Sponsored by Tripwire

Implementing the Critical Security Controls

April 2013

A SANS Whitepaper

Written by Jim D. Hietala

What Are the Critical Security Controls? *PAGE 2*

Implementing the Critical Security Controls *PAGE 3*

Two Real-World CSC Implementations *PAGE 4*

Commonalities and Conclusions *PAGE 9*

Introduction

Since the SANS Institute hosted the first version of the Critical Security Controls (CSC) in 2008, the controls have been upgraded four times to meet demands of an evolving threat and vulnerability landscape. During that time, the Department of Homeland Security essentially made the CSCs a de facto standard to be followed by its branches. Canadian and other international authorities are also using these controls as guidelines to support their own cybersecurity policies, and so, too, are private-sector organizations with the most to lose, such as those in the infrastructure and financial fields.

The question is: Just how do you implement the CSCs, and how do you scale them to meet the demands of today and tomorrow? Few case studies have examined this implementation; a 2010 U.S. Department of State **case study** described large development efforts that most federal and private-sector organizations can't fit in their budgets.[1]

Over time, the guidance in the CSCs has evolved to add detailed information on metrics for measuring effectiveness, implementation, automation and control test procedures, as well as "quick wins" suggestions. Through this guidance, organizations can begin to implement the controls in a way that illuminates their areas of vulnerability and ultimately improves their risk ratings, while making their networks more resilient to attacks.

This paper serves as a how-to for organizations in various stages of implementing the controls and offers two real-world examples of CSC adoption. The case studies are based on real-time interviews with the people behind the efforts and includes the security environments before the implementation, the challenges experienced in adopting the controls and the benefits they've experienced.

1 www.state.gov/documents/organization/156865.pdf

What Are the Critical Security Controls?

Before we dive into the "how," let's start with a brief description of the controls. Work on the **Critical Security Controls** (originally called the Consensus Audit Guidelines) resulted in the initial publication of a set of security controls that were judged by experts from both government and the private sector as being the most critical controls in preventing cyber attacks. The controls were initially published by the Center for Strategic and International Studies, and are now maintained and published by SANS with input from a large community of government and private-sector organizations.[2]

These controls cover network and endpoint devices, their applications and the vulnerabilities therein. They also cover malware defense, controlled access and recovery, as well as data protections.

Figure 1: The Critical Security Controls

The core tenet of these controls is that through automation and integration of controls already in place in many organizations, and by adding some new technologies and practices, organizations can deploy data networks that are more resistant and resilient when attacked.

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

Implementing the Critical Security Controls

The two case study examples examined later in this paper demonstrate that, for large enterprises with significant IT investment, getting value from the CSCs doesn't necessarily mean implementing all 20 controls at once. Few organizations have the capital budget, people resources and organizational bandwidth to do a simultaneous, wholesale implementation of all CSCs. A more pragmatic approach to implementing the controls includes these steps:

1. **Discover your information assets and estimate their value; think through potential attacks against those assets (including initial entry points, spread, system damage or exfiltration) and the potential impact. Begin by prioritizing controls around the most risky assets.**
2. **Assess the organization's current state of information security controls as compared to the CSCs. Make note of each control area needing work, including: where no security capabilities exist, where some work has been done and what that work is, the level of maturity for the control area, and integration paths with other associated controls. Also, map mature security control implementations and reuse successful components across your architecture.**
3. **Map the gaps between the organization's as-is state and the individual controls. Knowing what your vulnerabilities are is a critical first step in closing the gaps. Vulnerability assessment tools can create a list of vulnerabilities, but the key to success is combining the output of the assessment exercise in the preceding step with the value and loss risk analysis from the first step. This level of assessment should provide the organization with necessary visibility into the risks that exist at the present time so decision makers can appropriately prioritize the measures adopted in support of the controls.**
4. **Fill the priority gaps first and focus on remedies that you can achieve in the short term. Multiple factors go into prioritization, including where the most risk is perceived, and to some degree, where the most security improvement can be achieved at the lowest cost. This will be a little different for every organization and will depend on the organization's culture as well as the "as-is" state of procedures and automation already in place. Some choices may be driven by high-priority risks, others by stretching limited resources and leveraging existing or low-cost tools to make progress.**
5. **Obtain management buy-in for the plan, and form line-of-business commitments for necessary financial and people support.**
6. **Implement the controls, leveraging existing security tools, and integrate and automate as many tasks as possible, keeping an eye on trends that add new risk to the enterprise.**
7. **Measure progress, risk reduction and metrics, and communicate their status.**
8. **Build a long-term plan of attack for adding coverage of other controls.**

A well-thought-out plan for assessing current security deficiencies, adopting key new security controls and improving on the operational effectiveness of existing security controls should appeal to senior management. The CSC framework can provide an organization with a set of independently-developed best practices that should be integrated over time—but not too much time, given the continued improvements attackers are adding to their tools to thwart our current, often-fragmented security implementations.

Two Real-World CSC Implementations

Although every organization will have its own reasons for adopting a framework of security controls, many will share common challenges, such as budget constraints and the need for executive buy-in. The below case studies lay out pragmatic approaches to adopting the CSCs, which promise to deliver the best results while creating the least fuss.

The City of Portland (Oregon): Regulatory Compliance a Key Driver in Adopting Controls in Stages

Logan Kleier heads IT security for the City of Portland, Oregon, reporting to the CTO and leading a team in the Bureau of Technology Services. The bureau provides central IT services to more than 20 city "lines of business," including the fire department, housing, law enforcement, parks and recreation, and other bureaus and departments. Kleier leads a team of four analyst/engineers that provides support for firewalls, VPN, antivirus, configuration management and other operational security services. Across all its branches, the city has more than 6,000 employees, more than 6,000 endpoints and 350 servers.

Pre-CSC Environment

Portland's IT security had been haphazard and reactive, taking an ad hoc approach and not accomplishing much. There was little in the way of systematic thinking about what security projects to tackle, and why, and there was no long-term plan for securing the organization. The city's various departments are subject to various compliance regimes and standards based on their lines of business, including the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

Challenges

The IT security challenges facing Kleier's team were numerous. Among them:

- **Engaging other staff throughout the city's many departments, training them to recognize and deal with security risks**
- **Finding people suitable for the role of central IT security**
- **Obtaining budget for security projects**

It was clear to Kleier that adopting a security framework or control set that could apply across the entirety of the city's IT simply wasn't meant to be. Besides being constrained in terms of capital expenditures for new security controls, the city was also limited from a people/management resource perspective.

Portland's Timeline for Implementation of the CSCs

2011

Critical Control 5: Malware Defenses

2012

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers (focused on Windows systems)

Critical Control 12: Controlled Use of Administrative Privileges (migration of desktop users to standard user privileges instead of local administrator privileges)

2013

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers (focused on AIX systems)

To meet regulatory requirements, the city's IT group was granted budget for initial work in vulnerability management, regular penetration tests and wireless security. These first-round projects, and the funding, tools and processes that they brought with them, helped improve security and provided a jump-start on related critical controls.

Why the Critical Security Controls?

The city briefly considered using the PCI DSS control set across the entirety of its IT systems, but quickly realized that this wasn't a good approach. PCI DSS controls are optimized for protecting cardholder data, and many of these controls either don't apply beyond the scope of credit card data or are too expensive to be broadly applied.

Upon learning about the CSCs, Kleier felt the approach made sense and that the CSC framework could be leveraged to improve the security posture of his organization. His assessment was that the controls' structure would allow him to target those areas in greatest need of remediation and leverage "quick wins" to realize significant security posture improvements with minimal effort.

Kleier brought the controls to his CTO for executive buy-in. The CSCs provided Kleier with a structure for defining benefits, and he used these to show how these benefits would offset costs and add value over time. Kleier and his team determined that the savings in capital and human resources could fund implementation of two new controls per year.

In deciding which controls would first be implemented, the team considered a number of factors, including the cost/benefit ratio for each control. The team focused on so-called "low-hanging fruit." These were controls that had a low cost and were "low drag" in terms of people resources while providing real risk reduction. This approach leveraged those areas where some tools were already in use. Some examples of these "quick wins" include:

- **Making it standard for Windows users to run with ordinary user privileges on their PCs and revoking local administrator privileges wherever appropriate (Critical Control 12).**
- **Deploying standard configurations from gold master images (Critical Control 3). With Microsoft Security Compliance Manager already deployed and in use, Kleier's team leveraged Active Directory's Group Policy Objects (GPO) feature to implement this capability.**
- **Implementing regular and frequent patching for all core applications, and extended patching to include Adobe Flash, Adobe Reader and Oracle Java (Critical Control 3).**
- **Centralized antivirus for all endpoint computing devices (Critical Control 5).**

Benefits of Implementing the Critical Security Controls

The city's IT security posture has measurably improved since the initial adoption of the CSC framework. The pluses so far:

1. **The security team saw fewer hits or incidents of endpoints being infected, a visible indicator that security is improving for the city. Kleier attributes this to the progress made across the city government in limiting administrative privileges and making frequency and coverage improvements in patching.**
2. **Another indicator of improvement comes in the form of fewer trouble tickets being issued for configuration issues. The city now uses standard images for desktops and servers, and ensures policy conformance through the directory service. Although this result may not be a direct benefit to security, it helps the IT organization focus on higher-value tasks, such as improving the security posture, and demonstrates to the user community that security and stability go together.**
3. **The biggest benefits Kleier found while adopting the CSCs came in the form of additional structure for the information security program and a framework for planning additional projects and measuring progress.**
4. **A more subtle benefit of adopting the CSCs is the acceptance of a common vocabulary throughout the IT organization, as seen once again in the adoption of Active Directory GPOs. Before Kleier's team began its work, Group Policy wasn't commonly used in the city's IT environment, but by using it to implement the CSCs, staff members now grasp the feature's benefits.**
5. **As the security vocabulary is accepted, operations and business groups are more readily embracing security enhancements. Staff can understand the goals of each of the CSCs and how security will improve when they are adopted.**

It's also worth noting that for some new controls, the barrier to adopting them was more a matter of management resources, rather than capital expenditure for new tools. For example, as the IT security team considered implementing application whitelisting, the key issues turned out to be who would determine policy, who would pay attention to what applications would be authorized and how exceptions would be managed. It became clear that embracing application whitelisting would lead to new staffing requirements. The same turned out to be true of a Network Access Control (NAC) project that was abandoned due to staffing concerns and resource issues. In both cases, the city's help desk/end user support resources were already maxed out, and it wasn't clear how the city would afford the staff required to fully deliver the benefits of either control.

Bankia: How a Financial Conglomerate Used the Controls in Support of a Merger

Bankia is a Spanish financial conglomerate, headquartered in Madrid. Security consultant Vicente Aceituno was the project leader responsible for implementing the Information Security Management System (ISMS) at Bankia, which was formed in 2011 from a merger of seven Spanish banks, including Spain's oldest bank, CajaMadrid. Well before the merger, CajaMadrid began implementation of O-ISM3 (**Open Information Security Management Maturity Model, an ISMS standard**)[3] as an information security management system, starting its effort in 2009. At roughly the same time, Aceituno began working with CajaMadrid's then-CIO Miguel Ange Navarrete to bring a new approach to the bank's information security management. Their initial security control project involved vulnerability management (addressed by Critical Control 4 and O-ISM3 process OSP-19, Internal Technical Audit).

Pre-CSC Environment

Rather than attempt a top-down approach and build an entirely new ISMS for Bankia, Aceituno and Navarrete opted for a bottom-up approach, starting with vulnerability management. O-ISM3 provided the initial framework for measuring the vulnerability of the bank's web applications and remediation of any weaknesses, and for focusing web application development managers on the goal of continuous improvement.

Challenges

Before the O-ISM3 implementation, Bankia's vulnerability management efforts attempted to test new applications before putting them into production and then relied on subsequent scans performed at irregular intervals to detect flaws. No success criteria or metrics had been defined for vulnerability assessment or remediation efforts. The bank had no way to continuously improve its vulnerability management program because it did not capture metrics.

The team started with its web applications, which the bank considers to be highly critical, both for customer business and because web applications have become a primary attack vector. For these applications, vulnerability management represented "low-hanging fruit" in which the bank would get the most return on its investment in improving its security posture.

Finally, the bank also needed a consistent terminology for the security program, specifically in the area of vulnerability management. O-ISM3 provided Bankia with the framework to:

- **Establish goals and objectives**
- **Measure activity**
- **Define success criteria**
- **Manage vulnerability scanning and remediation toward continuous improvement**

3 www.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12238

Why the Critical Security Controls?

As Bankia's approach to managing vulnerabilities matured, its IT group focused on the CSCs, in particular Critical Control 4, Continuous Vulnerability Assessment and Remediation. Exploring Critical Control 4 in more detail, Aceituno and Navarrete realized that the how-to guidance it provided would add valuable practitioner detail to the knowledge-management aspects of the bank's vulnerability management program.

The guidance in Critical Control 4 included "quick wins" and configuration and hygiene details that could show immediate results. In addition to providing direction, Critical Control 4's metrics for success gave all the detail that the bank's ISMS required for its measurement and continuous improvement functions. As an even greater bonus, the control test guidance for Critical Control 4 was useful for the bank in validating control effectiveness over time.

Benefits of Implementing the Critical Security Controls

Bankia was able to add the additional guidance and metrics from Critical Control 4 to the existing O-ISM3–based vulnerability management program, with impressive results in outcomes:

- **Significantly more vulnerabilities were discovered and fixed**
- **Web applications checks now occur much more frequently**
- **Staff hours spent manually scanning applications are significantly reduced**
- **Fewer costs in dealing with vulnerabilities discovered**
- **Streamlined repair of vulnerabilities**
- **Less cost and overhead with managing web applications**
- **More applications are repaired, reducing the attack surface dramatically**

Large IT organizations have to respond to many needs and business requirements. Security is a critical requirement, but it is far from being the only important issue that IT organizations have to deal with, or even the most important one. In the real world where most CIOs operate, budgets are limited and other obstacles to change have to be managed when they can't be eliminated.

Commonalities and Conclusions

In both of these case studies, organizations had limited budgets with which to tackle new security projects and were able to leverage existing investment in security and IT systems management tools. They were able to make improvements in coverage, operational guidance, metrics and measurement to fully realize the security benefits of each control.

The organizations also faced common challenges in obtaining commitments from the business to provide the people resources needed to operate new security projects.

Both adopters were also seeking organizational principles and structure for their information security programs. These case studies show that some organizations are beyond the phase of merely figuring out the best way to implement a specific control and are implementing a systematic, programmatic approach to developing a security program. An important part of this effort is the acceptance of a standard terminology, brought about by adoption of the Critical Security Controls.

As both organizations implemented the CSCs, they employed a pragmatic approach that's somewhere between a risk-based method and a best-practices ideology. Although debates in the security industry treat these approaches as mutually exclusive, these case studies describe a practical synthesis of these extremes, where risks are assessed and evaluated by their immediate threat. In the real world, a "do-what-works" effort to control selection and implementation leads to quick wins and allows the achievement of measurable improvements in overall security posture.

About the Author

Jim D. Hietala, GIAC GSEC and CISSP, heads security standards activities for a major IT industry standards group. He has led the development of a number of IT security standards. Jim is an active participant in the articles on information security, risk and compliance topics in publications including the Risk Factor, Bank Accounting & Finance, SC Magazine and others. A security industry veteran, he has held leadership roles at a number of security technology startups. He holds a B.S. in marketing from Southern Illinois University.

SANS would like to thank its sponsor: