Global Information Assurance Certification Paper

Planning, Budgeting and Communicating the Critical Security Controls Implementation

GIAC (GCCC) Gold Certification

Author: Paul Hershberger, pjhersh@gmail.com

Advisor: Chris Walker

Accepted: January 13, 2016

Abstract

Cyber security fills the headlines with reports of data breaches and cyber attacks from all corners of the globe. Board rooms and executive management are more aware of the need for effective Cybersecurity today then they every have been. This awareness is driving action as many organizations look to frameworks for guidance on building effective security programs. The Critical Security Controls provides a Cybersecurity controls-based framework designed to directly address the actions attackers are taking. Creating a plan and gaining support for implementing a security program based on a control framework can be a daunting task. This paper will discuss a method for using the Critical Security Controls framework in conjunction with the NIST Cybersecurity framework to plan, budget and communicate the implementation project to senior executives.

Introduction

In 2008, the National Security Agency (NSA) initiated an effort to prioritize the controls within the multiple frameworks to identify a manageable set of controls that are effective in implementing a Cybersecurity program with an "offense must inform defense" approach designed to directly address how attacks happen. The initiative led to the publishing of Critical Security Controls (CSCs). The CSCs are maintained by the Council on Cyber Security (Council on CyberSecurity, 2014). The Council on Cybersecurity provides resources and guidance on the tactical aspects of how to implement the CSCs, including the most impactful controls to implement and quick wins designed to have immediate impact on disrupting attack cycles. Although the information available to guide a CSCs implementation is extensive and well documented, the start of every CSCs implementation effort is the Cybersecurity strategic plan and budget. Planning and budgeting initiatives are typically far removed from the tactical levels of detail contained within the CSCs implementation guidance. A key challenge for security professionals is the ability to gain support in the form of budget to support the people, processes and technology necessary to implement an effective Cybersecurity strategy.

Selling a Cybersecurity strategy can entail communicating a compelling need for certain organization capabilities well beyond the definition of any single set of controls. Information security is increasingly becoming a discussion amongst senior executives and boards of directors and the National Institute of Standards and Technology (NIST) Cybersecurity framework is often at the center of those discussions. With a growing concern over the need for improvements to the Cybersecurity of the Critical Infrastructure of the United States, Executive Order 13636 was issued on February 12, 2013 (Obama, 2013). Sec 7 of Executive Order 13636 established a mandate for the Director of NIST to collaborate with industry leaders to establish a voluntary Cybersecurity framework. The mandate further stipulated that the resulting framework be consistent with industry standards and provide a cost-effective approach to improving Cybersecurity. The resulting NIST Cybersecurity Framework was published in February 2014 (National Institute of Standards and Technology, 2015). The Cybersecurity Framework provides a means of aggregating and communicating Cybersecurity capabilities that is complimentary to other

frameworks and standards such as the CSCs. Planning and budgeting for a CSC implementation is only as effective as the ability to gain executive support to take action on those plans. This paper will focus on aggregating the detailed implementation guidance for the CSCs into a base set of capabilities based upon the NIST Cybersecurity framework. Demonstrating a method for planning and budgeting that incorporates the cost to procure technology, the ongoing software support cost, and the operational cost needed to maintain, operating and improving the processes and technology supporting the CSCs. This paper will combine the frameworks and the detailed planning processes into a method for communicating the benefits of a CSC implementation to executive leadership.

Approach and assumptions

Organizations have a wide variety of choices on how to build their information technology environments. Those choices are driven by factors unique to each organization such as:

- The nature of the business the organization is engaged in;
- The demands of the customers serviced by the organization;
- Legal and regulatory compliance requirements;
- The professional experience of the people leading the business and the technology decision making processes;
- The technical expertise and experience of the individuals selecting the technology to be deployed; and
- The risk tolerance of the organization.

The potential combinations of technology deployed in any one environment is extremely diverse; accordingly, this paper does not attempt to provide technical solutions to cover all possible environments. This paper provides a general guideline for companies considering implementing the CSCs. This paper will focus on the balance of People Processes and Technology as drivers for the effective implementation of the CSCs.

The principle of People, Processes and Technology has been used in the Information Security community since the early 1990's (Lacey, 2013) but may have roots back to the 1964 Leavitt "diamond" model of organizations (Edwards, 2011). The drivers of People, Processes and Technology will be used to help guide the decision process for designing and

implementing the individual controls. The approach for the individual controls will provide aggregate data used for consolidated budgeting estimates at the capabilities level. The technology solutions referenced in this paper are intended to be illustrative in nature and is not intended to be, and should not be considered an all inclusive listing of possible solutions available to implement the referenced controls.

Planning

When planning any Cybersecurity initiative, a detailed understanding of the organization's assets, threats against those assets and risk tolerance is important. Although control frameworks are helpful tools for designing and implementing Cybersecurity programs, embedding Cybersecurity into the organization's culture starts with aligning the Cybersecurity objectives to the business objectives in a way that manages the risk to the organization. There are multiple frameworks and methodologies to guide the process for risk management. It is not the intent of this paper to explore the risk management practices or recommend an approach to risk management, however, it is important to highlight the need for risk management practices in the development of a Cybersecurity program.

One of the key control frameworks, the NIST Cybersecurity framework is based on is the NIST Special Publication 800-53 Rev 4 (SP 800-53) (Joint Taskforce Transformation Iniative, 2013). Chapter 2 of SP 800-53 defines the fundamental concepts of a Cybersecurity program, these concepts begin with a risk management framework. In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published their *Enterprise Risk Management - Integrated Framework* and subsequently updated it in 2013 (COSO About Us, 2015). An example on integrating risk management practices to define an organization's risk tolerance is available from the National Institute for Cybersecurity Careers and Studies (NICCS) in the form of the Cybersecurity Workforce Planning Diagnostic (NICCS, 2013). These risk management frameworks can assist with building a comprehensive understanding of the organization's risk tolerance. Defining the assets of value and the threats against those assets is a key focal point of risk management efforts, however, to truly align with the business priorities it is critical to dive deeper into the concept of acceptable loss and risk tolerance. Understanding risk tolerance, and what is an acceptable loss, can sometimes be difficult from a Cybersecurity perspective.

Paul Hershberger pjhersh13@gmail.com

One approach to understanding acceptable loss is through the way the organization manages liability insurance. The insurance industry has a long history of understanding acceptable loss and have incorporated their experience into the policy deductible. The deductible defines the amount of money the policy holder will spend to cover damages before the insurance policy commences paying for damages. Choosing the right deductible allows the policy holder to manage their risks within their personal tolerance levels by balancing the risk exposure between the policy holder and the insurance company (Insurance Information Institute, n.d.). The concept of deductible and acceptable loss directly translates into the Cybersecurity planning in the form of risk tolerance. If the organization has a standard $10, $20, or $30 million deductible for insurance coverages, the Cybersecurity risk tolerance is likely to be in the same range. Likewise if the organization chooses to self-insure up to a certain dollar amount, this is a good indicator of the risk tolerance of the organization. Although these tolerance levels are clearly defined in dollar amounts and not all Cybersecurity risks can be easily quantified as by dollar amounts so additional analysis will need to be done to understand intangibles such as reputation, and brand image risk tolerances.

In addition to the organizations risk tolerance, special consideration must be given to the legal and regulatory compliance requirements of the organization. Each organization will face a set of requirements based on factors such as their industry, geographies in which they operate and customers they serve. Compliance with the legal requirements such as the European Union Privacy Laws can be complex and Cybersecurity practices can often come into conflict with those requirements. Lawyer and Blog Author Leonor Macedo notes in her January 2015 Blog post the need for "*unambiguous consent*" by employees under the EU Privacy laws in order for an organization to process data concerning their employees (Macedo, 2015). Compliance with privacy laws can determine the approaches to Cybersecurity capabilities that are legal for the organization to engage in.

The NIST Cybersecurity framework defines the organization's Cybersecurity capabilities to as:

- Identify- Develop the organizational understanding to manage Cybersecurity risk to systems, assets, data, and capabilities.

- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect - Develop and implement the appropriate activities to identify the occurrence of a Cybersecurity event.
- Respond – Develop and implement the appropriate activities to take action regarding a detected Cybersecurity event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impacted due to a Cybersecurity event.

The design and implementation of the CSCs will support the development and sustainment of these capabilities.

The Control drivers of people, processes and technology are key to influencing the design and operating effectiveness of controls within an organization. For the purpose of this paper, each control is given a weighting based on the driver related to that specific control. The control drivers are defined as follows:

- The People driver focuses on the staffing levels, skills and knowledge needed to perform the control
- The Processes driver focuses on the need for well defined, documented and broadly understood processes needed to perform the control
- The Technology driver focuses on the amount of automation, systems and/or tools needed to perform the control.

Each control driver is weighted based on how it may affect the implementation of the control using the following criteria:

- A Primary driver is one that shapes the control; the choices made in the design of this driver will determine the requirements of the other drivers.
- A Secondary driver is one that is key to the success of the control, although the requirements for this driver are defined by the Primary driver.

- A Supportive driver is one that is necessary for effectiveness of the control, however, the requirements for this driver defined by the Primary and Secondary drivers.

For planning purposes organization size is defined as follows:

- Small - under 1,000 users
- Medium - more than 1,000 but less than 10,000 users
- Large - over 10,000 users

Assumptions:

In order to keep the model and templates manageable, this paper cannot cover all possible scenarios for all potential environments and organizational structures. Accordingly, certain assumptions are made throughout this paper. The assumptions form a basis for the implementation options and approaches illustrated in this paper. The key assumptions include:

- An Information Technology Help Desk is established with a moderate level of process maturity covering incident reporting, management and tracking. Those processes are generally aligned with ITIL practices and are appropriately staffed to the size of the organization.
- A Microsoft Active Directory infrastructure has been implemented running Windows Server 2012 R2 and configured with a Forest Functional Level of no less than Windows Server 2008.
- IT processes have been implemented covering common infrastructure maintenance and management, generally aligned with ITIL practices.
- The use of Open Source or General Public License (GNU) software as an alternative to commercial packaged software will shift costs from software to human capital rather than eliminate the cost.
- The CSCs are implemented in order and the implementation effort builds upon itself with earlier control supporting the implementation of the later.
- Economies of scale exist in the implementation of the CSCs in which the cost to implement each control reduces as more controls are implemented.

Paul Hershberger pjhersh13@gmail.com

Prioritizing the CSC implementation

Planning for an implementation of the CSCs should be prioritized to ensure the resources available to the organization are used in the most cost effective manner possible. There are several factors to consider when prioritizing the CSCs, one of which is the guidance provided by the Council on Cybersecurity. The CSCs version 5.1 provides guidance on prioritization based on two key factors. The first factor is intended to establish a basic foundation for the Cybersecurity program of an organization and focuses on implementing controls 1 through 5 in order (Council on CyberSecurity). This approach has been adopted by the Department of Homeland Security Continuous Diagnostics and Mitigation Program and is considered as the primary means of building the foundation necessary for the implementation of the remaining CSCs. The second prioritization factor is based upon the "First Five Quick Wins" and is intended to help organizations take action that can provide immediate benefits to the organization and prevent attacks. These quick wins are:

1. Application whitelisting (found in CSC 2);
2. Use of standard, secure system configurations (found in CSC 3);
3. Patch application software within 48 hours (found in CSC 4);
4. Patch system software within 48 hours (found in CSC 4); and
5. Reduced number of users with administrative privileges (found in CSC 3 and CSC 12).

The final decisions on prioritization of the CSC implementation should take into consideration the risk tolerance of the organization and ensure that the implementation targets the most impactful actions that manage the Cybersecurity risk.

Planning the Control implementation

Planning the CSC implementation requires a significant amount of analysis and consideration to ensure that the control design is operating effectively and the organization has the proper skills and capacity to maintain the control over time. Although a significant amount of detail should be planned, that level of detail can hinder the effectiveness of communication with senior executives. The planning process should include detailed

analysis which can subsequently be aggregated into a set of high-level capabilities that can easily be explained to senior leadership. For the purpose of this paper, CSC #1 will be documented as a demonstrative control to illustrate the detailed analysis necessary for implementation planning. In this example, CSC #1 will focus on the implementation at a Medium-sized organization with an acceptable loss risk tolerance defined as $20m.

Inventory of Authorized and Unauthorized Devices

> *Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.*

Visibility into the devices that make up a technology environment is a fundamental requirement for effective Cybersecurity. The ability to identify unauthorized devices and respond accordingly reduces the attack surface available for an attacker to exploit. Maintaining and enforcing the inventory of authorized and unauthorized devices requires active and passive monitoring and analysis at a precision that can range from weekly to near real-time review and enforcement. The primary consideration in implementing this control is technology. The collection, processing, analytics and alerting of authorized and unauthorized devices requires a high level of automation. Accordingly, the decision process should focus on the technology needed to implement this control. Special consideration should be given to the tools and how they integrate with one another as well as integration with core technology for incident management processes.

Control drivers. The control drivers for CSC #1 are as follows:

People	**Processes**	**Technology**
Supportive	Secondary	Primary

Technology needs. When identifying technology solutions in support of the CSCs implementation it is essential to be aware of the potential for limitations on product availability in the geographies in which the organization operates. Restrictions such as those defined in the United States Department of Commerce's Export Control System may limit the ability to implement solutions in geographies where restrictions apply.

Asset inventory database. A technology asset inventory database is the primary technology needed for implementation of CSC #1. The technology asset inventory database should be capable of maintaining information about all of the authorized assets that constitute the organization's technology environment and anything that is allowed to connect to those technology assets. An asset inventory database is a foundational technology in the implementation of CSC #1 and is an essential element of the detective control objectives. Asset inventory databases often integrate with many of the leading help desk solutions and include software options such as:

- Agiloft Agile Asset Management;
- SpiceWorks IT Asset Manager
- Service Now Asset Management; and
- BMC Remedy Asset Management.

Device Scanners. A device scanner is a solution that scans the technology environment to identify devices connected to that environment. These scans can be active and/or passive in nature. An active scanner is one that can be configured to reach out across the environment and communicate with the devices to actively identify what is connected. Active scanners typically operate as a point-in-time scan on a predefined interval based on the business risk tolerance. Passive scanners connect to the environment and monitor device connections as they happen, recoding information about the devices as the connection takes place. Active scanners create an inventory of all devices at the point in time that the scan is executed. An active device scanner can lose sight of devices that are not connected during the scheduled scan. Passive device scanners can lose visibility into devices that remain connected but in a dormant state. Reliance on one type of scanner can create blind spots in visibility, therefore, the use of both active and passive scanners is recommended. Device scanners supports the implementation of CSC #1 from a detective

control perspective. This control capability can assist the organization to identify unauthorized devices before they can cause significant harm to the environment. The use of device scanners include solutions such as:

- NMap;
- Tenable Nessus;
- OpenVAS,
- SpiceWorks IT Asset Manager
- ForeScout CounterACT; and
- Tanium Endpoint Platform.

Network Access Control. A Network Access Control (NAC) solution manages the connections to the technology environment and enforces rules associated with device connections. A NAC implementation can range from a high-level control focused on what can connect to the environment down to granular rule sets that govern what types of assets can connect to each other down to the port and protocol allowed between devices within the environment. NAC is critical to the implementation of CSC #1 as it serves as a preventive control in which rules around authorized devices and connections are enforced. NAC solutions can vary in approach and underlying technology. NAC solutions include:

- PacketFence Zero Effort NAC;
- FreeNAC;
- ForeScout CounterACT;
- CISCO NAC Appliance; and
- Portnox Network Access Control.

Public Key Infrastructure. A Public Key Infrastructure (PKI) solution provides the organization with the means of creating, distributing, using and managing digital certificates. The PKI can support the organization in a variety of ways, including maintaining the confidentiality of information through the use of encryption, authentication of users and devices, along with supporting the use of electronic signatures for authorization. A PKI is a supportive technology and the need for a PKI solution in support of the CSC #1 is dependent on the solution used for asset inventory and NAC. PKI solutions include:

- Microsoft Windows Public Key Infrastructure;
- EJBCA Open Source PKI;
- OpenCA; and
- OpenSSL.

Dynamic Host Configuration Protocol. A Dynamic Host Configuration Protocol (DHCP) solution provides the organization with the capability to automatically provide Internet Protocol (IP) addresses and configurations such as subnet mask and default gateway to hosts connected to the environment (Internet Engineering Task Force, 1993). The ability to easily manage the IP address space within an environment is important for ease of connectivity as well as ease of managing the devices connected to the environment. A DHCP solution supports the technology solutions needed for implementing CSC #1 and can provide capabilities to enable both the preventive controls associated with NAC as well as the detective controls associated with authorized asset inventory and active device scanning. DHCP solutions include:

- Windows Active Directory DHCP Services;
- Infoblox Trinzic DDI;
- Solarwinds IP Address Manager;
- BlueCat DHCP; and
- Open DHCP Server.

Logging/Alerting/Analytics. A Logging/Alerting/Analytics system, commonly referred to as a Security Information and Event Monitoring (SIEM), provides data aggregation, correlation, alerting, reporting and forensic analysis capabilities. These capabilities are foundational for any information security program and the choice of technology can directly influence the options available for implementing numerous other controls. Because of the role of a SIEM in an organization, there are arguably more solution options available to meet the needs of the organization than any other technology needed to support the CSCs. An effective SIEM solution can be an integral part of both detective as well as preventive controls and can support the implementation of CSC #1 from both of those perspectives. Options for SIEM capabilities include:

- Open Source Security Information and Event Management (OSSIM);

- Alien Vault Unified Security Management (USM);
- Alert Logic Log Manager;
- Splunk Enterprise;
- FireEye Threat Analytics Platform;
- IBM QRadar;
- HPE ArcSight; and
- LogRhythm SIEM.

Processes supporting CSC #1. Although technology is the primary driver for CSC #1, the processes behind the technology must be carefully considered in order to sustain the operating effectiveness of the control beyond implementation. The core processes necessary to sustain CSC #1 include technology asset management, scanning and reporting, security event monitoring and alerting, and incident response. The technology asset management processes should incorporate the active maintenance of the asset inventory system tracking the additions, changes, and retirement of assets through their lifecycle. Scanning and reporting processes should incorporate the maintenance and support for scanning of the environment, comparison against authorized devices and the reporting of discrepancies into the established ticketing system for remediation actions. Security event monitoring and alerting processes should be established that incorporate the ability to identify unauthorized devices connecting to the environment, generate an alert based on unauthorized connection(s), and integrate confirmed incidents into the established ticketing system for remediation actions. The incident response processes should focus on the processes and procedures to respond to a security incident that include sub-processes for incident triage, containment, analysis, remediation, recovery and reporting. The processes implemented should be designed to operate at a level of maturity to maintain the risk exposure below the organization's risk tolerance.

Staffing considerations. In the implementation of CSC #1, the control driver of people plays a supportive role due to the need to automate the control as much as possible. The decisions made regarding automation of the control activities, the technology deployed, and processes implemented can directly influence the staffing levels necessary to sustain CSC #1. When evaluating staffing needs, consider the three functional roles of

maintain, operate and improve. The need to maintain should include general configuration, patching, updates, and overall system health monitoring. Next, analyze the workload and technical skills needed for operating the processes implemented to support the control. Finally evaluate the tasks to accomplish and the decisions necessary to complete the tasks and determine the experience level necessary to operate the processes. The final workload to consider relates to ongoing process improvements. Attackers continually work to improve their tactics, techniques and procedures; similarly, the defenses against those attackers needs to continue to improve. Considering the workload to review, evaluate and improve the technology, processes and procedures supporting CSC#1 is important to the long term success of the control activities.

Budget Considerations. Budgeting for the implementation of CSC#1 should include consideration for the purchase of technology, the implementation of the technology, the ongoing maintenance and support, along with the operational costs of the processes implemented to support the control long term. The first element that goes into the overall budget is the cost to purchase the technology necessary to implement CSC#1. An illustrative example for the individual technology solutions needed for CSC#1 at the example organization are represented by the ranges in Table 1:

Table 1 Technology Solution Budget Ranges

Solution	Low Range	High Range
Asset inventory database	$30,000	$150,000
Device Scanners	$50,000	$300,000
Network Access Control	$500,000	$1,200,000
Public Key Infrastructure*	$0	$0
Dynamic Host Configuration Protocol*	$0	$0
Logging/Alerting/Analytics	$300,000	$700,000
Total	**$880,000**	**$2,350,000**

*assumes the use of standard Microsoft functionality inherent with the existing Microsoft Active Directory environment.

In addition to the cost of the initial purchase, ongoing annual software support fees should be included in the operational budget to support the technology solutions. **Annual support fees are estimated to be 20 - 22% of the software purchase price (Spend**

Matters, 2014). Assuming a 21% annual maintenance fee will result in range of $184,800 to $493,500 in annual software support costs.

Staffing considerations are one of the most complicated decisions to make when planning and budgeting for any CSC implementation. Although the final staffing requirements will depend on the existing organization structure and available capacity along with the final decisions on the technology and processes implemented. Decisions around staffing needs in support of a CSC implementation effort should start with an assessment of current skills, availability and staffing against the additional workload associated with the new capabilities. Identifying existing skills and resource availability will help define the existing resource gaps. The operational requirements of the organization, depth of skills necessary in conjunction with the available of those skills in the local market can contribute to the final organization design. Potential staffing options include a blending of full time employees, contractors and outsourced service providers. For the purpose of this example, a staffing requirement of five additional full-time employees will be required to support the maintenance, operation and ongoing improvement activities necessary to sustain the long-term effectiveness of CSC#1.

Communicating the plan

Effective communication of the plan and budgetary requirements for a CSC implementation project can be a daunting task. Providing too much detail can cause executive leadership to lose interest in the proposal, while too little detail can jeopardize the leadership's confidence in your ability to be successful. Finding the appropriate balance in communication and approach is critical to success. Since the release of the NIST Cybersecurity framework, it has become a common talking point with senior executives and boards of directors. When talking about the importance of the NIST Framework to corporate boards of directors, The Securities and Exchange Commission (SEC) Commissioner Luis Aguilar stated (Aguilar, 2014):

> *"While the Framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes. At a minimum, boards should work*

with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed."

With the media, the SEC and the White House communicating the importance of the NIST Framework, it's become a common language to bridge the communications gap between Cybersecurity professionals and senior executives. Leveraging the NIST framework can help communicate the benefit in your CSCs implementation project. Developing the communication plan should take a simultaneous bottom-up and a top-down planning process. The bottom-up process includes performing the detailed analysis per CSC to identify the people, processes and technology needed to implement the control as shown in section 4 above. The detailed analysis can be aggregated into a planning template as seen in Appendix A. The top-down approach starts with an assessment of the current Cybersecurity practices against the guidelines documented in the NIST Framework. The assessment should consider existing Cybersecurity practices and operational effectiveness of those practices. The assessment should include an evaluation of the risk tolerance of the organization to identify the desired state of Cybersecurity operations needed to manage risk within acceptable tolerances. The results of this assessment should be represented in a gap analysis dashboard that can be presented to executive leadership and the board of directors. The dashboard should define the functions as identified in the NIST framework, provide some context behind the functions, and rate the current state against the desired state as show in table 2.

Table 2 NIST Maturity Matrix

Function	Objective	Current Tier	Target Tier
IDENTIFY (ID)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	0	4
PROTECT (PR)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	1	3
DETECT (DE)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	1	4
RESPOND (RS)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	1	3
RECOVER (RC)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	1	3

*for illustrative purposes only, this does not reflect the results of an actual assessment

Paul Hershberger pjhersh13@gmail.com

The initial communication of maturity based on the NIST framework can become foundational to the overall implementation effort. The maturity assessment and gap analysis should be the start point for the CSC implementation planning process as it can serve as a guide for focus of resources and what controls must be implemented to reach the targeted NIST Framework tier. Communicating the assessment results to senior leadership can happen in parallel to the detailed planning exercises outlined earlier in this paper. The final nature and timing of the communications with senior executives is dependent on the leadership and the general culture within the organization. Approaching those communications can start with the understanding of how the CSCs map to the NIST Framework and how the CSCs support the achievement of the tiers defined in the NIST Framework as seen in Appendix B. With the understanding of how the CSCs support the NIST framework, the dashboard can be expanded to include a reference to the CSC implementation effort necessary to achieve the targeted state of Cybersecurity operations within the organization as seen in Table 3.

Table 3 NIST Maturity to CSC Actions Matrix

Function	Objective	Role in Cybersecurity	Current Tier	Target Tier	Improvement Actions
IDENTIFY (ID)	Develop the organizational understanding to manage Cybersecurity risk to systems, assets, data, and capabilities.	Foundational - All other objectives depend upon the successful Identification of systems, assets, data and capabilities.	0	4	CSC 1, 2, 4
PROTECT (PR)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Supportive - Successful Protection reduces the burden on Detect, Respond and Recover.	1	3	CSC 3, 6, 7, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20
DETECT (DE)	Develop and implement the appropriate activities to identify the occurrence of a Cybersecurity event.	Enabling - Detection makes Respond and Recover possible.	1	4	CSC 5, 14, 16
RESPOND (RS)	Develop and implement the appropriate activities to take action regarding a detected Cybersecurity event.	Supportive - An effective Response helps minimize the need for Recovery.	1	3	CSC 18
RECOVER (RC)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a Cybersecurity event.	Supportive - Without effective Recovery, the risks associated with the other Objectives increase dramatically.	1	3	CSC 8

*for illustrative purposes only, this does not reflect the results of an actual assessment

Paul Hershberger pjhersh13@gmail.com

As seen in Table 4 below, the dashboard can continue to expand to incorporate the costs of both the initial implementation as well as the ongoing budget required to sustain the operations and improvement of the CSC implementation project over time. The budget needs should further summarize the information within the planning template in Appendix A.

Table 4 NIST Remediation Summary Template

Function	Current Tier	Target Tier	Improvement Actions	Implementation Budget	Sustainment Budget
IDENTIFY (ID)	1	4	CSC 1, 2, 4	$ 4,050,000.00	$1,165,000.00
PROTECT (PR)	1	4	CSC 3, 6, 7, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20	$ 3,025,000.00	$1,494,000.00
DETECT (DE)	1	4	CSC 5, 14, 16	$ 500,000.00	$ 270,000.00
RESPOND (RS)	1	4	CSC 18	$ 120,000.00	$ 344,000.00
RECOVER (RC)	1	4	CSC 8	$ 350,000.00	$ 60,000.00

*for illustrative purposes only, this does not reflect the results of an actual assessment

Conclusion

The planning and implementation of the 20 Critical Security Controls can be a daunting task and one that most certainly requires alignment across the organization. An understanding of the organization's risk tolerance can create alignment by positioning controls to support business objectives while responsibly managing resourcing needs. An implementation plan that demonstrates alignment with the organization and responsible resource management creates the foundation for successful communication with senior leadership. Effective communications with senior leadership is a critical component to the success of a CSCs implementation. Thoughtful consideration as to the resources necessary for implementation and long term sustainability of the CSCs is an essential component to the executive communication plan. Overestimating the requirements necessary for implementation could result in a denied request, while underestimating will impede the ability to effectively implement the controls. Internal factors such as organizational capacity and operational maturity along with external factors such as legal and regulatory compliance are important to successful deployment of the 20 CSCs and ensuring that

implementation of the CSCs do not introduce more risk than they mitigate. It is imperative that Cybersecurity processionals effectively work to bridge the gap between the details of the CSCs implementation plan and the high-level aggregate view to effectively communicate the need for improvements to Cybersecurity. The methods discussed in this paper can help bridge that gap to ensure the CSCs implementation plan resonates with executive management and garners their support.

References

Aguilar, L. A. (2014, June 10). *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus.* Retrieved Nov 7, 2015, from U.S. Securities and Exchange Commission: http://www.sec.gov/News/Speech/Detail/Speech/1370542057946

COSO About Us. (2015). Retrieved November 27, 2015, from Committee of Sponsoring Organizations of the Treadway Commission: http://www.coso.org/aboutus.htm

Council on CyberSecurity. (2014). *Critical Controls*. Retrieved May 9, 2015, from Council on CyberSecurity: http://www.counciloncybersecurity.org/critical-controls/

Council on Cybersecurity. (n.d.). *About Us*. Retrieved September 20, 2015, from Council on Cybersecurity: http://www.counciloncybersecurity.org/about-us/

Council on CyberSecurity. (n.d.). *CSC-5.* Retrieved Sep 15, 2015, from SANS.org: https://www.sans.org/media/critical-security-controls/CSC-5.pdf

Edwards, J. (2011). A Process View of Knowledge Managemtn: It Ain't What you do, it's the way That you do it. *Electronic Journal of Knowledge Management, 9*(4), 297-306.

Insurance Information Institute. (n.d.). *Insurance Information Institute*. Retrieved November 30, 2015, from Understanding Your Insurance Deductable: http://www.iii.org/article/understanding-your-insurance-deductible

Internet Engineering Task Force. (1993, October). *RFC-1531*. Retrieved November 27, 2015, from RFC Base: https://www.rfc-editor.org/rfc/rfc1531.txt

Joint Taskforce Transformation Iniative. (2013, April). *NIST Special Publication 800-53 Revision 4.* Retrieved October 15, 2015, from National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Lacey, D. (2013, January 20). Dtich the Triangle and use more technology. *Daveid Lacey's IT Security Blog*. ComputerWeekly.com. Retrieved August 15, 2015, from http://www.computerweekly.com/blogs/david_lacey/2013/01/we_need_more_use_of_security_t.html

Macedo, L. (2015, January 27). *Monitoring of Employees in the workplace: the very private parts of a job in the EU private sector*. Retrieved November 27, 2015, from The Public Privacy: http://thepublicprivacy.com/2015/01/27/monitoring-employees-workplace-private-parts-job-eu-private-sector/

National Institute of Standards and Technology. (2015, July 8). *Welcome*. Retrieved October 15, 2015, from Cybersecurity Framework: http://www.nist.gov/cyberframework/

NICCS. (2013). *Cybersecurity Workforce Planning Diagnostic*. Retrieved November 27, 2015, from National Initiative For Cybersecurity Careers and Studies: https://niccs.us-cert.gov/careers/cybersecurity-workforce-planning-diagnostic

Obama, B. (2013, February 12). *Executive Orders*. Retrieved October 15, 2015, from the White House: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Spend Matters. (2014, July 23). *How to Cut Software Maintenance and Support Costs (and Fund IT Innovation)*. Retrieved November 7, 2015, from Spend Matters: http://spendmatters.com/2014/07/23/how-to-cut-software-maintenance-and-support-costs-and-fund-it-innovation/

Paul Hershberger pjhersh13@gmail.com

Paul Hershberger pjhersh13@gmail.com

Appendix A Critical Security Controls Aggregated Planning Template

Control	People	Process	Technology	Technology Purchase	Annual Maintenance Cost	Implementation Cost	Additional Staffing	Start-Up Costs	Sustaining
CSC 1	Supportive	Secondary	Primary	$1,500,000.00	$315,000.00	$300,000.00	$600,000.00	$1,800,000.00	$915,000.00
CSC 2	Supportive	Secondary	Primary	$ 300,000.00	$60,000.00	$100,000.00	$180,000.00	$400,000.00	$240,000.00
CSC 3	Supportive	Secondary	Primary	$ 50,000.00	$10,000.00	$0	$0	$50,000.00	$10,000.00
CSC 4	Secondary	Primary	Supportive	$50,000.00	$10,000.00	$0	$0	$50,000.00	$10,000.00
CSC 5	Supportive	Secondary	Primary	$450,000.00	$90,000.00	$50,000.00	$180,000.00	$500,000.00	$270,000.00
CSC 6	Secondary	Primary	Supportive	$250,000.00	$50,000.00	$80,000.00	$180,000.00	$330,000.00	$230,000.00
CSC 7	Supportive	Secondary	Primary	$500,000.00	$100,000.00	$150,000.00	$180,000.00	$650,000.00	$280,000.00
CSC 8	Supportive	Primary	Secondary	$300,000.00	$60,000.00	$50,000.00	$0	$350,000.00	$60,000.00
CSC 9	Primary	Secondary	Supportive	$0	$150,000.00	$0	$90,000.00	$0	$240,000.00
CSC 10	Secondary	Primary	Supportive	$0	$0	$50,000.00	$0	$50,000.00	$0
CSC 11	Supportive	Secondary	Primary	$150,000.00	$30,000.00	$50,000.00	$0	$200,000.00	$30,000.00
CSC 12	Secondary	Supportive	Primary	$500,000.00	$100,000.00	$150,000.00	$250,000.00	$650,000.00	$350,000.00
CSC 13	Supportive	Secondary	Primary	$600,000.00	$120,000.00	$80,000.00	$0	$680,000.00	$120,000.00
CSC 14	Secondary	Supportive	Primary	$0	$0	$0	$0	$0	$0
CSC 15	Primary	Supportive	Secondary	$350,000.00	$70,000.00	$75,000.00	$180,000.00	$425,000.00	$250,000.00
CSC 16	Secondary	Primary	Supportive	$0	$0	$0	$0	$0	$0
CSC 17	Secondary	Supportive	Primary	$20,000.00	$4,000.00	$0	$0	$20,000.00	$4,000.00
CSC 18	Primary	Secondary	Supportive	$120,000.00	$24,000.00	$	$320,000.00	$120,000.00	$344,000.00
CSC 19	Primary	Supportive	Secondary	$0	$0	$120,000.00	$0	$120,000.00	$0
CSC 20	Primary	Secondary	Supportive	$50,000.00	$10,000.00	$0	$0	$50,000.00	$10,000.00
Total				$5,190,000.00	$1,203,000.00	$1,255,000.00	$2,160,000.00	$6,445,000.00	$3,363,000.00

All numbers are illustrative in nature and should not be used as a substitute for detailed individual planning.

Appendix B Critical Security Control to NIST Framework Template

Function	Objective	Role in Cybersecurity	Current Tier	Target Tier	Improvement Actions	Implementation Budget	Sustainment Budget
IDENTIFY (ID)	Develop the organizational understanding to manage Cybersecurity risk to systems, assets, data, and capabilities.	Foundational - All other objectives depend upon the successful Identification of systems, assets, data and capabilities.	0	4	CSC 1, 2, 4	$ 4,050,000.00	$1,165,000.00
PROTECT (PR)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Supportive - Successful Protection reduces the burden on Detect, Respond and Recover.	1	3	CSC 3, 6, 7, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20	$ 3,025,000.00	$1,494,000.00
DETECT (DE)	Develop and implement the appropriate activities to identify the occurrence of a Cybersecurity event.	Enabling - Detection makes Respond and Recover possible.	1	4	CSC 5, 14, 16	$500,000.00	$270,000.00
RESPOND (RS)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Supportive - An effective Response helps minimize the need for Recovery.	1	3	CSC 18	$120,000.00	$344,000.00
RECOVER (RC)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a Cybersecurity event.	Supportive - Without effective Recovery, the risks associated with the other Objectives increase dramatically.	1	3	CSC 8	$350,000.00	$60,000.00

All numbers are illustrative in nature and should not be used as a substitute for detailed individual planning.

Paul Hershberger pjhersh13@gmail.com