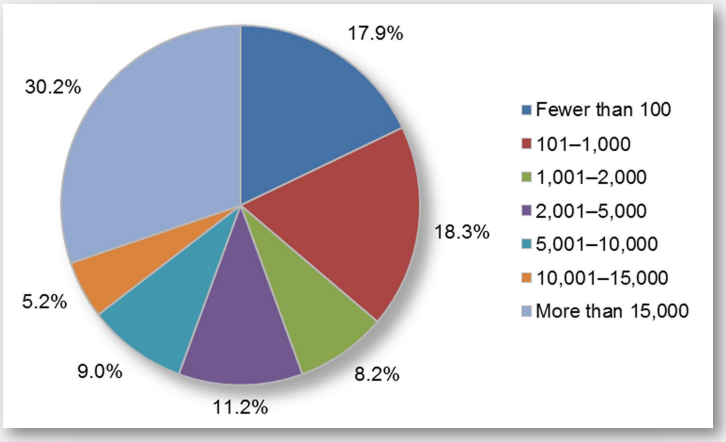
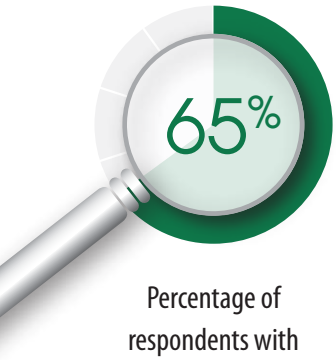


Figure 2. Organization Size



Percentage of respondents with facilities outside of the United States

The size of organization demographic is very similar to the 2013 survey results. This parity portrays that the industrialized processes of the modern world are typically provided by larger businesses. For example, 12 of top 20 businesses in the world operate in the energy sector using massive control systems for their energy harvesting and delivery systems.[3]

International Scope

Although the majority (84%) of the survey respondents have facilities in the United States, the participant base includes those whose employers have facilities in other regions of the world (see Figure 3).

In which countries or regions are control system operations for your organization located? Select all that apply.

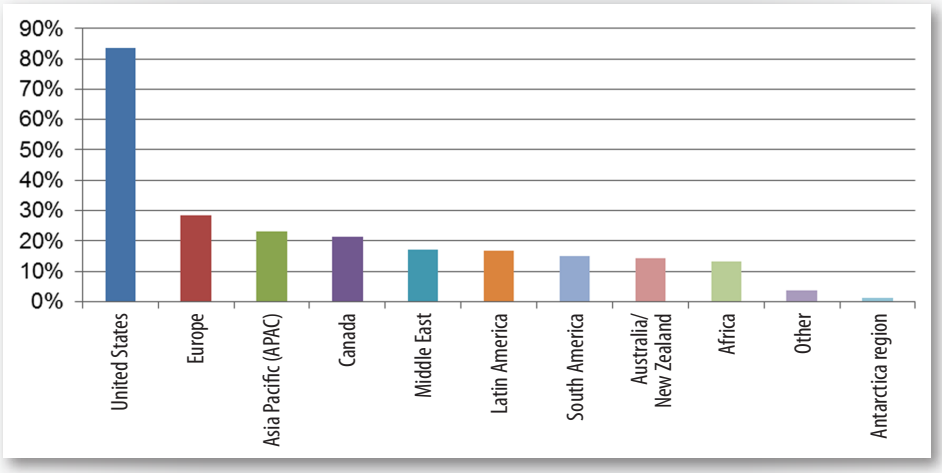


Figure 3. Worldwide Allocation of Control System Operations

The concerns and issues are the same, regardless of where the critical infrastructure is located.

As demonstrated in the survey, the concerns and issues are the same, regardless of where the critical infrastructure is located. Interest in and focus on SCADA and ICS security is likely to escalate dramatically as regional governments begin to adopt specific measures to protect their critical infrastructures and industrial control systems from cyberthreats. It's also likely that international facilities will increasingly be targeted for financial, geopolitical or other advantages.

[3] http://en.wikipedia.org/wiki/List_of_largest_companies_by_revenue

Security Titles Dominate

The roles of survey respondents were, as expected, dominated by security administration (31%), security management (14%) and network operations (12%). The "Other" category, accounting for 18% overall, actually broke down into a series of titles including educator, advisor, SCADA engineer and architect (see Figure 4).

What is your primary role in the organization?

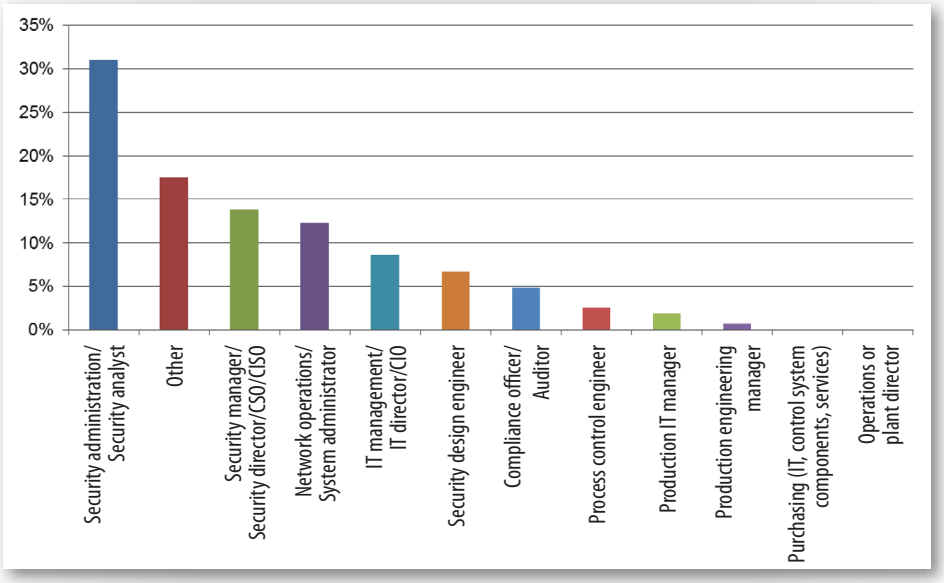


Figure 4. Respondent Roles

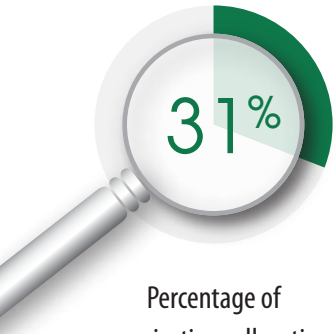
The survey suggests traditional information security officers (ISOs) and plant managers take the lead on integrating and maintaining cybersecurity controls. This may indicate the need for a new combined role that merges IT and security with SCADA and ICS knowledge and experience.

The survey also uncovered an interesting difference between the threat perception of security administrators and analysts as compared to security managers, directors or CISOs.

Of the first group, assumed to be more hands-on based on industry job descriptions, 37% expressed a "high" level of threat, and 48% of the second group, assumed to be focused less on hands-on tasks, perceived the threat level as "high." It is interesting that those further removed from the day-to-day security tasks feel a greater threat. This may be due to their overarching concerns about business continuity and the costs associated with experiencing and mitigating breaches.

Constrained Budgets

Of respondents who were aware of the budget allocated to cybersecurity, 31% stated their allocations were between 1% and 5% of the corporate budget. Given that there has been an 8,000% increase in per-worker economic output associated with cyber industrialization,[4] this amount is underallocated. Technology has automated personnel, but does not have a conscience, and now that technology needs to be protected. Even if security budgets were to be increased 500% from their current allocation, it would be a small fraction of the workforce productivity increases generated by the technology.



Percentage of organizations allocating 1–5% to control system cybersecurity

What is the approximate percentage of your organization's annual budget currently allocated to control system cybersecurity issues?

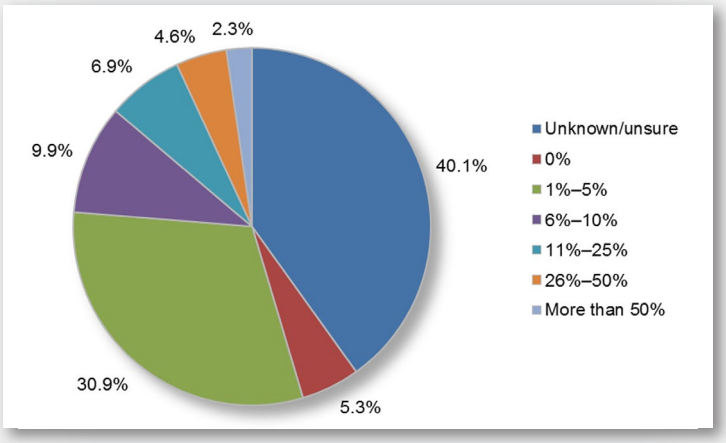


Figure 5. Cybersecurity Budget Allocation

The documented lack of awareness concerning budgetary allocations may be due to the specific roles of the respondents; however, personnel involved in protecting assets should have a working knowledge of how much of their budget can go toward protecting it.

Why is budget important? Success in responding to cyberthreats depends on having the appropriate cybercontrols, personnel and organizational commitment, which is often determined by the ability to secure the appropriate funding. Corporate leadership must understand the financial need, and security personnel must understand how to invest budgeted funds through the correct mixture of security controls, procedural enhancements and workforce education.

[4] "Decoding the Future with Genomics," Juan Enriquez, www.ted.com/talks/juan_enriquez_on_genomics_and_our_future.html

Interestingly, the perceived threat is slightly lower than it was in 2013. In the 2013 survey, 69% of the respondents perceived the threat to be high to severe, whereas in this year's survey only 53% of the respondents perceived the threat to be high to severe (see Figure 6).

What level do decision makers at your organization perceive the control system cybersecurity threat to be?

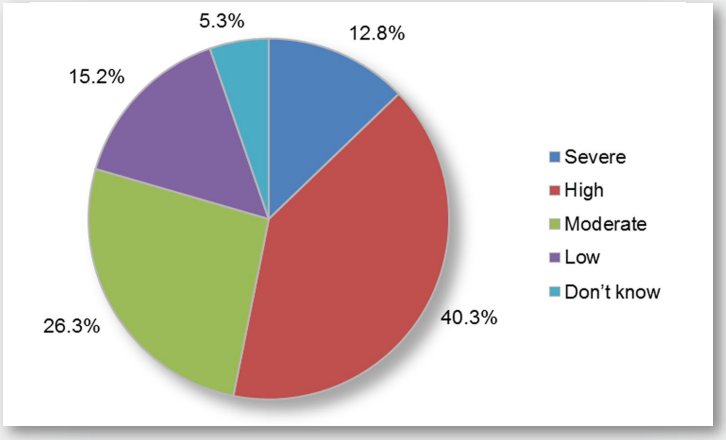


Figure 6. Decision Maker Perceived Threat Level

More than 50% of the respondents for two years in a row depict the cybersecurity threat as high or severe.

Last year's question asked the participants what *they* perceived the control system cyberthreat to be, whereas this year's question asked what *decision makers at your organization* perceive the threat to be. It is possible the respondents feel their organizational leadership does not evaluate the threat level as seriously as the respondents do, leading to this discrepancy.

Regardless, more than 50% of the respondents for two years in a row depict the cybersecurity threat as high or severe. This continued threat assessment might indicate that organizations in the United States, such as the Occupational Safety and Health Administration (OSHA), should be taking heed to protect the operational safety of the workforce due to cyber asset misuse. OSHA's core mission is to provide a safe and healthy workplace, which cannot be provided without security controls. A full text search on OSHA's website reveals no cybersecurity results.

Threat Vectors

External threats, malware and insider exploits continue to be the top three concerns among the respondents, as they were in 2013. Figure 7 provides the current results.

What are the top three threat vectors you are most concerned with?

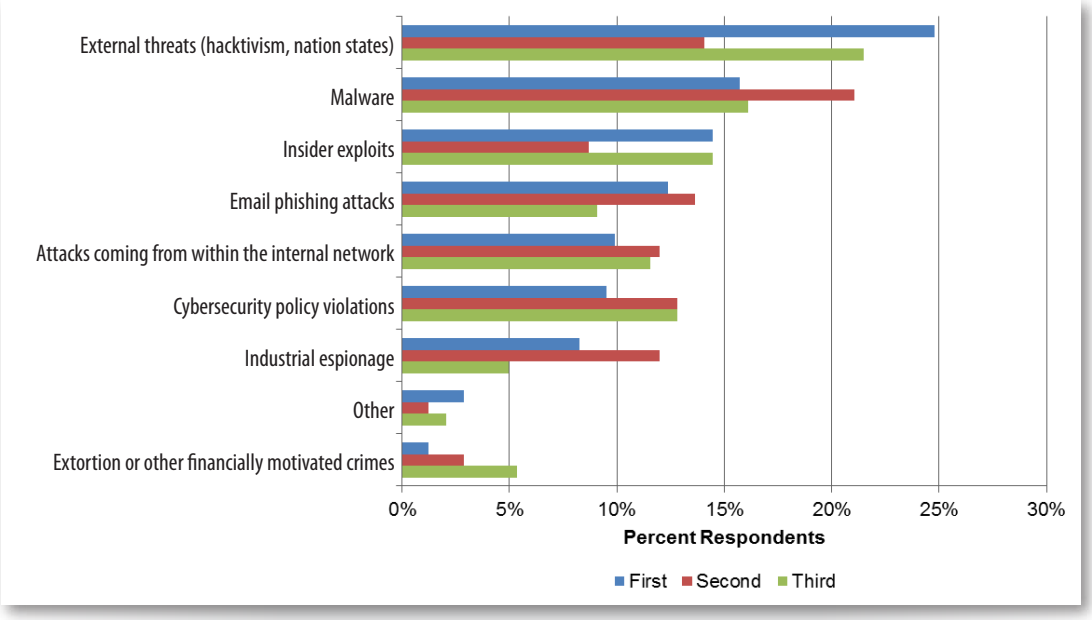


Figure 7. Top Threat Vectors

The remaining categories can easily be interpreted as the subcategories of external threats (industrial espionage and extortion or other financially motivated crimes), malware (phishing attacks), and insider exploits (attacks coming from the internal network and cybersecurity policy violations) and may have influenced the answers toward the broader categories.

By way of comparison, the financial services[5] and health care[6] industries are more concerned with insider threats and mistakes.

It is interesting to note that specific email phishing attacks are fourth highest on the list. Advanced persistent threats (APTs) typically use phishing as a mechanism to introduce malware. As in traditional IT security, these attacks continue to be not only effective, but also frequent. They are likely to continue because they are often successful for attackers.

[5] "Risk, Loss and Security Spending in the Financial Sector: A SANS Survey," www.sans.org/reading-room/analysts-program/survey-financial-sector

[6] "Inaugural Health Care Survey," www.sans.org/reading-room/analysts-program/2013-healthcare-survey

More guidance on specific steps organizations can take is offered later in this paper, but SANS cannot stress enough that, because APTs are often introduced via email, organizations should conduct an internal spearphishing education campaign. It is essential to provide the workforce with information about how and why they might be individually targeted and explain that the phishes might look more legitimate than the attacks that have been blocked in the past.

Furthermore, any security awareness should associate cybersecurity with every worker's job tasks and not assume security is the sole responsibility of IT or security staff. An organization's best intrusion detection capability is vigilant personnel.

Any security awareness should associate cybersecurity with every worker's job tasks and not assume security is the sole responsibility of IT or security staff.

Visibility into Threats

Survey respondents clearly need more visibility into their threats. In the survey 39% rate their visibility as only OK, poor or very poor, while only 26% rate their visibility into network cybersecurity threats as excellent or very good, as shown in Figure 8.

How would you rate the level of visibility into cybersecurity threats on your network? Select the most applicable answer.

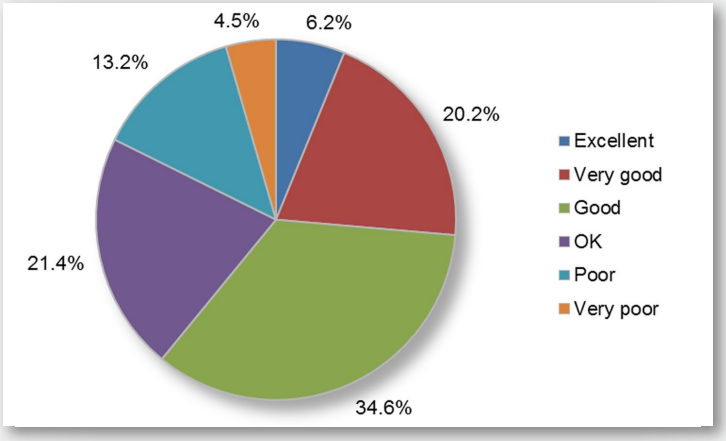


Figure 8. Cybersecurity Network Visibility

The asset owner/ operator's knowledge of cyber assets and the network serve as the one major advantage security personnel have over an adversary.

Asset owners must know their infrastructure, its connections and applications to identify changes an attacker might make in the environment. Furthermore, they should understand the interaction among the devices to the point that their system can identify new traffic patterns or industrial protocol interactions (e.g., Modbus/TCP coil reads or register writes). As active defenders, asset owners also have the ability to reshape the digital battlefield while under attack by introducing choke points and mechanisms to regain control.

The asset owner/operator's knowledge of cyber assets and the network serve as the one major advantage security personnel have over an adversary. Combine that advantage with the ability to modify the cyberbattlefield at the whim of the owner, and it is a powerful attribute.

Let's hope that future surveys show at least 90% of respondents can rate their visibility as very good or excellent within the next 24 months.

Visibility in Control Systems

Secure-minded organizations can achieve greater network visibility by knowing what cyber assets are on their industrial network, what role they play, who communicates with what asset, and how they communicate. Staff must be able to visualize how the network operates to detect attacks as well as remediate back to the original operational state.

Breaches on the Rise

Validated intrusions are on the increase in control system environments, according to respondents. In our 2013 survey, fewer than 20% of the respondents' control system cyber assets had been breached. This year almost 27% indicated their control systems networks had been infected or breached, while another 13% had suspicions of breaches, as shown in Figure 9.

Have your control system cyber assets and/or control system network ever been infected with malware or purposely breached by internal or external parties?

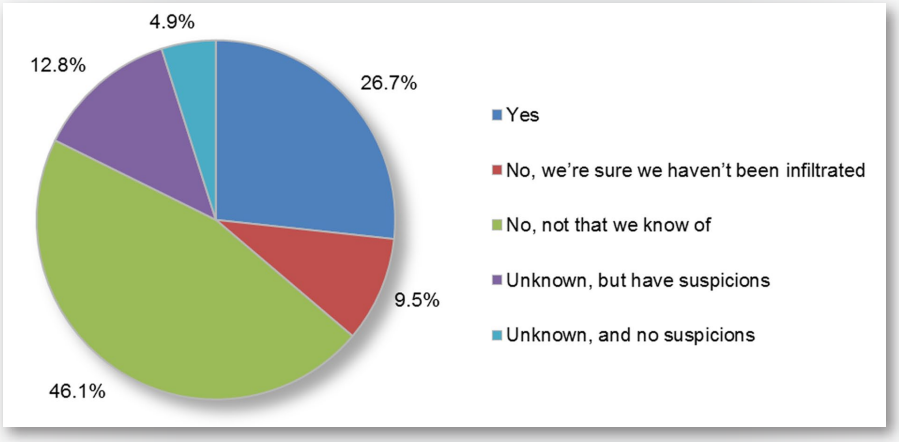


Figure 9. Control System Breaches

Percentage of respondents who know or suspect their systems have been breached

In addition, the percentage of those who suspect, but can't prove, they have been victims of a breach has increased from 8% in 2013 to nearly 13% this year. Recent ICS honeypot project results also validate that breaches are on the rise.[7]

Of those who say they experienced breaches, only 34% were able to answer how many attacks they endured during the same time period. Almost 28% of respondents who detected breaches have suffered three or more, as shown in Figure 10.

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

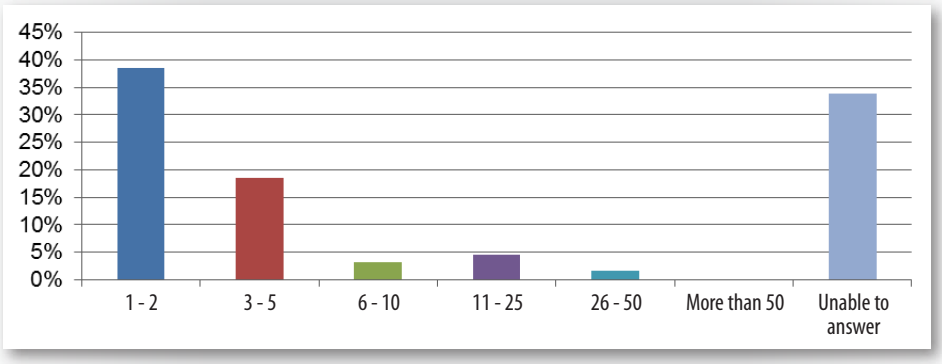


Figure 10. Frequency of Infiltration

[7] www.controleng.com/single-article/cyber-security-experiment-reveals-threats-to-industrial-systems

Typically, more than two breaches signal a systemic security problem that requires a complete business realignment to resolve. Multiple breaches essentially mean the environment has become untrustworthy. Furthermore, personnel physical safety is at risk, and the business may become legally liable for not performing due care. A recent Control Engineering article describes just this situation, where management no longer can use plausible deniability pertaining to control system cybersecurity awareness.[8]

Of those who could answer the question about duration of breaches (most could not), a surprising and somewhat reassuring result is that 28% say their organizations discovered the infiltration or exploit in less than 1 day; conversely, 39% took 2 or more days to identify the breach. Figure 11 provides a breakdown of reporting time.

EXPERT ADVICE:

Organizations will need to have better visibility and forensics capabilities to regain trustworthiness of their systems. The only mechanism to provide that visibility is having a sufficient baseline and a forensic trail of cyber activity.

How long did it take to discover the infiltration or exploit?

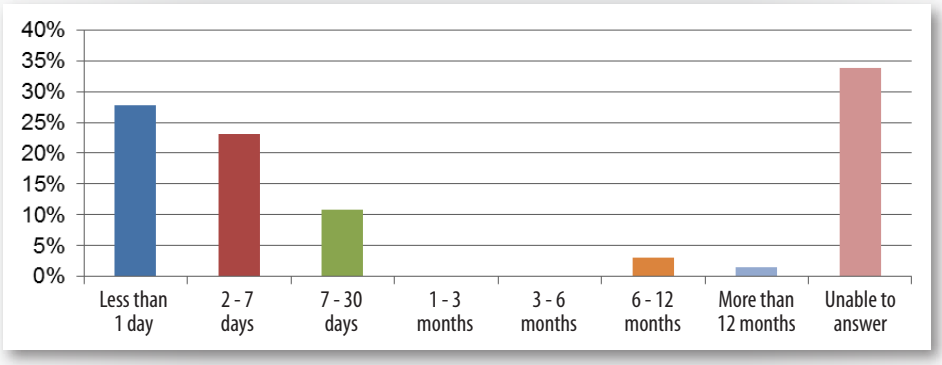


Figure 11. Exposure to Detection Time Period

A single-second breach can lead to disastrous consequences within control system environments. Imagine what damage (e.g., chemical spills, toxic aeration, fresh water tampering and extortion) could be caused by an undetected breach that continues for days, weeks or even months. Because control system protocols are typically not authenticated, don't require security-grade integrity checking and are left wide open to OSI layer 2 attacks, they are highly vulnerable.

Adding to the potential mayhem, man-in-the-middle tools that have been publicly available for three years are able to manipulate control signals while blinding the operator.[9]

Vendor-neutral protocols are even more at risk because they are more readily documented. Information on how to manipulate and attack such protocols is widely available publicly for attackers to use. For example, a Modbus/TCP man-in-the-middle tool took only 90 minutes to develop—and DNP3 took another 60 minutes.

The risks escalate exponentially when technical weaknesses are combined with the amount of Open Source INTelligence (OSINT) that can be found on the Internet (e.g., social media, support forums, job boards and marketing materials). Ultimately those responsible for security must assume that when they first detect a breach, their entire infrastructure—logging system, email communication network, VoIP systems—has been compromised.

[8] www.controleng.com/single-article/plausible-deniability-is-not-a-security-strategy/cb137008643d0dec3774217ee03b2d69.html

[9] www.youtube.com/watch?v=04AQMfA1AbM

Asset owners and operators care about the safety of the general public and their personnel while ensuring continued operations, based on survey results. According to respondents, the top three priorities for implementing security controls are:

- Preventing harm to the general public
- Preventing control system service interruption
- Protecting the health and safety of personnel

These are the strict requirements of operating control systems that utilize processes that may have an impact upon the general welfare of the surrounding population, such as nuclear power plants or hydroelectric dams with people downstream. Figure 12 illustrates the priorities that drive implementation of controls to protect critical systems.

What are your top three priorities when it comes to implementing effective controls for the security of your control systems? Rank the top three, with "First" being the highest priority.

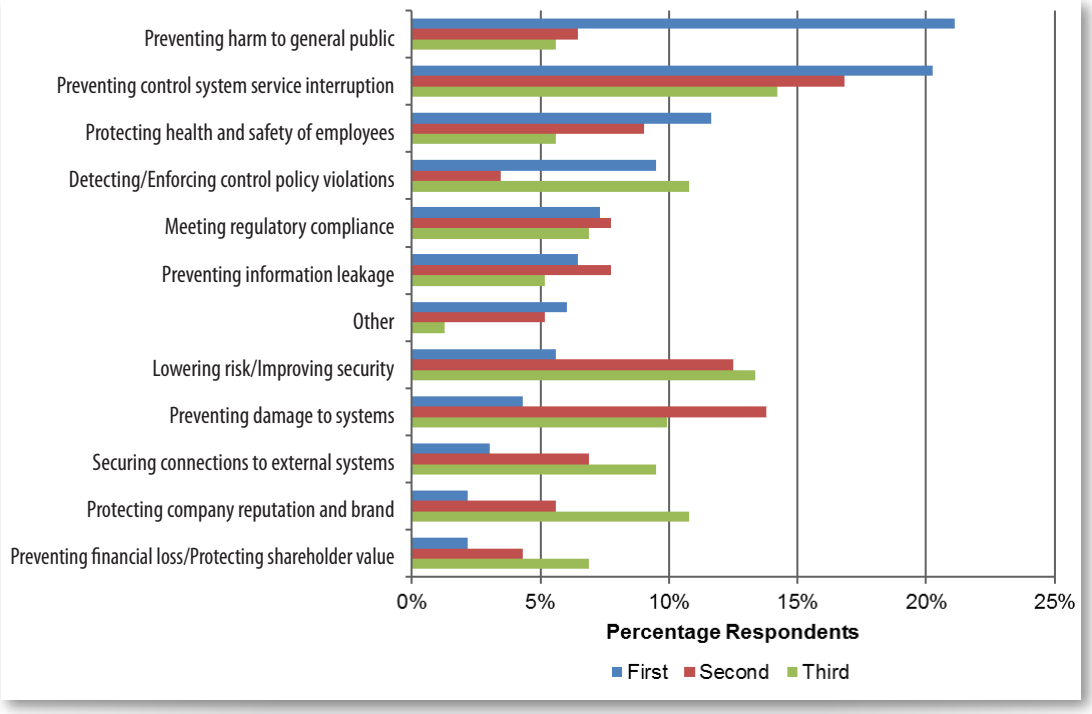


Figure 12. Primary Drivers

Note that items such as protecting shareholder value and reputation are low on the list of priorities in this survey. It would be interesting to learn whether the board of directors, investors and management would agree with this perspective. Their motivations are financially oriented, while it is likely the survey respondents are focused on different topics.

On the technical side, securing connections to external systems was also low on the list, as it was in our 2013 survey. SCADA and ICS staff should look more closely at including external connection security as part of their ongoing security efforts, especially since external threats are a prime attack vector, as illustrated previously in Figure 7.

Critical Asset Risk Allocation

The particular assets that respondents are most concerned with from a risk perspective include their traditional IT infrastructures and systems interacting with embedded controllers. In our survey computer assets (77%) and network devices (66%) were higher on their list of concerns than embedded controllers (53%). See Figure 13 for greater detail.

Of your critical assets, which are you most concerned with from a risk perspective? Select all that apply.

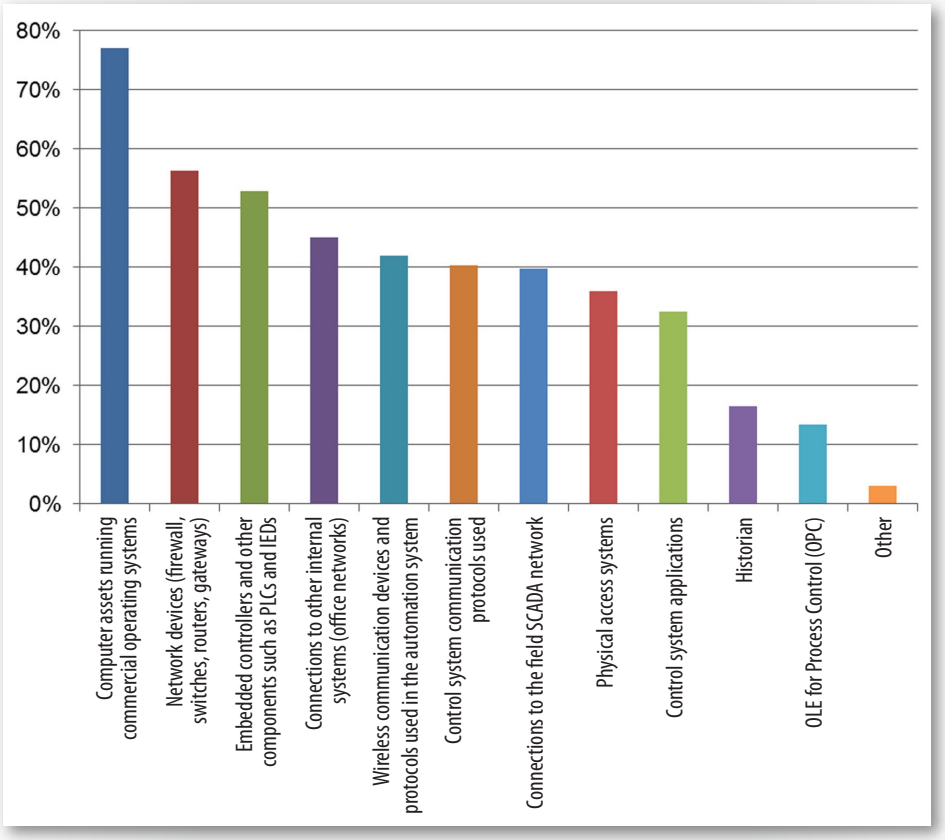


Figure 13. Components of Concern

The apparent current focus on securing traditional IT components and software as opposed to the deeper industrial control system components may make sense as part of a logical ICS security maturity model. Tools and practices for securing operating systems, for example, have ample precedent. The disproportionate focus on segmentation and firewall technology is not surprising, either, considering their maturity and adaptability to control system architectures. Newer security technologies, including security information and event management (SIEM) solutions and tools, which will provide much better visibility into control system networks and underlying components, are in early use now.

However, the true operational tasks reside in the embedded controllers, control system applications, OPC servers and historians. While at the low end of the risk equation for survey respondents, these systems are primary targets for state-motivated and other attackers bent on causing disruption in systems and possible human harm. OPC systems serve as ICS protocol gateways, providing just the means necessary to impact operations while blinding the operator.

Asset Monitoring

As would be expected, respondents say their organizations are applying the most resources to their top concerns. Network infrastructure and computers are also the most commonly monitored in control system environments, as shown in Figure 14.

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

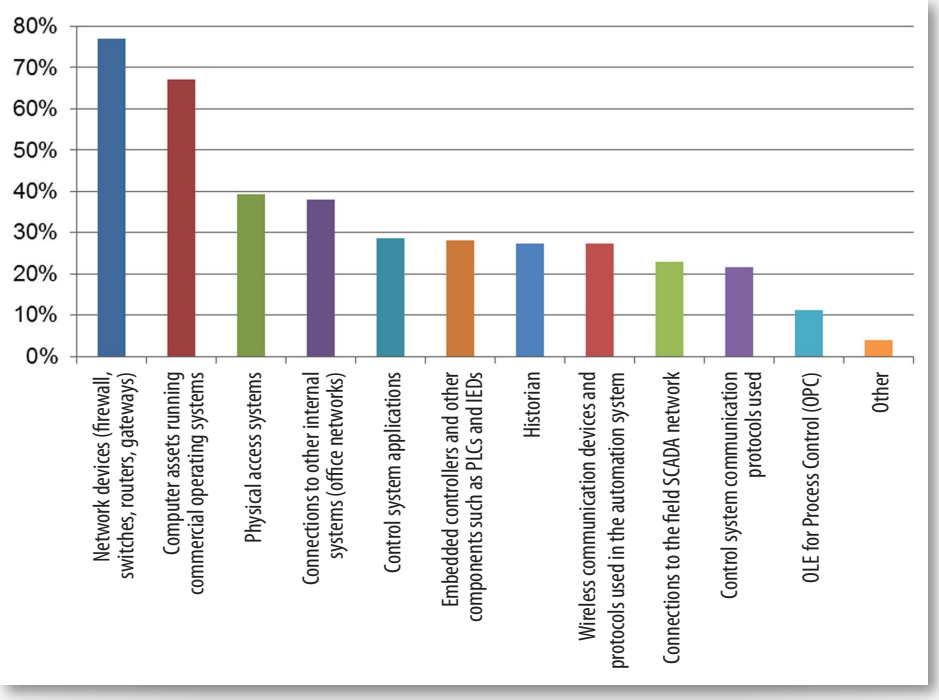


Figure 14. Availability of Log Data

The risk allocation illustrated previously (Figure 13) primarily matches the logged assets—except for the visibility into embedded controllers. The actual control system assets are not as commonly monitored, because many may not have the capability to generate log reports. The most critical elements and the ones that actually control operations need mechanisms to be monitored, whether in the form of an agent on the controller and system or a network-based agent watching for signals and communications that should not be associated with that system, for example.

Alarmingly, OLE for Process Control (OPC) is rated as the least frequently monitored asset—yet it typically serves as a conduit between the control system and corporate networks. The OPC application and its underlying database can serve as a great pivot point for attackers and must be monitored for signs of abuse.

Control System Security Advice

It is highly recommended that those responsible for control system security take steps to protect the actual control system assets and their native ICS protocols. Consider these suggestions:

- Reach out to the vendors to understand how their software developers have been educated to build secure software, as well as traditional operating system security controls.
- Harden the operating system. Bastille Linux is a great tool to help users learn about an operating system hardening methodology. Keep a keen eye out for developments in this space to help address this necessary capability.
- Tools such as passive ICS network mapping, infrastructure configuration analysis and ICS protocol dissection can serve as great mechanisms to protect ICS cyber assets.
- Once a system is compromised or an intrusion is detected, immediately assume everything is compromised and work from there.
- Start validating the trustworthiness of infrastructure and prioritize your remediation checklists.
- Look at securing OPC and other networks that are gateways to attacks.

More advice is provided in a recent control system forensics article.[10] The article describes specific defenses to have in place, as well as active procedures to enact during an incident.

[10] www.controleng.com/single-article/making-digital-forensics-a-critical-part-of-your-cyber-security-defenses/2be797b1e79934f142781ac59e33110a.html

Vulnerability Detection

Survey respondents use a number of techniques to detect vulnerabilities in their systems. Active or passive scanning is used by 61%. The second largest category that respondents monitored against was CERT notifications, which 60% say they use in detection (see Figure 15).

What processes are you using to detect vulnerabilities within control system networks?

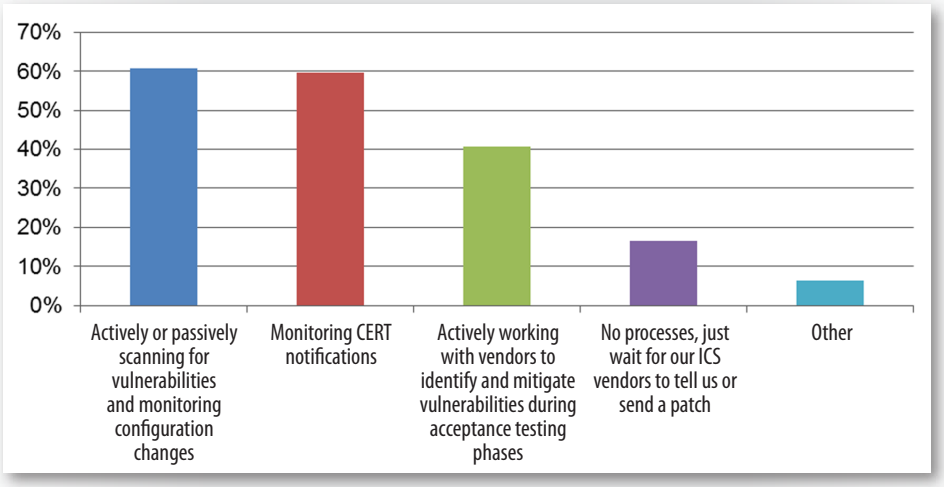
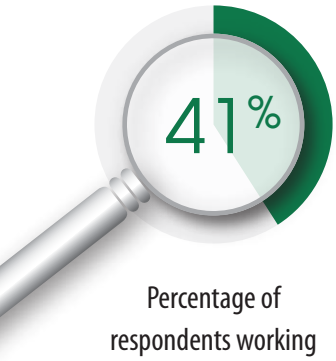


Figure 15. Processes Used to Detect Vulnerabilities



Percentage of respondents working with vendors to identify and mitigate risks

Active Scanning and Control Networks

For those using active scanning, here's a very important piece of advice: Never use an active scanner within an operational control network. It can disrupt operations, and most active scanners do not identify weaknesses in control system cyber assets anyway. Most active scanners are tuned to identify vulnerabilities on commercial operating systems, not control system–embedded devices and applications.

Control system vulnerability documentation, such as that provided by CERTs worldwide, contains valuable information and should be routinely monitored, interpreted and applied to each organization's environment.

In addition, vendors are an important part of the detection picture, with 41% of respondents saying they work with vendors to identify and mitigate risks. It is absolutely essential that organizations and their vendors work together on a per-environment basis. Then, over time, cybersecurity controls added into one vertical, such as the electric sector, are available for all industries.

Organizations such as critical infrastructure groups are already consolidating and sharing this type of information. There have been many successes provided to other verticals that have not been bound by North American Electrical Corporation Critical Infrastructure Protection (NERC CIP) standards simply because the lessons learned have provided new products and matured existing ones.

Threat Intelligence

Detecting active threats pointed at an organization's systems is a key to preventing an attack from expanding throughout an organization. Threat intelligence is a specific science that is still maturing within the ICS sector. Is the role of an organization's personnel to keep track of all of the active threat actors, their intentions and active attacks? Or, is their role to act upon this information and associate it with the organization's environment?

Commercial entities that provide this service are springing up, so it is a bit alarming to see that almost 58% of respondents rely on their own trained staff to search out events. The internal staff should be trained to perform an initial detection of the threat; however, it is then highly recommended that the threat be turned over to incident response and forensics experts for scoping and remediating the event.

Other types of intelligence they rely upon are nearly equally allocated across threat intelligence vendors (46%), government agencies (45%), anomaly detection (41%) and industry partnerships (36%), as shown in Figure 16.

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

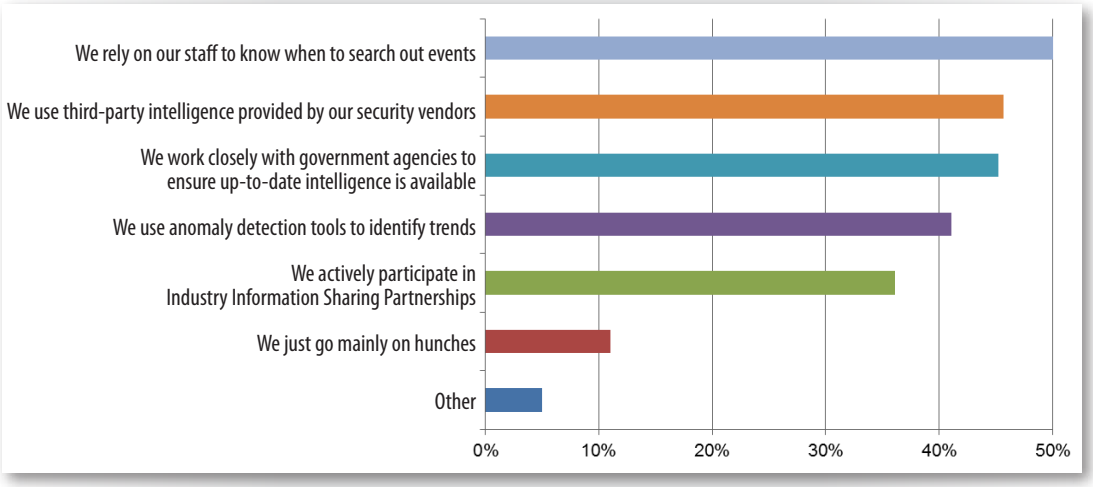


Figure 16. Detecting Threats Aimed at Control Systems

Responsibility for Cybersecurity

Identifying who is responsible for cybersecurity is one of the early, critical steps to protect cyber assets. The seat of responsibility should be one that affords accountability and constant communication channels with operations and physical security. The role should be at the appropriate level of the organization to allow access to resources and provide executive awareness to cybersecurity risks.

Personnel

The two roles most commonly seen as responsible for security of control systems are the information security officer (57%) and the owner/operator (52%). This further supports our contention that a new role for the control system cybersecurity manager is being defined as more embedded control systems are identified and brought online.

Other roles with responsibility for control system security are listed in Figure 17.

EXPERT ADVICE:

Any IT-educated cybersecurity personnel must think about high availability of accurate control information with loss-of-life scenarios that can be protected not only by cybermodifications and protections, but also by physical, electrical, mechanical, biological and chemical re-engineering.

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

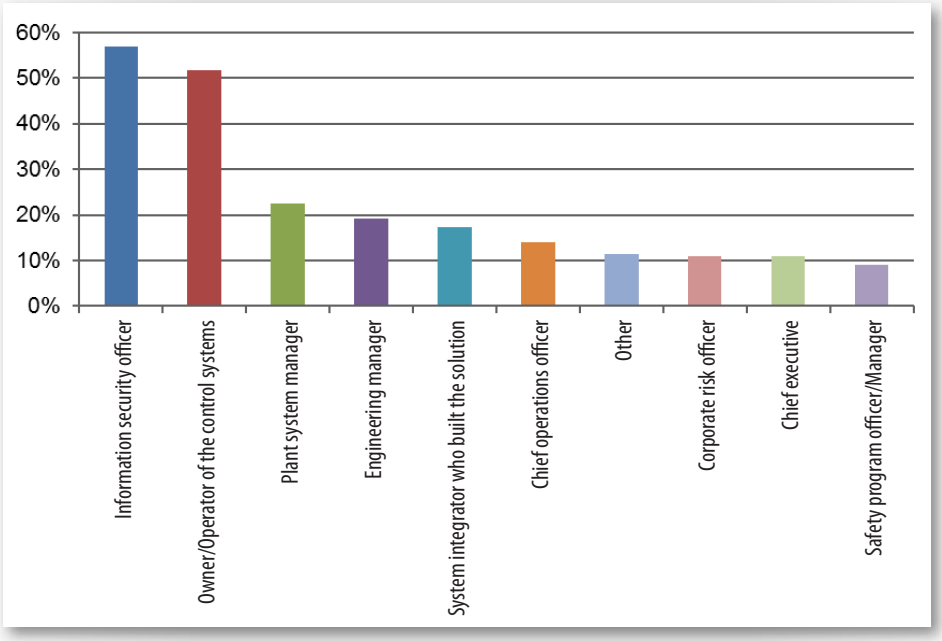


Figure 17. Responsibility for Security of Control Systems

Education is important to bridge the gaps in knowledge for both IT and operations personnel. An IT-scoped individual migrating into the control system realm will need transitional education, as would an owner/operator stepping into a security role. Such education may assist operators and security staff working together and ultimately lead to the creation of a dual role such as Information and Control Security Officer (ICSO) or two individuals working together to fill a control security office.

Standards

Similar to our 2013 results, the most frequently used standards today include the United States NIST Guide (32%), followed by the Critical Security Controls (26%) and then NERC CIP and ISO 27000 series (both at 20%). See Figure 18.

Which of the following cybersecurity standards do you currently utilize (or plan to use in the next 6 months) in your control system environment? Which do you plan to continue using or to implement within the next 24 months? Select all that apply.

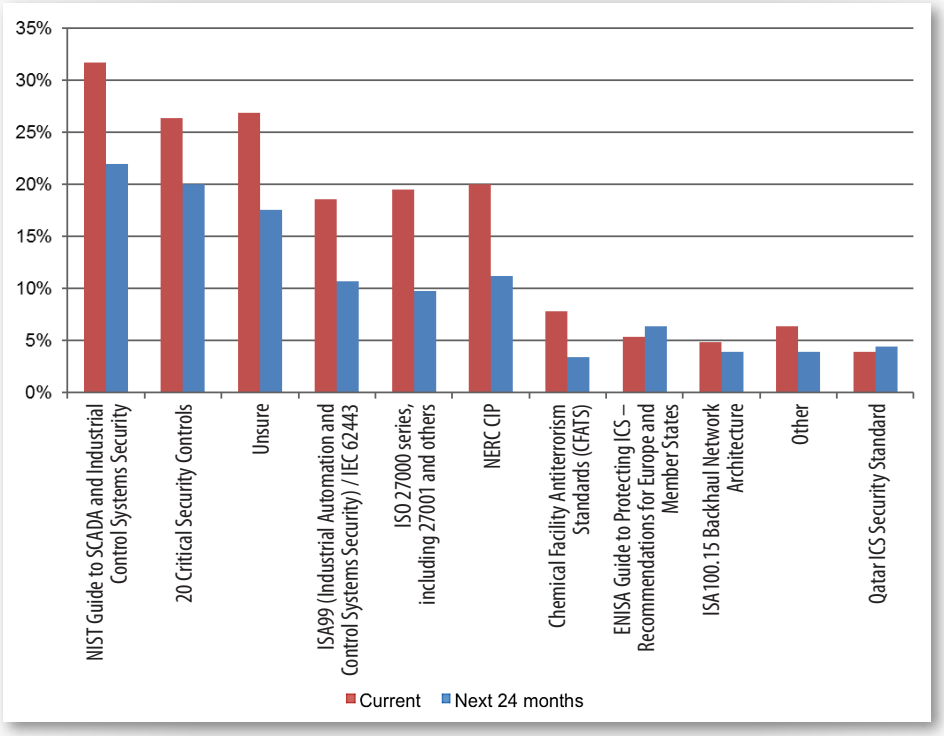


Figure 18. Cybersecurity Standards Mapping

Percentage of respondents who are unsure of the standards their organization uses

Interestingly, 27% of respondents are unsure of the standards their organization currently uses. It is difficult to ensure security when you are unaware of the security standards you should be adhering to.

Getting Started with Standards

Regardless of which standard is adopted, utilize a security framework to manage requirements interpretation and security metrics. Here are some options:

1. Adopt a cross-standard approach, whether bound by specific regulations or not. Begin by reviewing the NERC CIP reliability standards and their lessons learned, which are documented throughout the NERC portal. Review requests for interpretations, industry responses and voting, and compliance announcements at the NERC website.[11] NERC CIP will also be continuing its growth phase as asset owners and operators integrate NERC CIP version 5.
2. Then, review the Critical Security Controls and their supporting metrics.[12] Finally, review guidance documentation provided by documentation such as NIST 800-82 and worldwide CERT organizations.
3. Centralize response by consulting the National Institute of Standards and Technology (NIST), NERC CIP or Department of Homeland Security (DHS) Chemical Facility Antiterrorism Standards (CFATS) in the United States, or the International Electrotechnical Commission (IEC), International Society of Automation (ISA) or Qatar ICS standards in the international community.
4. Consider other, newer collaborative standards, such as the ISA/IEC-62443 (formerly ISA-99, currently 19% usage), Qatar's ICS Security Standard (currently 6%) and the European Union's ENISA guidance (currently 5%).

System Procurement

Success in integrating cybersecurity into the business is directly associated with making security part of the procurement process. It is a constant dialogue between the asset owners and operators as to what requirements constitute security. Although vendors try to respond with better security of their controllers either through add-on or newer versions of products, control system operators are not willing to pay extra for extra security or newer, more security control systems.

[11] https://standards.nerc.net

[12] www.sans.org/critical-security-controls

According to the survey results, 32% consider cybersecurity in procurement, and 35% "Somewhat" consider cybersecurity, as shown in Figure 19.

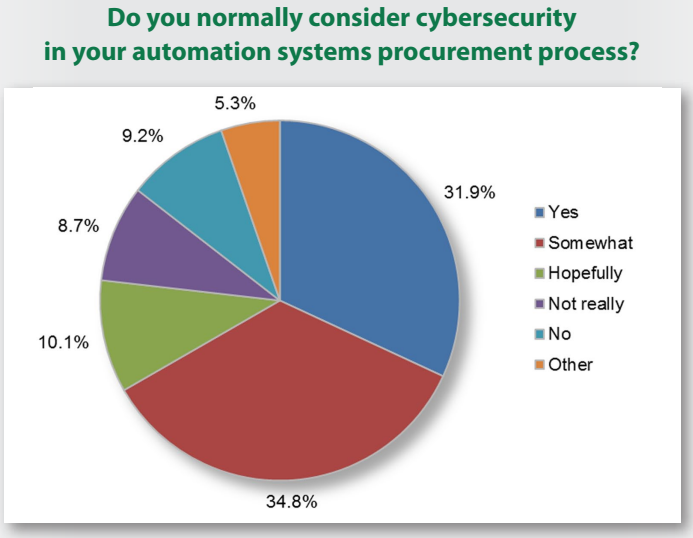


Figure 19. Cybersecurity in the Automation Procurement Process

These numbers are in keeping with our 2013 survey, leading us to conclude that the asset owners and operators are not, by default, willing to bear the cost of additional security within their systems. The playing field needs to be equal among owners/operators; therefore, the entities will need to be forced into using regulatory mechanisms like NERC CIP to influence business changes.

Security Control Methodologies

Effective active defense requires some key security tools. Survey respondents noted they use an up-to-date baseline of identified cyber assets (used by 51%), whitelisting of applications (used by 28%), configuration management (used by 52%) and log aggregation (used by 43%). Access controls, used by 78% of respondents, will be insufficient if deployed without this knowledge.

Which of the following methods do you currently utilize for control system security, detection of attacks and violations, and enforcement of policies? Which do you plan to continue using or to implement within the next 24 months? Select all that apply.

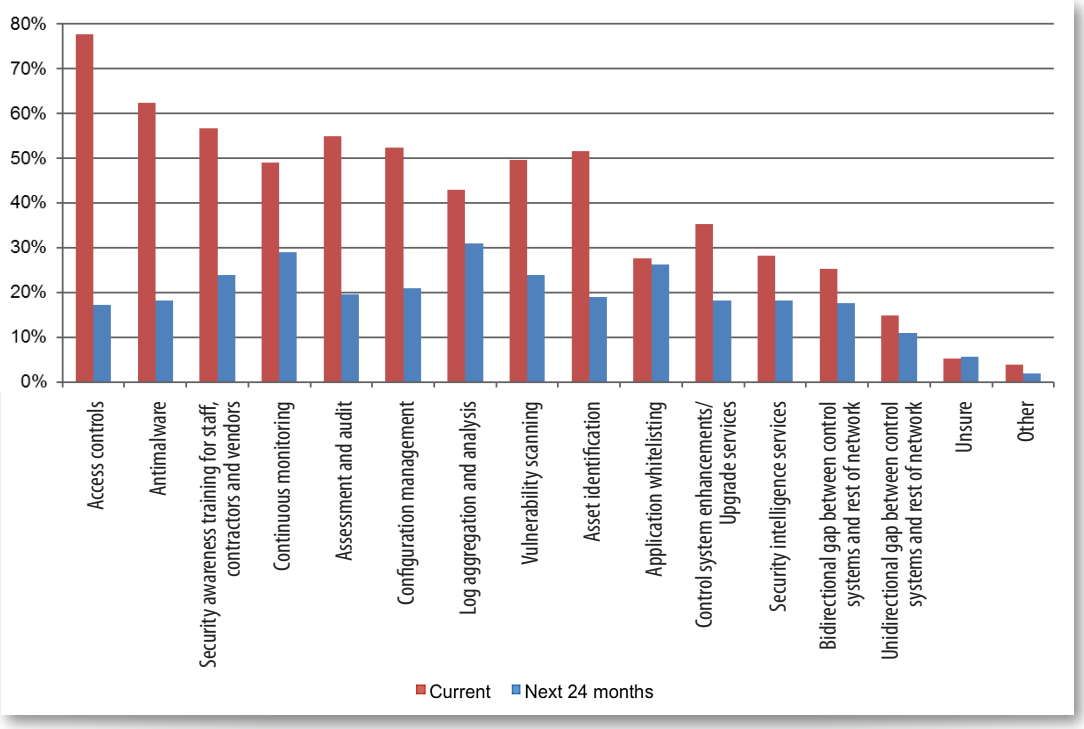


Figure 20. Control System Security Controls

These results are also similar to our 2013 survey, indicating that budgets haven't expanded significantly in the last year to address the cybersecurity challenge. This is disturbing given the increase in attacks against these systems and the inherent vulnerabilities organizations aren't managing well enough.

How can one protect assets with access controls if they are not properly identified and restricted to a specific application baseline of activity? Systems must be inventoried and monitored to determine what systems the organization has and how they communicate, and then restrict access. Armed with a sufficient baseline, organizations can monitor for unexpected activity, and trained insider personnel can execute predefined incident response procedures using preplanned on-call external resources.

Patching Practices

In our survey 52% patch on a regular basis, 23% use virtual patching to avoid downtime issues and 7% layer controls instead of patching. Another 23% patch in batches when downtime is available. But a surprising 8% neither patch nor layer controls to mitigate vulnerabilities (see Figure 21).

How does your organization handle patches and updates on your critical control system assets? Select the most applicable.

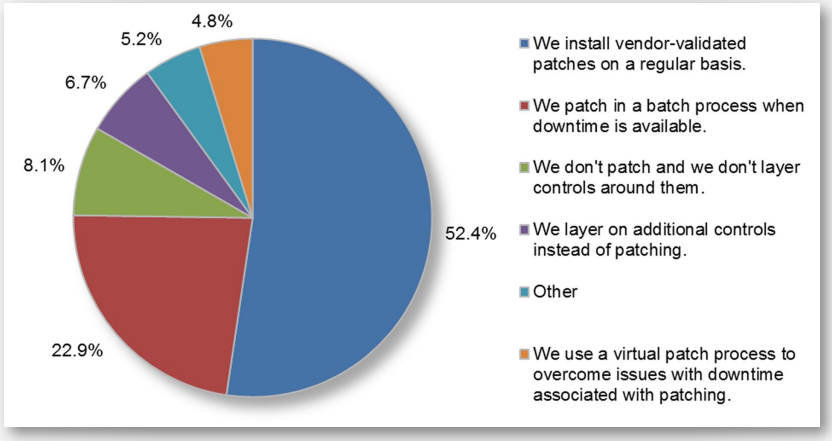


Figure 21. Patching and Updating Critical Control System Cyber Assets

Percentage of respondents who neither patch nor layer controls to mitigate vulnerabilities

Patching of industrial systems is a struggle. Typically, more time is required to identify and implement compensating measures than is spent on patching the systems. Ultimately, the choice to patch or not to patch depends upon the type of control system assets, whether they have a common outage window or whether there are sufficient compensating security controls in the case that a patch is not possible (see the Advice box, "Scheduling Patching Outages").

Scheduling Patching Outages

Designing control system network and system architectures with security in mind requires an active defense mentality and a flexible control system architecture that can be adjusted during live processes.

Asset owners should choose when to perform the updates to control uptime and downtime. Each control system is different and has different outage windows; specifically, batch versus continuous processes. There is an additional struggle: Attackers have an advantage if the outage windows are documented in publicly accessible sites.

For example, scheduled maintenance plans at NRC-regulated facilities are readily available on the Internet. In these situations the attacker can know exactly what patches have been installed based upon the last outage window. As a result, potential attackers can easily determine, for example, that patches released since the last window (and most likely the past two or three windows) have not been installed.

Breach Reporting Procedures

Most organizations do have official breach-reporting processes. Among responding organizations, 57% use internal resources to respond to the signs of a breach (see Figure 22).

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

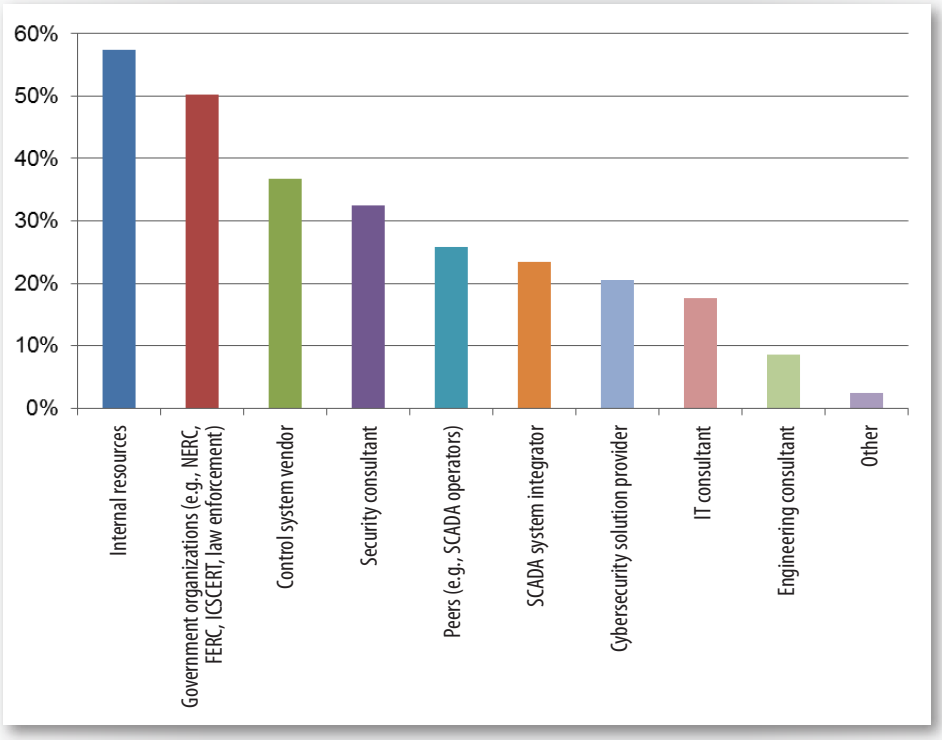


Figure 22. Who do you call in case of a breach?

Control system assets are easily worth hundreds of millions of dollars, and one wrong move can impact millions of lives. Survey respondents note that after consulting with internal resources, organizations solicit help from government entities, including law enforcement (50%), vendors (37%), security consultants (33%) and peer resources (26%) to manage incidents.

Test Your Security Aptitude

The simplest metric to identify an organization's security integration and effectiveness is to review its incident response plan and the documentation generated each time it has been executed and updated.

Organizations assessing their security posture also should carefully consider the following and integrate the suggestions into security planning:

- How well trained is staff concerning potential attack vectors an active adversary may use? Help staff get the necessary training to identify and defend widely used attack vectors.
- Do procedures, people and technology cover current threats against your systems and their vulnerabilities? This should include visibility, assessment and closed remediation for threats discovered.
- What are your response procedures? Assign responsibility for cybersecurity response.
- At what point does onsite physical security personnel hand confrontations over to law enforcement? An effective cybersecurity program should follow similar policies that are well documented and communicated.

If there is no incident response plan or follow-up reporting, this is a simple indication of an immature cybersecurity organization—regardless of how many personnel or controls are in place.

Recommendations

Consider these final recommendations:

1. Know and map devices, their physical interconnections, the logical data channels and the implemented ICS protocol behaviors among the devices (e.g., read coils, write registers, scans and time stamps).
2. ICS protocols (e.g., Modbus/TCP, DNP3 without authentication, Ethernet/IP, ProfiNet, BACnet, ISO-TSAP, S7, ICCP without certificates and similar) are inherently vulnerable by design, configuration or vendor implementation. As such, they must be protected from attackers reaching the internal communications network.
   - Use bidirectional and unidirectional firewalls coupled with strict operational procedures to protect the communication channels.
   - Investigate latency/scan rate challenges using protective options like SSL or IPSEC for communication to field devices and ICCP links.
3. Protect vulnerable OPC systems and database servers. These systems provide pivot points to attackers.
4. Make backups, protect systems from alteration or destruction and establish procedures to verify all configurations and device firmware.
5. Enable device logging, strict change management and log analysis automation based upon the environment's baseline of activity.
6. Define a well-maintained incident response procedure providing authorizations to impact operations.
7. Identify or create obsolescence procedures for decommissioning or redeploying each type of cyber asset used within the organization's facilities.
8. Educate personnel for the new normal of protecting assets during a time period of an international cyber arms race. Companies with cyber assets are, in essence, on the battlefield. This requires designing security into the environment with the appropriate choke points, active defense capabilities and manual procedures to enact during an active incident.
9. Expand cybersecurity budgets and define security needs during the procurement process. Then, be sure security is actively maintained by people within the organization.

Conclusions

Control system connectivity and the number of controlled physical assets is expanding rapidly. The active threat actors are increasing, while the organizational budgets for cybersecurity (for the past two SANS surveys) have not been sufficient to deal with system vulnerabilities, let alone these threats.

As a result, more respondents report being breached, with many of them suffering more than one breach. They also lack the visibility into their enterprises and the vulnerabilities associated with their devices. These trends reveal the need for more and better coordination between control system operators and their control system vendors. Ultimately, the efforts to protect control system assets reside in the hands of the asset owner, who can implement gap security measures. It is also up to the owner to work with vendors to ensure better security, visibility and patching.

Fortunately, resources for IT groups tasked with protecting control system environments are on the rise, and control system cybersecurity standards are maturing. On the other hand, individual nations are creating their own specific variants of guidelines to follow, meaning that organizations, particularly of international scope, will have multiple standards and regulations to adhere to.

It is SANS' hope that the industries responsible for managing the security of control systems do not get caught up in filling out check boxes to meet regulations rather than actually reducing risk through better security.

About the Author

Matthew E. Luallen is a co-founder of two control system cybersecurity companies: CYBATI, focusing on education, and Dragos Security, LLC, focusing on products and research. He has written, consulted and trained extensively on process control and SCADA security issues and continues to work with electric utilities in the US and Canada on the NERC CIP reliability standards. He has also presented and consulted on ICS cybersecurity within critical infrastructures to the government organizations and asset owners and operators. Mr. Luallen holds a bachelor's degree in industrial engineering from the University of Illinois-Urbana, a master's degree in computer science from National Technological University and is a 14-year Cisco Certified Internetwork Expert (CCIE). He serves as adjunct faculty for DePaul University's capstone cybersecurity and control system courses, as a certified instructor for Cisco Systems and as a certified instructor for the SANS Institute.

Sponsors

SANS would like to thank this paper's sponsors:

QUALYS® CONTINUOUS SECURITY

Raytheon

SOURCEfire®

tenable network security