Sponsored by
EiQ Networks, FireEye, IBM, Symantec and Tenable Network Security

SANS 2013 Critical Security Controls Survey: Moving From Awareness to Action

June 2013

A SANS Whitepaper

Written by: John Pescatore

Advisor: Tony Sager

Executive Summary

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In 2008, the U.S. National Security Agency (NSA) recognized the diversion of resources as a serious problem, and the agency began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats.[1] A consortium of U.S. and international agencies quickly grew, and ultimately, recommendations for what were to become the Critical Security Controls (CSCs) were coordinated through the SANS Institute.[2]

How well are the CSCs known in government and private industry, and how are they being used? More importantly, what can we learn from CSC implementations to date? These and other questions were posed to 699 respondents to a recent online survey conducted by the SANS Institute.

This is what we found:

- The majority of respondents (73%) are aware of the CSCs and have adopted or are planning to adopt them, while a further 15% are aware of the Controls, but have no plans to adopt them. Only 12% hadn't heard of the Controls before the survey.
- The respondents' primary driver for Controls adoption is the desire to improve enterprise visibility and reduce security incidents.
- Operational silos within the IT security organization and between IT and other business departments are still the greatest impediment to implementing repeatable processes based on the Controls.
- Only 10% of respondents feel they've done a complete job of implementing all of the Controls that apply to their organizations.

More detailed information and advice about the results and the CSCs are included in this paper.

1 www.sans.org/critical-security-controls/history.php

2 www.sans.org/critical-security-controls

Demographics and Analytics

The SANS Institute conducted an online survey on attitudes toward the adoption of the CSCs during March and April 2013. The survey had a total of 699 respondents.

Who Took the Survey

Security professionals represented the largest occupational group among the respondents, with the largest single occupational category in the survey being security administrators or analysts, at 45% of the total. Senior security professionals (security managers, directors or CSO/CISOs) made up 25%, and the IT manager/director/CIO categories each represented slightly more than 10%. Network operations/systems administration personnel made up 20% of respondents, and compliance officer/auditors and consultants made up another 11% (see Figure 1).

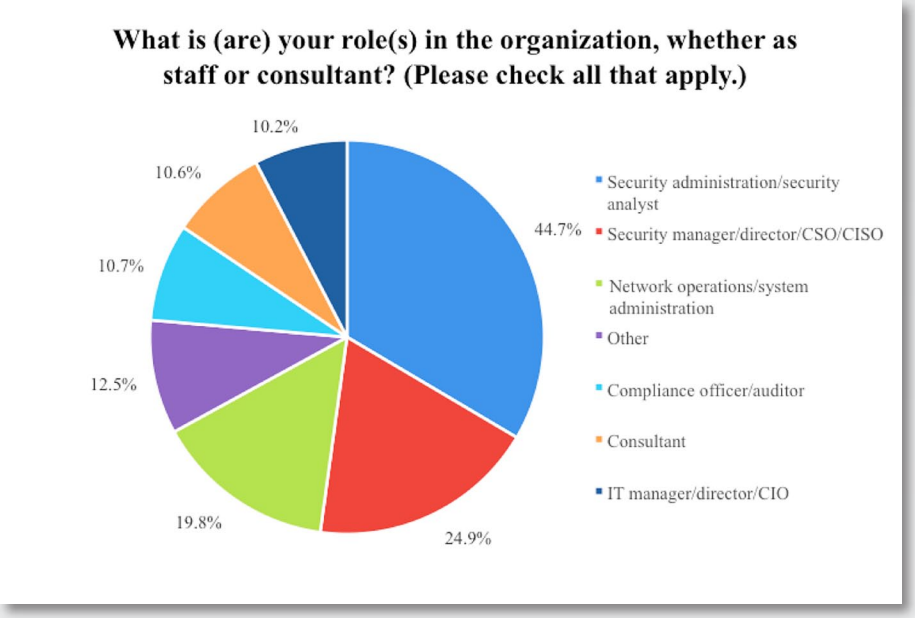

Figure 1. Roles of Respondents

Numerous respondents in the broadly distributed "Other" category indicated they are also administrators, but many developers were also represented in the "Other" category. (Note that respondents were allowed to choose more than one option, representing an overlap in responsibilities in some cases.)

The Industries Represented

The types of organizations represented by the respondents skewed heavily toward multinational or other large enterprises. The single largest group of respondents (40%) work for large enterprises (defined as having 2,000 or more employees), and 14% work for global 200 enterprises, which typically have more than 50,000 employees. The remaining respondents were more or less evenly distributed among small- and medium-size enterprises, as shown in Figure 2.

Figure 2. Size of Organization

Interestingly, though the CSCs were initially conceived as a framework oriented toward federal government IT, a broad range of industry verticals were represented in this survey, with government entities (20%) and financial institutions (17%) being the largest. Smaller but still significant industry segments were education, high tech, health care/pharmaceutical, manufacturing and energy/utilities (see Figure 3).

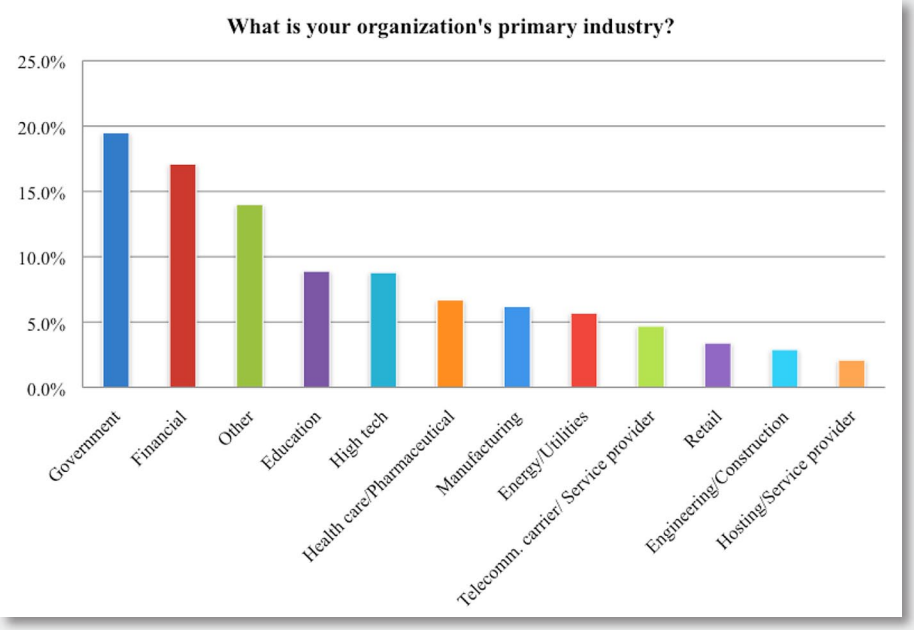

Figure 3. Industries Represented

This varied industry representation indicates that organizations of all types are finding uses for the Controls.

The Focus of SANS' Analysis

For analytical purposes, SANS grouped the responses to the survey questions into six areas, which are essentially arranged chronologically:

1. **Awareness –** The levels in the organization that are aware of the CSCs
2. **Perception of benefits and barriers to adoption –** "Going-in" assumptions of both gains expected from Controls adoption and reasons the Controls couldn't be adopted or wouldn't work
3. **Initial assessment –** Whether and how an initial gap assessment was performed
4. **Levels of adoption –** The extent to which the Controls have been integrated with and optimized for IT and IT security processes
5. **Implementation progress and experience –** Which Controls have been implemented, and what roadmaps and tools were used
6. **Measurement and metrics –** How benefits have been quantified and where major benefits have been seen

Level of Awareness

Currently, 20 areas of security are listed in the Critical Controls, version 4.1. These Controls begin with inventory and assessment of devices and applications, and include perimeter defenses, vulnerability remediation, application security, incident response and more. Figure 4 displays each of the Controls with links embedded beneath the buttons.

Figure 4. Top 20 Critical Controls

As noted in the introduction, a large percentage of the survey respondents (73%) have adopted, or are planning to adopt, some or all of the Controls, and another 15% are aware of them but have not adopted any of them. Surveys on any topic tend to attract respondents who are familiar with that topic, but even when this fact is taken into account, a combined 88% represents a very high level of awareness.

This finding is consistent with many of the long-form responses to the last question on the survey—which asked for suggestions for improvements to the Controls effort—as well as with anecdotal information SANS has received at CSC-related briefings and meetings. For example, the Multi-State Information Sharing and Analysis Center (MS-ISAC)[3] has shown a very high level of awareness in U.S. state government agencies. The fact that the CSCs meet the need for a "lens" that focuses security efforts on the areas offering the highest payback against existing threats is clearly driving this high level of adoption.

The survey results also show significant awareness—and influence—by high-level decision makers, with CIOs displaying slightly higher awareness than CISOs. Almost one-third reported that CEOs/COOs are aware and supportive of the Controls, as shown in Figure 5.

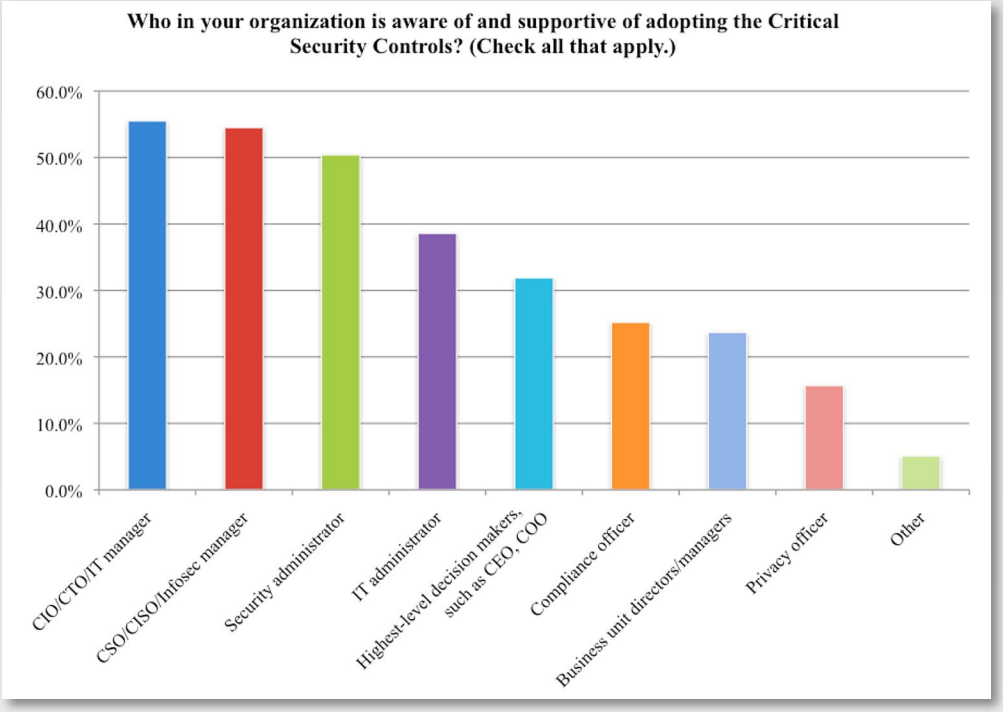

Figure 5. High-Level Support

The low awareness reported by compliance managers may seem surprising, but it's important to note that companies that match the survey respondents' demographics often don't have a formal chief compliance officer position. This same factor impacts the reported level of privacy officer awareness. However, a more significant factor is that although security and privacy are intertwined, the CSC effort has not been directly focused on issues like disclosure, notification and other legal requirements that are top-of-mind for privacy officers. As stated earlier, the CSCs are focused on reducing the cost and complexities of IT security through automation and, ultimately, on improving risk posture.

> ***Takeaway:*** *The high degree of awareness by top-level decision makers presents an opportunity to leverage the CSCs to make meaningful long-term gains in the effective and efficient delivery of enterprise security.*

3 http://msisac.cisecurity.org

Perceived Benefits and Barriers to Adoption

One goal of the survey was to determine what benefits enterprises see in adopting the Critical Security Controls, as well as what barriers are preventing or slowing adoption.

Perceived Benefits

The CSC effort began as a way to prioritize the security tools that are most effective in detecting, mitigating or blocking current threats. That benefit has clearly come across to the respondents: The top three drivers for adopting the CSCs all relate to increasing visibility of attacks, improving response and reducing risk, as shown in Figure 6.

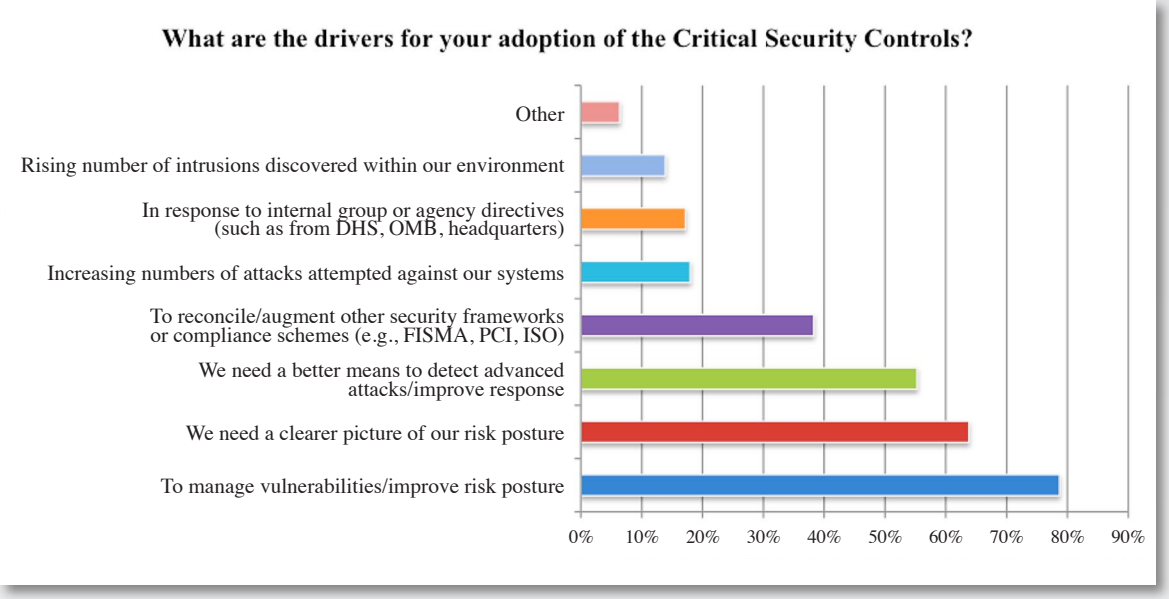

Figure 6. Drivers of Adoption of the Critical Security Controls

Another major goal of the CSC effort has been to focus on threats first, and then to address compliance-driven requirements. Compliance should be focused primarily on reporting on the results of a threat-focused approach to security rather than on compliance itself as the primary goal. So, it's no surprise that reconciling and augmenting compliance regimes and other security frameworks was the next most frequently cited driver for adopting the CSCs.

Only slightly more than 17% of the survey respondents cited internal directives as their major driver. This is actually higher than expected, because the CSCs are a community-driven, voluntary effort. They do not replace any compliance regime, and there is no compliance regime forcing businesses to adopt them. This makes the fact that almost one in five respondents do have internal policies driving their use rather impressive. However, if the gains realized by implementing the Controls are to become lasting, they must be embedded into formal policies and security program directives.

> ***Takeaway:*** *Due to all the publicity around advanced attacks, higher levels of awareness of risks mean gains for support of the CSCs.*
>
> *The use of the CSCs should be "baked into" updates to security architectures, policies and roadmaps.*

Barriers to Adoption

To understand how to implement the Controls, it's important to know what gets in the way of adopting them. According to the respondents, the two most significant barriers to CSC adoption (see Figure 7) are organizational problems (operational silos) and training issues.

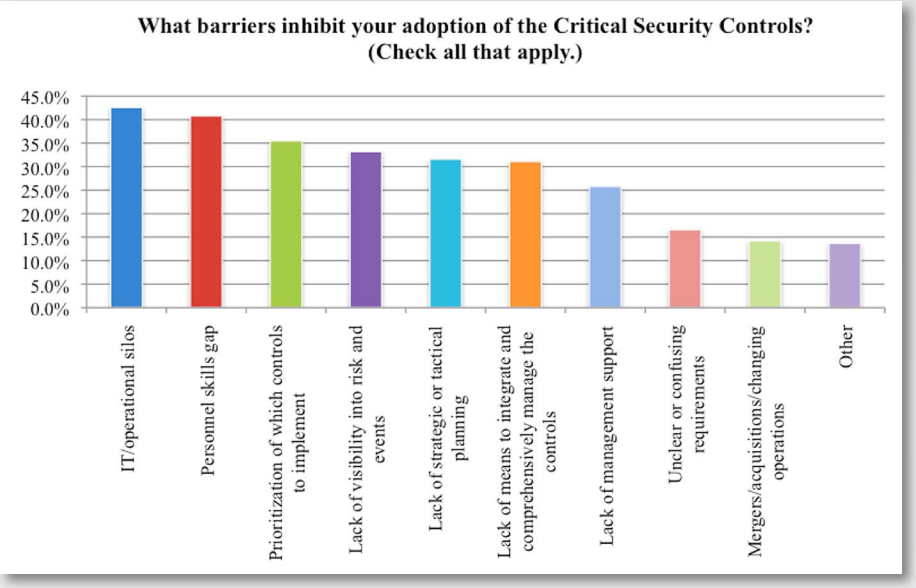

Figure 7. Barriers to Adopting the Critical Security Controls

Many of the CSCs either are aimed at mitigating IT operations deficiencies (for example, configuration management, patch management and privilege management) or require integration with IT operations processes and systems (such as inventory, application development and need-to-know access). In order for security improvements to be made, security and IT operations must work together and have integrated processes.

The third most frequently cited barrier to adoption is the inability to prioritize which of the Controls to implement first. This might seem surprising, because the CSCs are numbered in attack mitigation priority order. However, the concern over prioritization highlights the fact that very few of the Controls actually stand alone: There are relationships between individual Controls, between Controls and other compliance drivers and between groups of the Controls—all constricted by the demands of legacy systems and limited budgets. These interactions are unique to each company and require individual prioritization efforts.

The perceived lack of planning or management capabilities was also highly cited. This is a common problem with any attempt at change; organizations may have great implementation skills, but without planning strength and management systems, they calcify and find change difficult. It becomes much easier for them to focus on repeating the same compliance processes, even if those processes are not effective.

> ***Takeaway:*** *The best way to fight resistance to change is to gain high-level management support. Almost 55% of respondents indicated they have CIO awareness and support for the CSCs, and 32% have awareness at the CEO/COO level. Only 25% reported lack of that support as a problem, so CISOs should prioritize and leverage this high level of visibility to accelerate implementation of the controls.*

Assessment: Identifying the Gaps

Organizations would see significant benefits from starting with an initial gap assessment—because knowing which Controls to start with is perceived as such a barrier—and then looking at implementing the Controls in risk-prioritized order. The survey asked the respondents how they performed an initial gap assessment. Of those who answered this question, only 13% have not performed gap assessments at all. The remainder reported that they were conducting gap assessments. Their responses, however, show a heavy reliance on manual processes for assessing the gaps between the current state of security and the Controls, as shown in Figure 8.

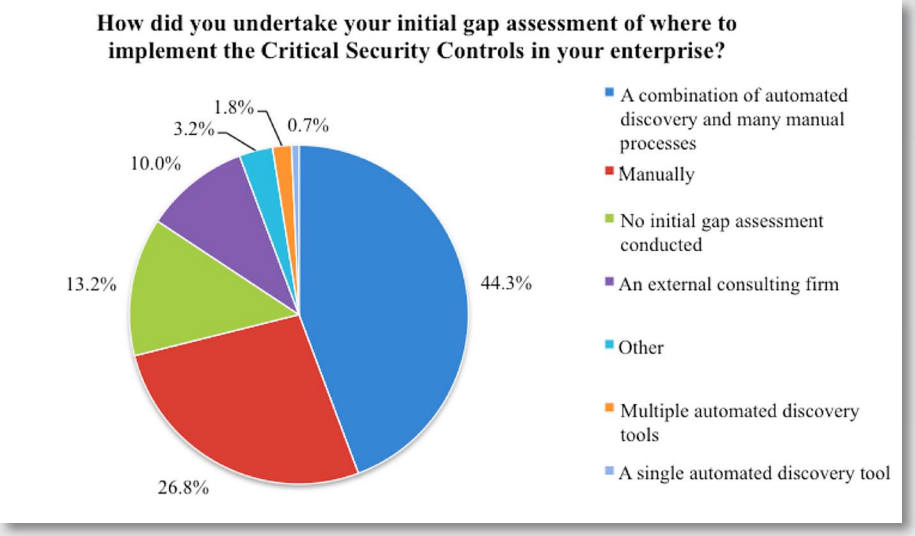

Figure 8. Means of Performing Initial Gap Assessments

Fewer than 3% of the respondents rely solely on automated tools, 27% are using only manual processes and 44% are using a combination of automated and manual tools—which means that more than 73% are relying heavily on manual processes. There is a "Catch 22" effect at work here: Until an organization has mature security processes, it won't be able to automate those processes using automated tools. However, without focusing on updating and automating the key threat-facing processes, organizations are often consumed with day-to-day "firefighting" and don't have the time or resources to focus on process maturity.

It ultimately comes down to resources. No security organization can just let existing "fires" burn in order to improve processes—both tasks have to be tackled at the same time. This invariably requires increased effort, which requires approval from management. Obtaining this approval requires that the security organization convince management that there's a problem that impacts the business and then demonstrate that the increased investment of resources will solve the problem in a cost-effective manner.

A traditional way around the first part of this problem is to use external consultancies to perform the gap assessment, but the survey results show that only 10% of the respondents have done so. This most likely reflects two factors: Budget concerns during the period of economic uncertainty leading up to the survey prevented many organizations from using outside consultants (SANS estimates that typically 25% of enterprises routinely use external consultancies for security assessments), and much of the community effort around the CSCs has come from end-user organizations and not from security services providers. In the first months of 2013, at SANS events and in other discussions, we have seen growth in consultancies focusing on the CSCs.

> ***Takeaway:*** *Organizations that have not conducted gap assessments, or have only ad hoc processes for doing so, should look to external consultancies that have embraced the CSCs (see* ***www.sans.org/critical-security-controls/vendor-solutions****). The engagement deliverables should include recommendations for automated tools for future self-assessment.*

The second part of this problem will be addressed in the "Measurements and Metrics" section of this paper.

Levels of Adoption

A key goal of the survey was to determine where enterprises were in planning and implementing the CSCs.

Implementation Roadmaps

A large percentage of respondents have plans to adopt the Controls, and about 54% have some form of implementation roadmap in place. Only 18% have a complete roadmap, 27% have some parts of a roadmap defined and 9% are focusing on one or two Control areas in their roadmaps, as illustrated in Figure 9.

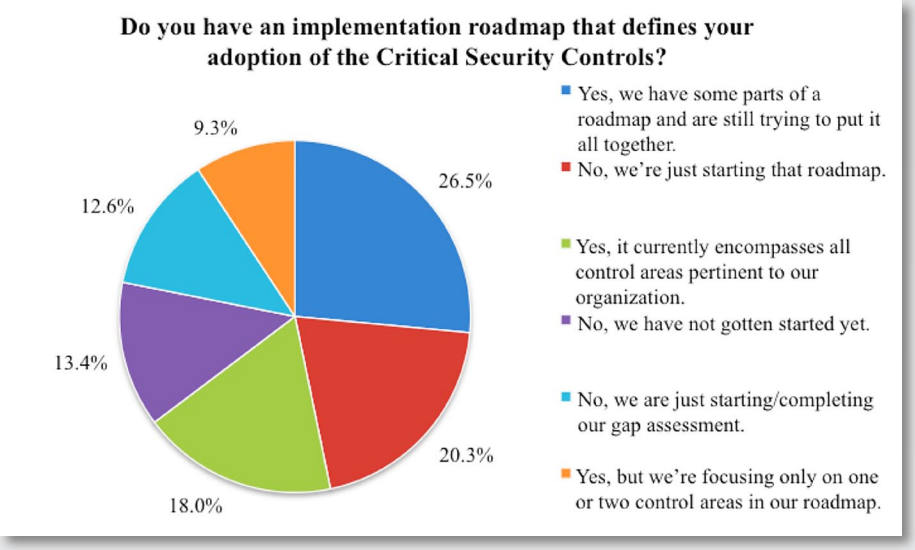

Figure 9. Use of Roadmaps for CSC Implementation

In keeping with the prioritized "secure a little, test a little" approach that drives the CSC effort, we don't expect more than 25–30% of enterprises to ever complete a formal roadmap. The majority will focus their efforts on near-term implementations of the highest-priority Controls and on upgrading existing implementations of some of the lower-level Controls. Roadmap efforts will be focused on the remaining Controls and longer-term efforts where upgrading security controls will be tied to IT infrastructure upgrades and transitions.

The 13% of respondents who have not yet started to develop a roadmap will likely remain in the range of enterprises that will never formally put one together. Many of the remaining respondents who indicated that they are just starting are likely to require external consultancy support or additional personnel to begin developing a roadmap.

When respondents were asked whether they've actually implemented Controls, 22% of them indicated they have not implemented any of the Controls. Because the CSCs essentially represent a basic level of security "hygiene" to mitigate targeted threats, it would be deeply troubling if more than one out of five enterprises hadn't implemented any of the Controls. However, other industry figures and anecdotal evidence show that, for example, border defense and firewall penetration is above 95%. Other long-form responses suggest that survey respondents were likely commenting on the low levels of effectiveness of their existing Controls as opposed to a complete lack.

> ***Takeaway:*** *Most enterprises should prioritize first upgrading or enhancing existing Controls to address identified threats in the short term and then move on to formal roadmaps.*
>
> *An enterprise that really hasn't implemented* any *vulnerability assessment, antimalware or border defense should find Control 18 (Incident Response and Management) a good starting point—because its network has likely already been compromised.*

Controls Being Implemented Now

A mature security program using the CSCs would have policy, automation and centralized management integrating all 20 Controls into all other elements of security. In another survey question concerning maturation of implementations, less than 10% of the respondents reported having reached this level across all Controls, but more than one-third reported having reached that level for some of the Controls (most likely the ones we call "Mature" and "Evolving" controls in a question later in the survey.) Less than one-third of respondents stated that "only a few" of their Controls are at the mature state, and these are most likely only the Mature Controls, such as desktop antimalware and border defense.

Just over 20% of the respondents indicated that they're working on policy but haven't yet reached the implementation stage for any of the Controls. This may indicate the phenomenon that is sometimes called "paralysis by analysis," because none of the Controls requires any major changes to typical existing security policies.

Table 1 provides a ranking of the Controls survey respondents are already deploying—either as partial or full implementations.

Control	Partial	Full	Total	Weighted
Malware defenses	122	**126**	248	500
Boundary defense	99	**125**	224	474
Data recovery capability	115	**107**	222	436
Secure configurations for network devices such as firewalls, routers, and switches	119	**104**	223	431
Controlled use of administrative privileges	131	**92**	223	407
Limitation/control of network ports, protocols and services	127	**88**	215	391
Inventory of authorized and unauthorized devices	172	**71**	243	385
Continuous vulnerability assessment and remediation	136	**82**	218	382
Incident response and management	121	**86**	207	379
Wireless device control	119	**83**	202	368
Secure configurations for hardware and software and mobile devices, laptops, workstations, and servers	156	**68**	224	360
Controlled access based on the need to know	136	**72**	208	352
Inventory of authorized and unauthorized software	168	**61**	229	351
Account monitoring and control	137	**66**	203	335
Secure network engineering	123	**67**	190	324
Maintenance, monitoring, and analysis of audit logs	144	**53**	197	303
Data loss prevention (DLP)	121	**54**	175	283
Penetration tests and red team exercises	129	**49**	178	276
Application software security	146	**37**	183	257
Security skills assessment and appropriate training to fill gaps	134	**38**	172	248

Table 1. Critical Security Controls Deployed

By weighting full deployment at three times partial deployment ("Weighted") and then looking at the ratio of full to partial, we broke the implementation level of the Controls down into different segments:

- **Mature controls.** Antimalware, boundary defense and data recovery show up with higher levels of complete implementations. This isn't surprising, because antivirus tools, firewalls and business continuity/disaster recovery/continuity of operations (BC/DR/COOP) are the most mature areas of security. Note that nearly half of the answers on malware cited only partial deployment, which doesn't align with the market realities that more than 95% of desktops and more than 90% of email servers have antivirus software installed. With so many enterprises indicating a partial deployment for antimalware tools, enterprises may be recognizing that advanced threat detection techniques are needed to augment traditional signature-centric approaches. Similar responses around data recovery likely represent movement toward cloud-based recovery capabilities as a way of reducing costs and addressing mobility.

- **Evolving controls.** Controls such as those for controlling administrative privileges, limiting ports, vulnerability assessment, inventory and account monitoring are basic security configuration practices. However, these Controls show only medium levels of full adoption and high levels of partial adoption. This result reflects the dynamic threat and vulnerability environment, as well as the impact that bring your own device (BYOD) policies and the use of the cloud have had on how IT and security organizations try to implement these Controls. Anecdotal evidence suggests that many enterprises have begun to realize that vulnerability scanning on a quarterly basis, done in isolation from other security processes, does not even come close to "continuous vulnerability monitoring," which leads to upgrades and improvements.

- **Immature controls.** Controls like log monitoring, data loss prevention (DLP), penetration testing and application security show low levels of full adoption and medium levels of partial adoption. These are areas in which enterprises have frequently made investments, found the first generation of products to be overhyped and often abandoned them. (Common examples are security information and event management [SIEM] and DLP.) Another scenario may be that an enterprise did not have the trained personnel to implement products (such as application security and pen testing tools) and resorted to sporadic use of consultancies for assessments.

> ***Takeaway:*** *Enhancing existing implementation of Mature and Evolving Controls likely represents the most effective and efficient approach to increase resistance to current advanced threats. But they're not the only controls needed to reduce risk and automate security processes. The Controls listed as Immature can provide very high payback, but may require training of security staff or the use of external professional services to ensure adequate return.*

Implementation Progress and Experience

One of the most effective and efficient ways to implement the CSCs is to integrate them with existing operational practices, such as configuration and asset management. However, almost 80% of the survey respondents indicated that they are focusing on the Controls that make the most sense, while the next-largest group, at 52%, is conducting outreach to other business groups to integrate the management of the Controls into existing IT and security operations. (Note that respondents were allowed to choose "All that apply" for this question.) Only 21% said they are actively developing connectors to other programs or processes, as shown in Figure 10.

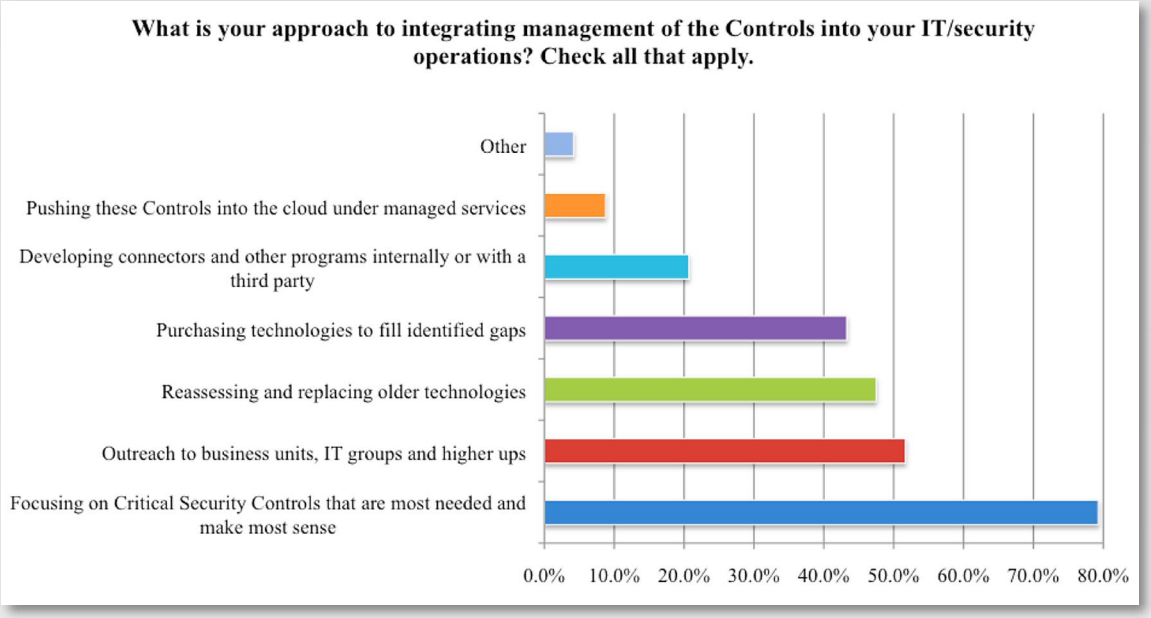

Figure 10. Level of Controls Integration

To gain long-term security benefit from the Controls, integration into formal repeatable business and IT processes is critical. More than half of the respondents reported that they have made some effort to reach out to other groups, and this should lead to higher levels of integration in the future.

Security organizations are also taking advantages of technology refresh cycles (47%) and identified gaps (43%), all of which can be used to justify investment in technologies to implement the CSCs. Less than 10% of the survey respondents indicated that they are using managed security service providers (MSSPs) to monitor CSCs, indicating that they do not yet consider the CSC effort routine enough or mature enough to outsource. We believe this will change rapidly over the next few years, as MSSPs begin to map their service offerings to the CSCs, especially for mature Controls such as advanced boundary defense and antimalware.

> ***Takeaway:*** *Implementing the CSCs can deliver immediate benefits, but repeatable, reliable long-term benefits will require integration into business, IT and security management processes.*

Tools to Manage

Figure 11 indicates the systems the survey respondents cited as already in place to manage Control areas, along with the level of update or addition to capabilities needed to manage the Controls.

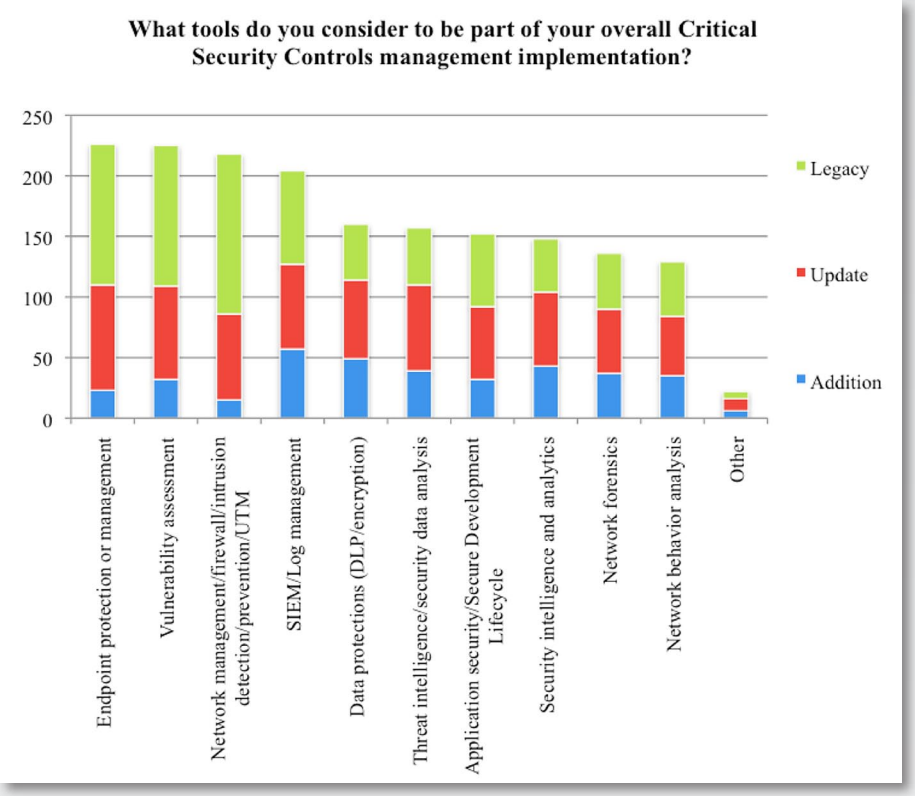

Figure 11. Tools Used to Manage Critical Control Areas

Boundary defense, endpoint protection and vulnerability assessment showed the lowest levels of enhancement, as well as high legacy levels. SIEM/log management and application security were reported at significantly lower legacy levels, and both showed high levels of updating needed. Many enterprises focused their initial SIEM deployments on compliance-driven reporting, and these deployments likely aren't scalable enough to support enterprisewide continuous monitoring and security analytics. Similarly, secure development life cycles put in place for traditional client/server apps often break when the application developers' focus moves to mobile and cloud-based apps that require more rapid development cycles.

Security intelligence and analytics, data protection and network behavior analysis came in at much lower legacy levels, with even higher levels of update and addition, indicating that these are the least mature areas overall.

> ***Takeaway:*** *Enterprises are planning to take advantage of near-term opportunities to upgrade SIEM and application security capabilities as part of their efforts to deploy the CSCs. More advanced capabilities, such as security analytics, DLP, network behavior analysis and network forensics, represent longer-term initiatives.*

Measurement and Metrics

In at least one respect, the world of the CSCs is not very different from the broader security world: Spreadsheets still dominate as the reporting and analysis tool of choice, according to the survey responses. However, commercial reporting tools were the next most frequently cited, and were the highest reported as being planned for use in the next 12 months, as shown in Figure 12.

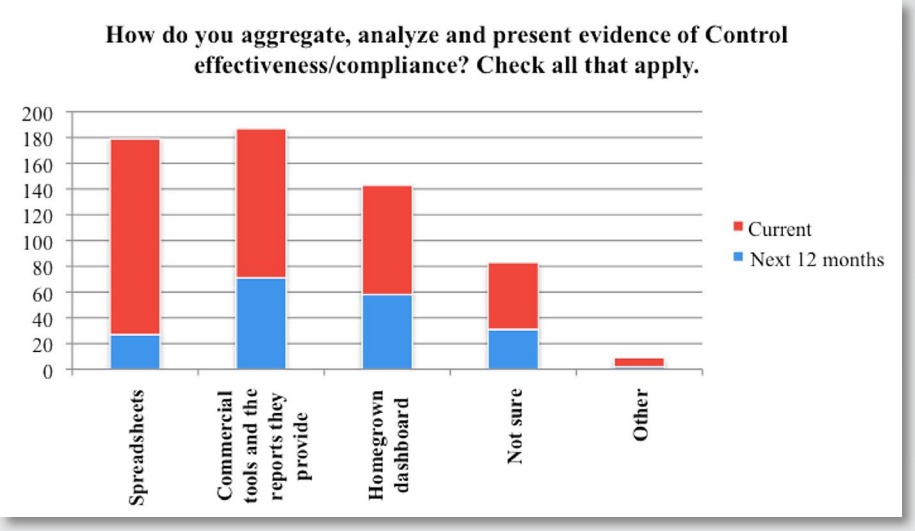

Figure 12. Type of Reporting

Homegrown dashboards were the next most frequent choice for the next 12 months, at almost twice the level of spreadsheets.

> ***Takeaway:*** *As implementations of the CSCs mature, demand for commercial reporting tools and dashboards will grow.*

Systemic Improvements: The Ultimate Goal

The goal for implementing the Critical Security Controls is systemic improvement through assessment, remediation and improved/streamlined system defenses—and the documentation of these improvements then used to satisfy compliance reporting requirements.

Security managers have historically reported that what they do reduces risks, but have had problems quantifying that reduction. That trend continues here, with almost 80% of the survey respondents who have implemented the Controls believing they have reduced risk, but less than 25% able to quantify that improvement in risk posture. The rest were uncertain (13%) or didn't quantify their security postures (8%).

When asked about specific improvements and benefits derived from the Controls they have implemented so far, respondents cited risk reduction, improvements to risk posture and improved situational awareness as their most important benefits (see Figure 13).

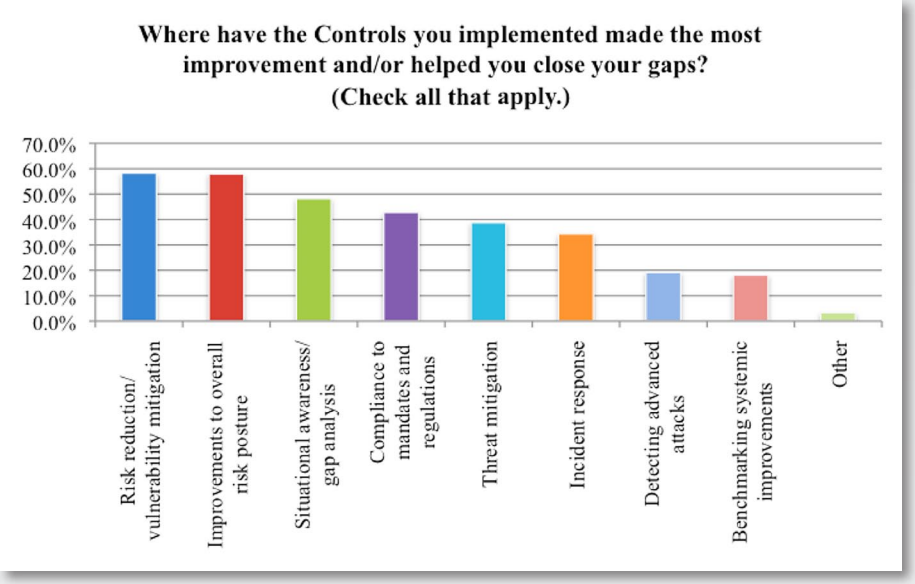

Figure 13. Benefits of Controls Implemented

These results reflect, once again, a strong belief that a major benefit of the CSCs lies in risk reduction (58%) and improvements to overall risk posture (even though only 24% could quantify this, as shown in the preceding section). Compliance benefits ranked slightly higher than those from threat mitigation.

As an example of comparative costs of CSC-related risk reduction, SANS recently looked at a recent security incident, where Idaho State University was fined $400K by the Department of HHS for not noticing firewall policy changes that resulted in the potential exposure of personal health information for 17,500 patients.[4] We estimated the overall cost of that incident as roughly $2M, whereas the implementation of a single CSC (Critical Security Control 10: Secure Configurations for Firewalls, Routers, and Switches), at an estimated cost of $75,000, would have avoided the incident and attendant costs.

> ***Takeaway:*** *One of the major benefits of mature use of the CSCs is that it allows auditors to focus their compliance monitoring efforts on those Controls that have the most impact in terms of vulnerability reduction and threat mitigation. The survey results show that the respondents appear to be achieving that synergy.*

Enhancing the Value of the CSCs

The last question in the survey allowed for free-form answers, and 123 respondents took the time to give their suggestions on how to improve the CSC effort. Most of their responses concerned benchmarking, making the Controls interactive and adding the ability to map to other requirements, such as the U.S. Federal Information Security Management Act (FISMA). Other respondents asked for better statistical interfaces and more real-life case studies involving the Controls. (More case studies do exist, and they're being added to the SANS Reading Room.)[5,6]

Here are some of the most commonly cited responses:

1. Show benchmarks and metrics of successful CSC implementations.
2. Provide more information on case studies and best practices around implementation and operation.
3. Show links to and integration with other compliance regimes and security frameworks.
4. Provide more information on products, tools, and templates that help implement the CSCs.
5. Show dashboards used for ongoing monitoring of effectiveness of the Controls.
6. Provide tailored versions of the Controls for different verticals, different business priorities, etc.

SANS is also mapping the Controls to tools in a poster that it updates annually.[7] And, some vendors are developing tools that include compliance components for the CSCs, as well as compliance modules they already include (for example, for FISMA and the Sarbanes-Oxley Act). They should also be integrating dashboard reports and tailored versions based on industry verticals.

> ***Takeaway:*** *Organizations are addressing many of the Controls by developing tools and middleware for their own uses. However, tool vendors are also integrating more functionality and templates into their products. SANS hopes that in 2014, when this survey is revisited, more of these tools and metrics will be in place.*

4 www.sans.org/security-trends/2013/05/30/analyzing-the-cost-of-a-hipaa-related-breach-through-the-lens-of-the-critical-security-controls
5 www.sans.org/reading_room/analysts_program/implementing-critical-security-controls.pdf
6 www.sans.org/reading_room/analysts_program/mcAfee_next_generation.pdf
7 www.sans.org/critical-security-controls/spring-2013-poster.pdf

Conclusion

The survey results show that the CSCs have quickly reached a high level of visibility and, crucially, have attention and support at high levels within enterprises.

There are many partial CSC implementation efforts currently under way. Many of those efforts focus on upgrading earlier implementations of mature security controls, such as border defenses, endpoint protection and vulnerability assessment tools, to make them more effective against advanced threats. Other areas, such as SIEM, antimalware and application security, require investments in new skills or new products to reduce the likelihood of breaches.

Enterprises are looking at more advanced technologies as well, but they are assigning high priority to more visibility into successful implementations of the CSCs and effective benchmarks and metrics to measure and demonstrate benefit. Because the CSC effort is community driven, SANS believes we will see increased information sharing across the CSC community of products that work, processes that scale, awareness approaches that do change behavior and metrics that *do* demonstrate to management the return on investment provided by implementing the CSCs.

Within that broad community, we also expect to see vertical-specific tailoring of the priority of Controls and of the ways to overcome barriers to adoption. There are already vibrant vertical efforts in federal and state government and industrial applications, and growing efforts in the health care and retail industries.

Compliance regimes are invariably rigid, top-down structures, whereas the CSC effort is purposely bottom-up and is continually being updated. While that has obvious benefits, it also relies on a community effort to succeed. This survey shows that that the required community effort is under way and is already beginning to drive changes.

SANS and the survey sponsors invite you to participate in the continuing process.

7 www.sans.org/critical-security-controls/winter-2012-poster.pdf

About the Author

John Pescatore joined SANS in January 2013, with 35 years of experience in computer, network and information security. He was Gartner's lead security analyst for more than 13 years, working with global 5000 corporations, government agencies and major technology and service providers. In 2008, he was named one of the top 15 most influential people in security and has testified before Congress on cybersecurity.

Prior to joining Gartner Inc. in 1999, John was senior consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and public key infrastructures. Prior to that, he spent 11 years with GTE developing secure computing and telecommunications systems. In 1985 he won a GTE-wide Warner Technical Achievement award.

John began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems—and the occasional ballistic armor installation. He holds a bachelor's degree in electrical engineering from the University of Connecticut and is an NSA-certified cryptologic engineer. He is an Extra class amateur radio operator, callsign K3TN.

SANS would like to thank this survey's sponsors:

FireEye™

IBM®

Symantec™

tenable network security

Simplified Security Intelligence