Global Information Assurance Certification Paper

Leading Effective Cybersecurity with the Critical Security Controls

GIAC (GCCC) Gold Certification

Author: Wes Whitteker, wes_whitt@yahoo.com

Advisor: Richard Carbone

Accepted: March 15, 2016

Abstract

Over the past several years, global news coverage has been plagued with media headlines of multiple private and public institutions falling victim to significant data breaches. With this fact in mind, it is important to note that these breaches are happening in spite of the fact that there have been heavy investments in cybersecurity resources (people, processes, technology, etc.) over the past several years. When one combines the idea that significant data breaches continue to happen while large investments have been made to mitigate them, it paints a picture of an ineffective response to the problem. As such, two critical questions require further investigation. The first is what is preventing leadership from creating an effective response to the global cybersecurity problem? The second is how can the Critical Security Controls (CSCs) be used by leadership to overcome these challenges and improve effectiveness within their organization?

1. Introduction

Cybersecurity is a domain where organizations need to be right all the time and a bad actor needs to be right once. As such, the traditional mindset of 100% prevention in keeping a bad actor from accessing an organization's systems is quickly changing. The new mindset for organizations is one where they need to strive for cyber resiliency (i.e. detection, response, & recovery) (Goche & Gouveia, 2014; World Economic Forum, 2014). This change in mindset is due to increased visibility from the fact that, inevitably, organizations will experience data breaches. As we have seen over the past several years, global news coverage and media headlines are plagued with multiple private and public institutions falling victim to significant data breaches (CSIS, 2015; ITRC, 2014; ITRC, 2015).

As the cybersecurity community moves to focus on resiliency (a more advanced function), it is important to note that these breaches have been happening in spite of the fact that there has already been heavy investments in cybersecurity resources (people, processes, technology, etc.) (Gartner, 2015; Gilligan, 2013; Giles, 2014). When one combines the idea that significant data breaches continue to happen while large investments have been made over the past several years to mitigate them, it paints a picture of an ineffective response to the global cybersecurity problem. To this end, in order to achieve effectiveness in cybersecurity and become cyber resilient, it is critical that an effective cybersecurity foundation is in place (KPMG, 2015).

In terms of building a house, if the foundation is not properly structured, the integrity of everything built on top of it is compromised. Extending this concept to cybersecurity, if an advanced security solution is architected on top of a flawed security foundation, the solution has an extremely high risk of its integrity being compromised. It is important to note that a good foundation is not about being compliant; it is about what works (Sager, 2016). Cyber resiliency requires a sound cyber security foundation that is built on what works. This paper will take a meta-analytic view at investigating the global cybersecurity problem with a focus on answering two fundamental questions:

1. What is preventing leadership from creating an effective response to the global cybersecurity problem?

2. How can the Critical Security Controls (CSCs) be used by leadership to overcome these challenges and improve effectiveness within their organization?

2. Barriers to Effective Cyber Security

As previously noted, it is evident that effectiveness in cybersecurity has been a struggle for leaders over the past several years. To complicate matters, it seems that many of the more popular avenues for understanding why these barriers continue to persist focus on analysis of singular technical problems while leaving out important analysis of people and processes. Though a focus on technical issues is certainly valuable information for professionals at a tactical level, bigger questions need to be asked from an organizational context that includes consideration for people and processes. This allows for a deeper understanding of root causes to the problems – the crux.

One can arrive at several of these larger organizational issues by asking the simple question, "What is preventing leadership from creating an effective response to the global cybersecurity problem?" Once these higher-level issues are understood, effective and comprehensive solutions can be considered. Using the CSCs as the lens for addressing these higher-level issues, solutions can be identified by asking the question, "How can the Critical Security Controls (CSCs) be used by leadership to overcome these challenges and improve effectiveness within their organization?

In answering the previously stated questions, several over-arching themes have been identified and will be discussed. Those issues are:

- Proper Priorities (What Steps to Take First)
- Not Sure What to Measure?
- Ineffective Solutions
- Lack of Executive Support
- Leadership Skills Gap

- Organizational Maturity (Dimensional Research, 2015; Finn & McCullock, 2015; FINRA, 2015; Korn Ferry Institute, 2014; Lobel & Loveland, 2012; Tripwire, 2014)

2.1. Proper Priorities (What Steps to Take First)

In a sea of regulatory and compliance requirements (i.e. RMF, PCI, HIPPA, SOX, etc.), focus on setting effective cybersecurity priorities is often lost (Childs, 2015). When looking at these requirements from the perspective of an organizational leader, it can be challenging to determine what should be done to ensure the organization is attaining a proper level of cyber-readiness. Often times, leaders see the efforts toward regulatory and compliance requirements as equivalent measures for true cybersecurity. Though there can be crossover between them and true information security; there is a distinct difference between the two areas. This difference has played out in various news sources over the last several years (Brookings Institution, 2013, p. 3-8).

In order to set organizational priorities for cybersecurity readiness, organizations need to move their mindset away from compliance. What is needed for setting these is a trusted set of prioritized best practices built on what actually works within the cybersecurity community as a whole – a community framework. The CSCs offer exactly this, an easily understood framework that consists of a set of community developed and prioritized cybersecurity best practices. According to the CEO for the Center for Internet Security (CIS), Jane Holl Lute:

> One of the benefits of the 20 Critical Security Controls is that they represent a risk judgment by a respected segment of the expert community, that you can prevent 80-90% of all known attacks by implementing and staying current on basic cyber hygiene…no enterprise needs to conduct a cyber risk assessment as if nothing were known. We know what to do to get you to a baseline of protection that prevents the vast majority of all known attacks (Tripwire, 2014).

As the cybersecurity domain continues to move into the future, the necessity for a prioritized set of pragmatic best practices will be become more evident. This will be, in large part, due to the growth in the Internet of Things (IoT), mobile computing, and cloud technologies. As these technologies consume our lives, more information and more

systems will connect to organizational networks. Thus, prioritizing core CSCs such as inventorying devices and software, secure configurations, and continuous vulnerability assessments will be critical to ensuring cybersecurity visibility for developing future cybersecurity strategies (PwC, 2016, p. 11). To this end, the U.S. Department of Homeland Security (DHS) is leveraging these four foundational controls in the first phase of their recently developed Continuous Diagnostics and Mitigation program (Department of Homeland Security, 2015). In addition to the DHS efforts, the California Attorney General has recently stated that implementation of the CSCs is the number one recommendation to show reasonable security for personal information (Harris, 2016).

2.2. Not Sure What to Measure?

As the saying goes, "You can't manage what you can't measure." This idea, though simple in concept, holds very true in the cybersecurity domain. Organizations tend to have very robust "dashboards" for tracking various business processes, but when it comes to true organizational cybersecurity readiness, they either struggle with what to measure or tend to focus on compliance. Unfortunately, neither of these approaches offer data points that directly translate into understanding an organization's true state of cybersecurity. This lack of focus on effective cybersecurity metrics has left organizations either completely unaware of their cybersecurity posture or assuming they are achieving an acceptable level of readiness when in fact they are not (Dimensional Research, 2015).

Again, the CSCs can be used to address this issue. The latest version of the CSCs offers 20 community developed controls that have been proven to combat over 80-90% of the cybersecurity issues experienced by organizations (Tripwire, 2014). The fact that the CSC control framework offers a known roadmap to an 80-90% solution is extremely remarkable as no other framework can offer this statement. As such, it makes sense that organizations would leverage these controls to establish metrics. Quite simply, there is no reason not to measure these controls.

From these controls, any size organization could easily develop a dashboard that tracks their own level of cybersecurity readiness (Eubanks, 2011). This has been the case in several organizations over the past several years (CIS, 2016b). In one example, the U.S. Department of State, after setting up monitoring and metrics around the key CSCs in

2008, experienced an 89% reduction in the level of cybersecurity risk across 80,000 systems in a 12-month period, and continued to improve upon this in subsequent years (Tarala, 2014, p. 17). Thus, an information centric approach to measuring an organization's state of cybersecurity readiness is clearly achievable with the CSCs.

Several vendor solutions have begun to incorporate pre-made metric dashboards based on the CSCs (Splunk, 2014; Dumont, 2014). By leveraging a vendor or in-house solution, once an organization begins to actively measure and report on the implementation of CSCs they are now managing those cybersecurity issues that are attributed to 80-90% of cybersecurity related issues will be represented. Below are two images of CSC based dashboards to show a few options for measuring and managing the CSCs. The first is a vendor provided dashboard and the second is an example of what was used by the Department of State in its iPOST system described above:

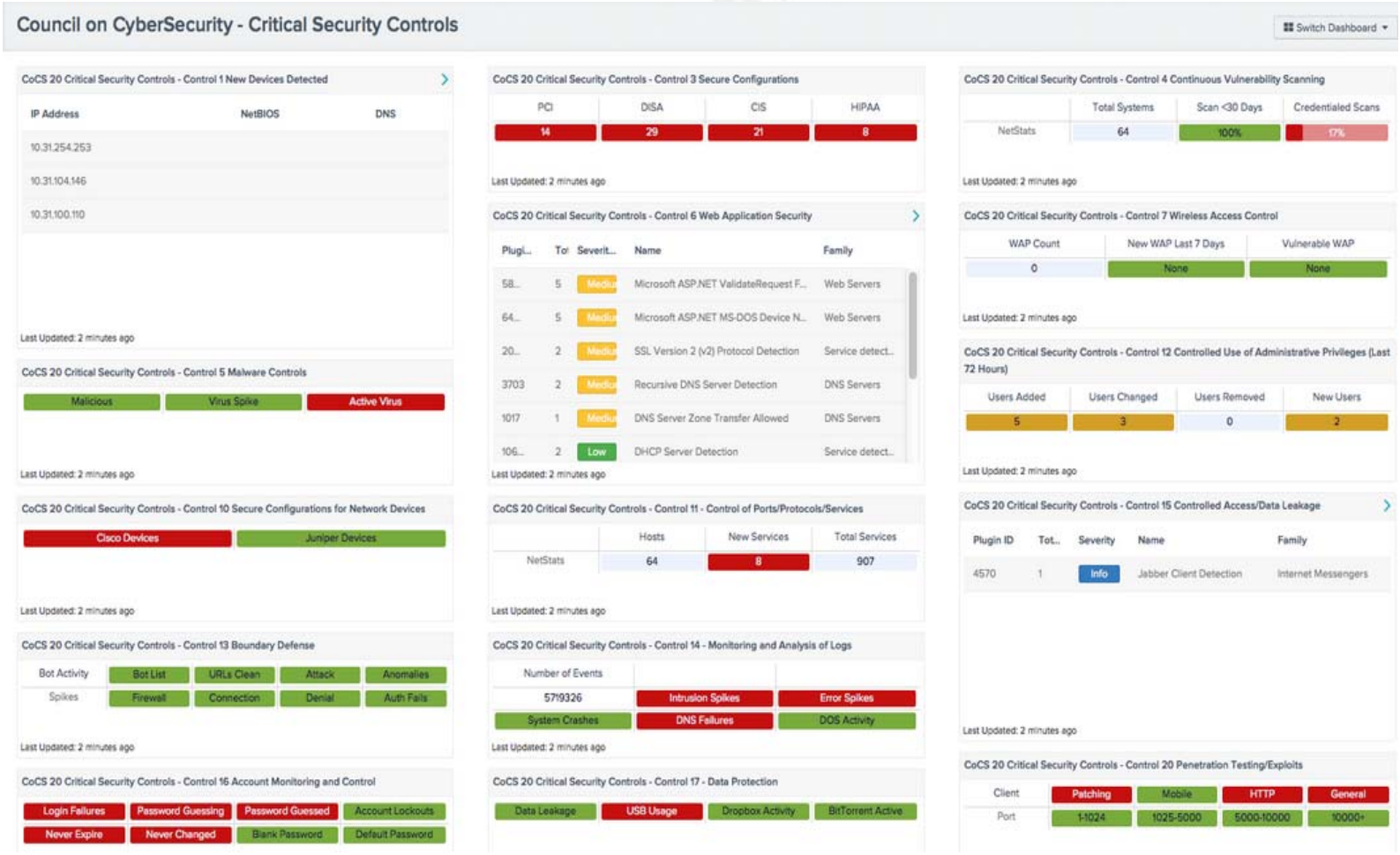

Figure 1: Council on Cybersecurity 20 Critical Security Controls Dashboard (Dumont, 2014)

Site_XYZ
Risk Score Advisor

The following grading scale is provided by Information Assurance and may be revised periodically.

Site Risk Score	4,792.4
Hosts	63
Average Risk Score	76.1
Risk Level Grade	B
Rank in Enterprise	234
Rank in Region	27

Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

The Site_XYZ Site Risk Score was calculated as follows:

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
Vulnerability	96.4	1.5	2.0 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
Patch	807.0	12.8	16.8 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
Security Compliance	1,089.0	17.3	22.7 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
Anti-Virus	1,068.0	17.0	22.3 %	6 per day for each signature file older than 6 days
SOE Compliance	975.0	15.5	20.3 %	5 for each missing or incorrect version of an SOE component
AD Computers	3.0	0.0	0.1 %	1 per day for each day the AD computer password age exceeds 35 days
AD Users	479.0	7.6	10.0 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS Reporting	200.0	3.2	4.2 %	100 + 10 per day for each host not reporting completely to SMS
Vulnerability Reporting	32.0	0.5	0.7 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
Security Compliance Reporting	43.0	0.7	0.9 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	**4,792.4**	**76.1**	**100.0 %**	

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

Figure 2: Risk Score Advisor (US Dept of State, 2010)

Wes Whitteker, wes_whitt@yahoo.com

2.3. Ineffective Solutions

Another significant area that organizations tend to struggle with is determining what solution, or solutions, would prove to be effective for positively affecting their cybersecurity readiness (Dimensional Research, 2015, p. 22). In a recent survey by Tenable Network Security, global cybersecurity readiness was given a C. According to Ron Gula (Dark Reading, 2015), CEO of Tenable Network Security, "What this tells me is that while security innovations solve specific new challenges, practitioners are struggling to effectively deploy an overarching security strategy without gaps between defenses."

The idea that organizations are lacking effective solutions is further demonstrated in a recent healthcare organization survey conducted by consulting firm KPMG. According to the KPMG (2015b), "25% of respondents surveyed by KPMG say that, based on their organization's current protection systems, they don't have or don't know their capabilities, in real time, to detect if their organization's systems are being compromised." This finding by KPMG is not surprising since a common theme throughout the past several years has been that organizations are normally notified by a third party that they have a data breach. As show in a recent Trustwave (2015) report, it was discovered that 81% of breached organizations did not detect the breach themselves.

Based on these statistics, it is apparent that the cybersecurity solutions organizations have in place are not as effective as desired. Once again, the CSCs offer a roadmap for improving this deficiency. By working through the implementation of the CSCs, organizations would build a solution that is known to address 80-90% of the cybersecurity issues they face. It is easy to see how focusing investments on solutions built around a framework that has solid metrics for effectiveness is a good approach. It allows purchases to be strategic and offers an avenue for measuring the effectiveness of the purchase.

At a minimum, building a solution around the CSCs is certainly a much better approach to making cybersecurity solution investments in comparison to the ad-hoc approach that is often times taken despite the lack of known results. In fact, in many cases, many of the toolsets needed for building a solution that supports the CSCs are

already within an organization. In these cases, making the solution effective is simply a matter of focusing on the right data (i.e. the CSC requirements). Once the decision is made to align solutions around the capabilities outlined in the CSCs, organizations can also begin to use the CSCs to prioritize activities and build metrics for continuous improvement.

Essentially, by building a solution that aligns with the CSCs, an organization would be improving its cybersecurity posture across several critical areas in parallel. Areas such as effectiveness, measurements, and priorities will all see improvements by leveraging the CSCs.

2.4. Lack of Executive Support

If the recent string of notable breaches over the past few years is any indicator of the level of executive support for organizational cybersecurity readiness, you can easily infer that support has been lacking. However, as news feeds continue to report on the latest breach, executives are forced to become more aware of the problems that cybersecurity can bring to an organization (i.e. loss in brand value, fines, ransoms, etc.). Unfortunately, awareness does not equal action. In a recent survey published by CyberArk (Dimensional Research, 2015), the data shows that there is still plenty of room for growth in terms of executive support. The report found the following:

- 53% of CEOs make decisions without cybersecurity consideration
- 1/3 of CEOs are not briefed on cybersecurity risks
- 61% of CEOs do not know enough about cybersecurity
- Only 39% of security professionals feel fully supported by the CEO

Though these numbers are concerning, PricewaterhouseCoopers (PwC) found that there is growing visibility by executive boards on the issue of cybersecurity. This growth is giving organizations' cybersecurity professionals a voice. Given this platform, it is critical that each opportunity to share cybersecurity information with the board is used to communicate key issues in a manner that a board can understand (PwC, 2015, p. 21). The fact that business leaders (boards and executives) are focused on the variables that influence business value means simple, quantifiable concepts are keys to communicating cybersecurity issues.

By their nature, CSCs are not very complex ideas, which make them easily transferable into language fitting for a board. In fact, it is arguable that many of the key CSCs (Controls 1-5) are sound IT operational practices that have been in use for years. Thus, business leaders should already be familiar with the value they bring. In a recent survey by the SANS Institute, a great example of the CSCs ability to facilitate communication at the board level was shared:

> A new security manager at a mid-sized utility learned about the CSCs and saw their implementation as a way of getting his arms around the challenges and opportunities he would face in his new position. He first measured and mapped the utility's current posture in each of the 20 controls, produced an implementation score for each and charted the scores on a red/yellow/green satellite chart. He then worked out a 3-year plan to improve those scores substantially. His CIO asked him to brief the Chairman of the Board and the Executive Committee on the current status chart and the 3-year plan. The Chairman's reaction was remarkable; he said, "This is the first time a security person has made sense to me." (Tarala, 2014)

As shown in this example, using the CSCs as the medium for communication with executives is a great approach to beginning new dialogue, or improving existing dialogue. When a board member or executive asks those simple yet hard to answer questions such as, "How secure will these investments make us?", it would be much better to respond with, "They have been shown to reduce cybersecurity issues by up to 90%" or "Based on the latest CSC metrics, this purchase will reduce vulnerabilities in [insert area]." These types of responses show business leaders' confidence, competence, and understanding of a problem instead of answering the question using untrusted data, or no data at all.

2.5. Leadership Skills Gap

It is no secret that leadership starts at the "top" of an organization and permeates throughout the entire organizational culture (Chambers & Stewart, 2015). However, after over a decade of spending and effort, the level of effectiveness that has been seen in the cybersecurity space leads one to question the type of skillset required for cybersecurity leaders (Sileo, n.d. & Krebs, 2015). This leadership shortfall is evident in several

research papers sponsored by the Pell Center for International Relations and Public Policy (2016), which clearly show that cyber leadership is lacking in both public and private institutions around the world. Granted, leaders are the result of their experiences and the cyber domain is very new so it is arguable that the skillset required for effective cyber leadership is still being defined and has some maturing to do in comparison to other professional domains.

Leaders need the ability to adapt to a new environment, in this case the cyber environment (McChrystal, 2011). They need to identify opportunities to improve their current situation and then capitalize on them. Cybersecurity leaders do not need to have an engineering background but they need to be able to see the critical cybersecurity areas their organizations need to focus on and develop strategies to address them. According to Conti and Raymond (2011), "leading cyber warriors takes a different type of leader, one who is comfortable in the inherently technical cyber domain, appreciates technical expertise, and understands the personality types, creativity, culture, motivations, and intellectual capability of cyber warriors."

Considering the aforementioned concepts and the fact that most universities are still developing ways to address the cyber leadership gap by modifying graduate programs to include cybersecurity as a topic, it will take some time before the majority of organizations are led by people with a good amount of cybersecurity awareness (Spidalieri, 2013, p. 2). However, leaders who are currently lacking this awareness or trying to improve upon their existing awareness but struggling to identify critical areas of focus for cybersecurity efforts can leverage the CSCs (Tripwire, n.d.).

The CSCs, by their very design, are a perfect "on-ramp" for those leaders trying to address the cybersecurity learning curve that is readily apparent in organizations. The CSCs offer the following key tenants that make them extremely useful for leaders:

- They are easily understood
- They focus on root cause analysis
- They can be easily measured
- They encourage automation
- They are tied to a known metric of directly combatting cyber threats (SANS, n.d.)

Keeping the aforementioned tenants of the CSCs in mind, identifying opportunities to improve a leader's current situation becomes much more attainable. The ability to improve is attainable because the amount of cyber visibility a leader has is increased exponentially. With the increased visibility, leaders become better informed allowing them to develop effective strategy improvements with confidence. Once the strategies are in place, the increased visibility also allows for continued monitoring of the execution and progress of the strategies. This ensures those people responsible for the various efforts can be held accountable for their action, or inaction.

2.6. Organizational Maturity

Keeping in mind the areas described in the aforementioned sections, and the growing need for cyber resilience, it is apparent that organizations have a critical necessity to increase their overall level of cybersecurity maturity (Krebs, 2015a & The Economist, 2015). This idea is further reinforced by research conducted by the World Economic Forum (2014, p.16) who concluded that only 5% of those surveyed were considered mature for cyber risk management. Further, recent research from the Ponemon Institute (2015, p.22) concluded that a combined total of only 20% of U.S. local, state, and federal government entities are considered mature in their approach to cyber security. RSA (2015, p.4) also provided supporting data by concluding that 75% of those surveyed have significant cybersecurity risk exposure.

The alarming points just discussed show further evidence that fundamental cybersecurity practices are still are not being exercised in the majority of organizations around the world. The lack of fundamental cybersecurity practices is not only extremely concerning from a cybersecurity perspective, but also a business perspective. According to Lute (2014), "Over the long term, companies that succeed financially always seem to focus on the basics of business first – and keeping customers' data safe is one of the most important business basics." Using the concept of "the basics" as the foundation for achieving cybersecurity maturity, senior leaders should make sure to understand how their organization stacks up to the following questions:

- Do we know what is connected to our company's systems and networks?
- Do we know what is running, or trying to run on our systems and networks?

- Do we limit and manage the number of people who have the administrative privileges to change, bypass, or override our IT security settings?
- Do we have in place continuous automated processes backed by security technologies that will allow us to prevent most breaches, rapidly detect all that do succeed, and minimize damage to our business and customers?
- How would we demonstrate this to ourselves and to others? (Lute, 2014)

As can be seen, these questions are basic in nature. However, by being able to confidently answer "yes" to these questions, organizational leaders can rest assured in knowing they have cybersecurity visibility throughout their respective environment. This visibility is a key differentiator between mature and non-mature organizations. In the maturity chart below, it can be seen how visibility comes into play at levels 4 and 5 of the security model with tenants such as effective metrics, info-centric approach, and a risk-aware culture.

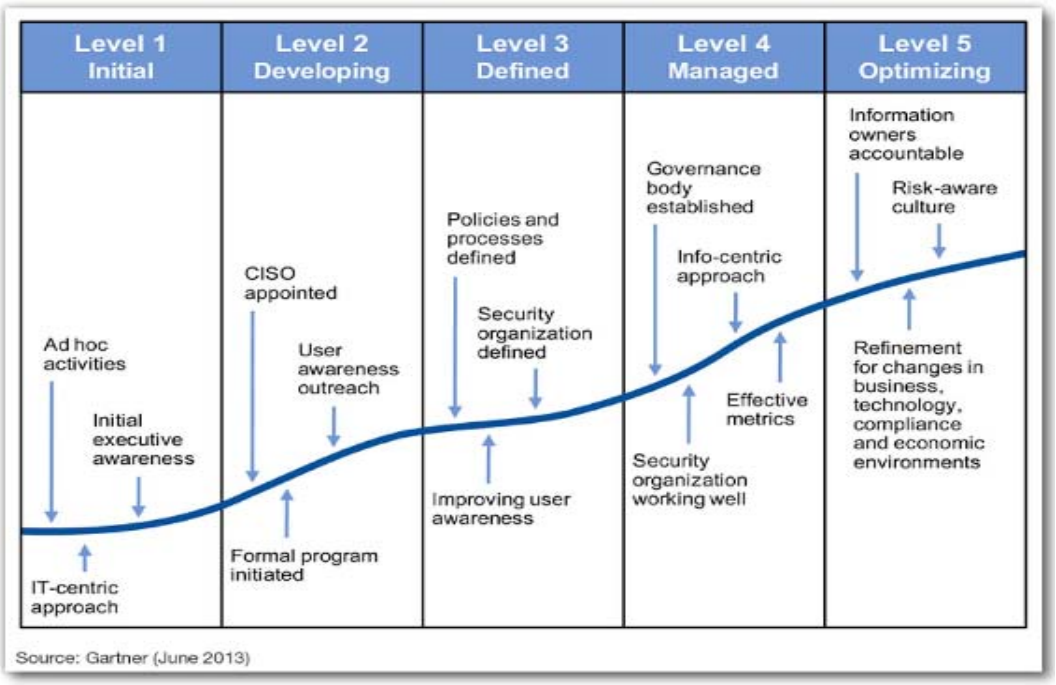

Figure 3: Defined Information Security Score Levels (Acohido, 2015)

The CSCs are a great resource when it comes to achieving the level of visibility needed to achieve maturity. They not only answer those basic questions on the path to maturity, described above, but also focus on continual improvement, increased awareness, automation, efficiency and effectiveness, and several other areas that aid

organizations in achieving cybersecurity maturity. Looking at the latest list of the CSCs (Version 6.0) referenced in Appendix A, it can be seen how the controls have an over-arching theme of knowing, managing, and testing your environment. All of these activities are critical for organizations with a desire to move from a non-mature state to a mature state.

3. The Critical CSCs

In a recent presentation given by Rob Joyce (2016), Chief of the National Security Agency's Tailored Access Operations (TAO) organization, he began his presentation with a very insightful and fundamental statement, "If you really want to protect your network, you have to know your network." Joyce's statement is obviously a very basic concept yet it does an excellent job of summing up what is needed if an organization truly wants to protect itself from cyber threats – a thorough understanding of the environment it intends to protect. Throughout his presentation, Joyce continued to describe several areas of understanding that are particularly important for network defense such as knowing what is running on the network, secure configurations, thorough software patching, and managed administrative privileges (Joyce, 2016).

In addition to Joyce's recommendations, several other efforts that share these same recommendations can be found. For example, the Australian Signals Directorate has the Top Four Mitigation Strategies to Protect Your ICT System (ASD, 2016). The DHS has the Continuous Diagnostics and Mitigation programs (DHS, 2015). The most recent effort is by the Center for Internet Security and National Governors Association Governors Homeland Security Advisors Council who have the National Campaign for Cyber Hygiene (CIS, n.d.). In keeping with the aforementioned concepts relayed by Joyce and other reputable sources, we will discuss the details of the first five CSCs.

The first five CSCs are known as "Foundational Cyber Hygiene" (CIS, 2015, p. 3). They are the CSCs that lay the groundwork for understanding and protecting the network. Essentially, they provide the necessary elements for a sound organizational cybersecurity foundation. The first five CSCs are as follows:

- CSC 1: Inventory of Authorized and Unauthorized Devices

- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges

3.1. CSC 1: Inventory of Authorized and Unauthorized Devices

Systems are constantly being added and removed from networks, which offers opportunities for bad actors to exploit weaknesses in system configurations. In order to manage this dynamic behavior, an organization needs to set a baseline for what assets are authorized to connect to its network. Once a "known good" asset baseline is established, it can be compared to future baselines looking for unexpected deltas. This particular control is really the foundation for the remaining controls because one cannot secure what one does not know about. The bottom line is that anything with an IP address on an organization's network should be inventoried (CIS, 2015, p. 6-7).

From an executive perspective, two fundamental questions should be asked to assess the state of the organization in relation to this control:

- Has the organization implemented scanning tools (active & passive) to identify all the devices attached to the network?
- Has the organization implemented a Network Access Control (NAC) solution, which requires certificates, to authenticate devices before they can connect to the network? (AuditScripts, n.d.)

The entity relationship diagram below offers a systems view of the types of activities, components, and information that are needed to support this control. Additional details regarding this CSC and others can be found using the references in Appendix A.

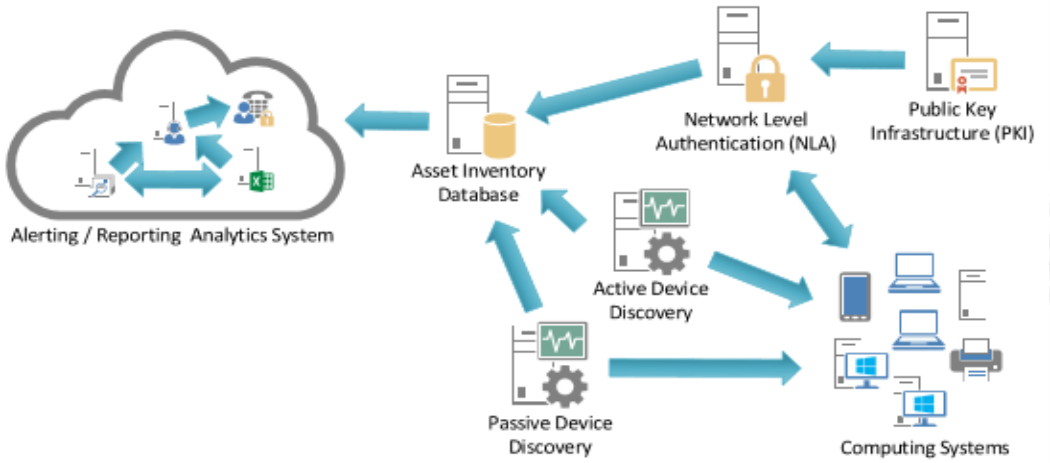

Figure 4: CSC 1 System Entity Relationship Diagram (CIS, 2015, p.8)

3.2. CSC 2: Inventory of Authorized and Unauthorized Software

Once an organization has a process in place to continuously inventory for authorized and unauthorized devices, it can begin the process of inventorying for authorized and unauthorized software. One of the most common avenues of attack for bad actors is exploiting an organizations lack of awareness when it comes to software running on their networks. However, this type of activity can be mitigated by creating an organizational specific "known good" software list – a whitelist. Once the list is created, execution of software on endpoints should be limited to the software on the list, and changes to software on the authorized list should be monitored. If software other than what is on the whitelist attempts to execute or make changes to authorized software are detected, an alert should be generated (CIS, 2015, p. 9-10).

From an executive perspective, two fundamental questions should be asked to assess the state of the organization in relation to this control:

- Has the organization implemented scanning tools to identify all software applications installed in the organization?
- Has the organization implemented a software whitelisting tool that only allows authorized software programs to execute on the organization's systems? (AuditScripts, n.d.)

The entity relationship diagram below offers a systems view of the types of activities, components, and information that are needed to support this control.

Additional details regarding this CSC and others can be found using the references in Appendix A.

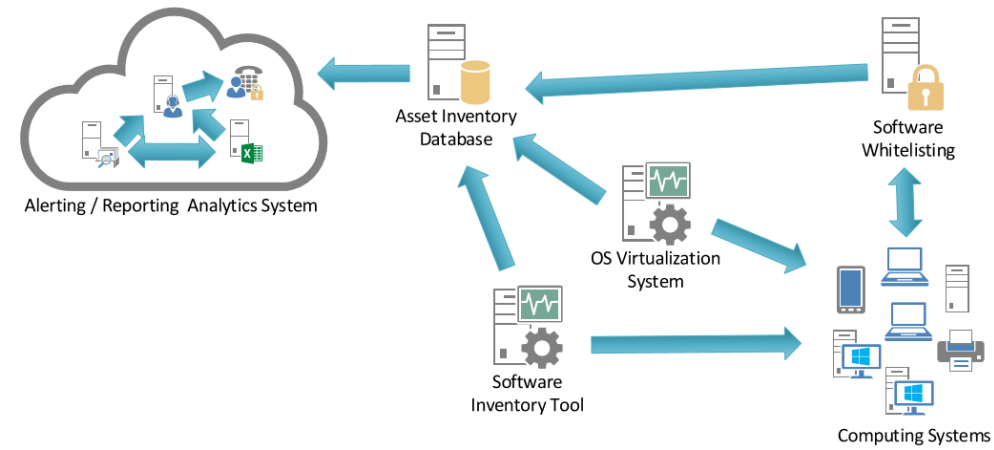

Figure 5: CSC 2 System Entity Relationship Diagram (CIS, 2015, p.11)

3.3. CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Ensuring an organization is using secure configurations on its computing platforms is extremely important. Bad actors will leverage misconfigurations in both applications and the operating systems that host them to compromise organizational computing platforms. With a thorough understanding of what is running on an organization's network, provided by CSCs 1 and 2, ensuring the secure configuration of hardware and software assets becomes manageable. It is best to begin this process by developing a standard image, or images (for large enterprises), using industry recognized hardening guides. After the standard image is developed and deployed, it should be monitored for changes. It is not enough to "set and forget" the configuration settings. The settings must be actively enforced throughout the organizational enterprise to avoid "security decay" resulting from patching and updates (CIS, 2015, p. 12-14).

From an executive perspective, two fundamental questions should be asked to assess the state of the organization in relation to this control:

- Has the organization implemented scanning tools to identify any misconfigured security settings on systems in the organization?
- Has the organization implemented a security setting configuration enforcement system on the organization's systems? (AuditScripts, n.d.)

The entity relationship diagram below offers a systems view of the types of activities, components, and information that are needed to support this control. Additional details regarding this CSC and others can be found using the references in Appendix A.

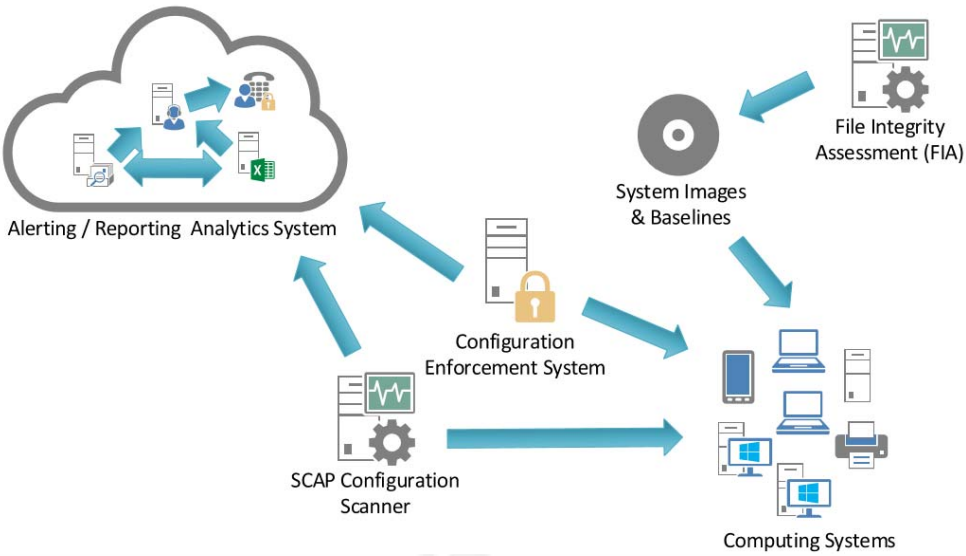

Figure 6: CSC 3 System Entity Relationship Diagram (CIS, 2015, p.15)

3.4. CSC 4: Continuous Vulnerability Assessment and Remediation

In addition to actively enforcing secure configurations, organizations must ensure they have a continuous patch management system. Security patches and updates are continuously published by vendors, researchers, etc., to correct flaws in software. Once the flaw or patch is published, bad actors begin to develop exploits for the specific weakness. Until an organization patches for this weakness, they remain vulnerable to exploit. Scanning should be done on a weekly basis, at minimum, for both code and configuration vulnerabilities. Scanning should be automated and performed with an authenticated account. The results of successive scans should be compared to ensure computing assets are being properly patched (CIS, 2015, p. 16-19).

From an executive perspective, two fundamental questions should be asked to assess the state of the organization in relation to this control:

- Has the organization implemented scanning tools to identify any software vulnerabilities on systems in the organization?

- Has the organization implemented an automated patch management system to continuously update the organization's systems? (AuditScripts, n.d.)

The entity relationship diagram below offers a systems view of the types of activities, components, and information that are needed to support this control. Additional details regarding this CSC and others can be found using the references in Appendix A.

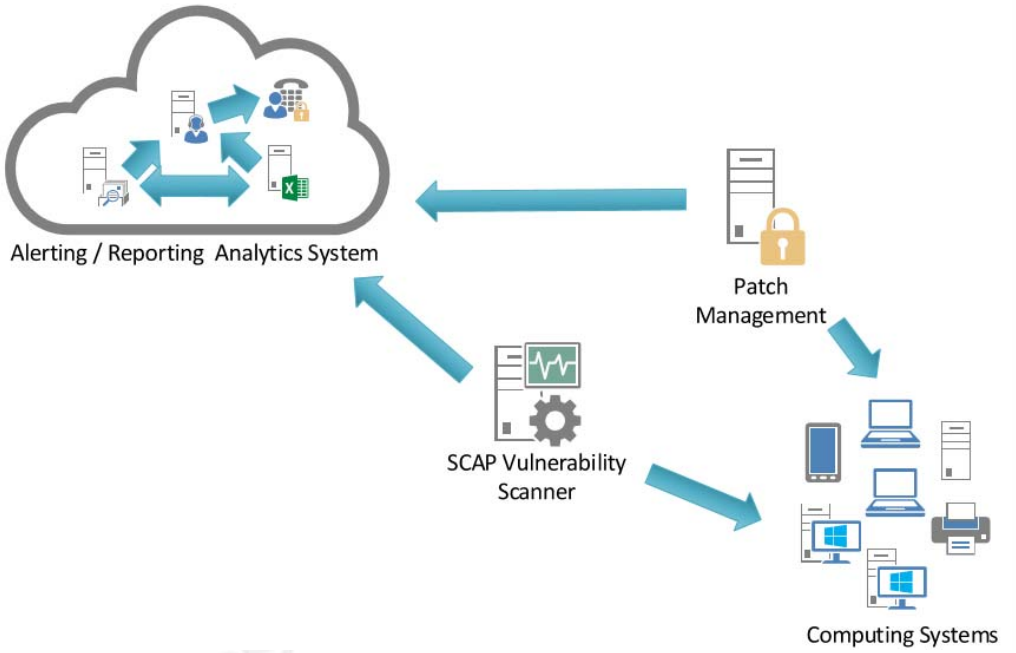

Figure 7: CSC 4 System Entity Relationship Diagram (CIS, 2015, p.19)

3.5. CSC 5: Controlled Use of Administrative Privileges

With controls one through four providing overall visibility of an enterprise's systems and configurations, the next area of concern is the level of privileged access to those systems. One of the most common activities by bad actors is to exploit unmanaged administrative privileges to gain access and move around within an organization. As such, it is critical that extreme focus is placed on managing these privileges. Administrative privilege should be minimized as much as possible to create a baseline for comparison – this includes operating system and application accounts on all networked devices. If adjustments are made to the baseline, an alert should be generated and investigated. Additionally, anomalous behavior around privileged access should be monitored. These include attempts to access password files, unauthorized attempts to

logon to systems with administrative accounts, unauthorized attempts to change administrative passwords, or unauthorized attempts to add users to the administrators group (CIS, 2015, p. 20-22).

From an executive perspective, two fundamental questions should be asked to assess the state of the organization in relation to this control:

- Do we limit and track the people who have the administrative privileges to change, bypass, or override our security settings? (CIS, 2015, p. 79)
- Are all administrative accounts on desktops, laptops, and servers authorized by a senior executive? (CIS, 2015, p. 20)

The entity relationship diagram below offers a systems view of the types of activities, components, and information that are needed to support this control. Additional details regarding this CSC and others can be found using the references in Appendix A.

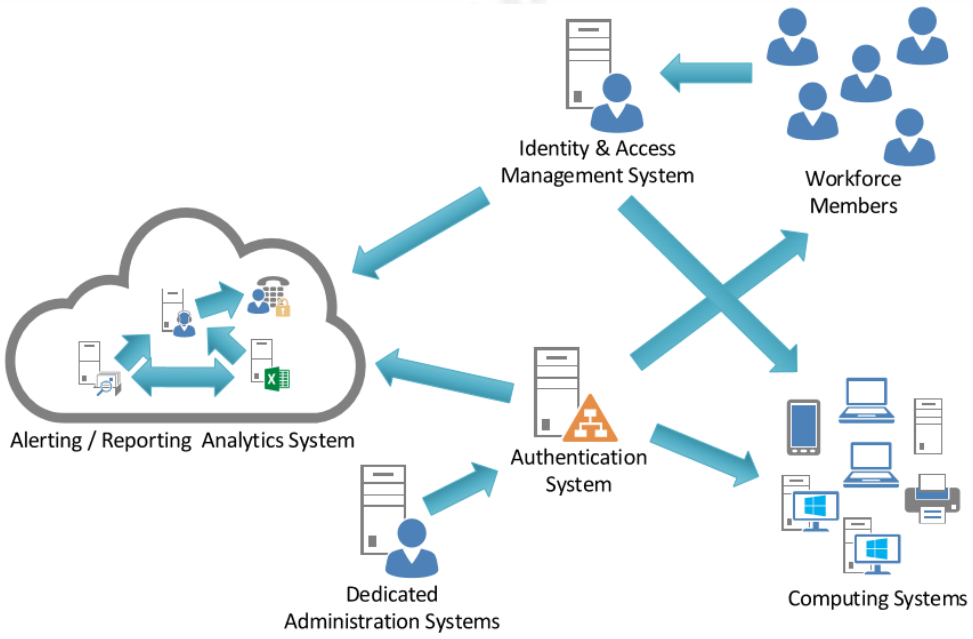

Figure 8: CSC 5 System Entity Relationship Diagram (CIS, 2015, p.22)

4. Conclusion

While the cybersecurity community continues to find ways to improve upon defensive technologies in order to increase breach detection and response capabilities, it

is important that organizations ensure they have a strong cybersecurity foundation. In addition to having a strong foundation, as a leader in the cybersecurity space, the importance of getting a comprehensive understanding and visibility of the information infrastructure has never been more important. Unfortunately, much of the latest data does not indicate that organizations have a strong foundation or the needed visibility to lead effective cybersecurity.

The data, instead, indicates that organizations lack proficiency in several strategic and managerial cybersecurity functions. This is an extremely disconcerting point because these higher level/foundational capabilities set the tone for the lower level/tactical response. Thus, if the functions that set an organization's cybersecurity foundation are flawed, it is very likely that the solutions they choose will be flawed, too.

The CSCs offer a framework that provides the critical visibility needed to aid in strategy development and manage existing organizational environments. By leveraging the CSCs to improve upon the areas described in this paper, organizations can have confidence in knowing that they are moving toward a resilient cybersecurity architecture. A resilient architecture that is prepared for continuous improvement and adaptable to the latest cybersecurity threats.

5. Reference

Acohido, B. (2015, May). Improving Detection, Prevention, and Response with Security Maturity Modeling. Retrieved from https://www.sans.org/reading-room/White papers/analyst/improving-detection-prevention-response-security-maturity-modeling-35985

AuditScripts. (n.d.). Critical Security Control Executive Assessment Tool (v.6a). Retrieved from http://www.auditscripts.com/projects/critical-security-controls/

Australian Signals Directorate (ASD). (2016). *Top 4 Mitigation Strategies to Protect Your ICT System*. Retrieved from http://www.asd.gov.au/publications/protect/top_4_mitigations.htm

Brookings Institution. (2013, February). Bound to Fail: Why Cyber Security Risk Cannot Simply Be "Managed" Away. Washington, DC: Langer, R., & Pederson, P. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2013/02/cyber-security-langner-pederson/cybersecurity_langner_pederson_0225.pdf

Center for Strategic and International Studies (CSIS). (2015, December 11). *Significant Cyber Incidents Since 2006*. Retrieved from http://csis.org/files/publication/151211_Significant_Cyber_Events_List.pdf

Center for Internet Security (CIS). (2015). *The CIS Critical Security Controls for Effective Cyber Defense Version 6.0.*

Center for Internet Security (CIS). (2016). *WELCOME TO THE CIS CONTROLS.* Retrieved from https://www.cisecurity.org/critical-controls.cfm

Center for Internet Security (CIS). (2016b). *Where have the CIS control been successfully implemented?* Retrieved from https://www.cisecurity.org/critical-controls/faq/#toQuestion

Center for Internet Security (CIS). (n.d.). *CYBER HYGIENE*. Retrieved from https://www.cisecurity.org/cyber-pledge/

Chambers, J. & Stewart, J.N. (2015, July, 13). Why Cybersecurity Leadership Must Start At The Top. *Forbes*. Retrieved from http://www.forbes.com/sites/frontline/2015/07/13/why-cybersecurity-leadership-must-start-at-the-top/#5af3a2234f3e

Childs, M. (2015, March 30). COMPLIANCE VS SECURITY. Retrieved from https://www.rooksecurity.com/compliance-vs-security/

Conti, G. & Raymond, D. (2011, July 11). Leadership of Cyber Warriors: Enduring Principles and New Directions. Small Wars Journal. Retrieved from http://www.rumint.org/gregconti/publications/811-contiraymond.pdf

Dark Reading. (2015, November, 17). Practioners Give Global Cybersecurity a "C" *According to New Research from Tenable Network Security*. Retrieved from http://www.darkreading.com/practitioners-give-global-cybersecurity-a--c--according-to-new-research-from-tenable-network-security/d/d-id/1323180

Department of Homeland Security (DHS). (2015, November 6). Continuous Mitigation and Diagnostics. Retrieved from http://www.dhs.gov/cdm

Dimensional Research. (2015). *The Gap Between Executive Awareness and Enterprise Security*. Retrieved from http://lp.cyberark.com/rs/316-CZP-275/images/CyberArk-Dimensional-Security-Survey-Report-12_05_15.pdf

Dumont, C. (2014, March, 14). Council on Cybersecurity 20 Critical Security Controls. Retrieved from https://www.tenable.com/sc-dashboards/council-on-cybersecurity-20-critical-security-controls-dashboard

Eubanks, R. (2011, August 10). A Small Business No Budget Implementation of the SANS 20 Security Controls. Retrieved from https://www.sans.org/reading-room/whitepapers/hsoffice/small-business-budget-implementation-20-security-controls-33744

Finn, D. S., & McCulloch, G. W. (2015). COMMENTARY: WHAT CISOs ARE UP AGAINST IN 2015. *Health Management Technology*, *36*(1), 4.

FINRA. (2015, February). Report on Cybersecurity Practices. Retrieved from https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

Gartner. (2015, September 23). *Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015.* Retrieved from http://www.gartner.com/newsroom/id/3135617

Gilligan, J. (2013, October). *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*. Retrieved from http://www.afcea.org/committees/cyber/documents/CyberEconfinal.pdf

Giles, M. (2014, July 12). Defending the digital frontier. *The Economist.* Retrieved from http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals

Goche, M., & Gouveia, W. (2014, January 15). *Why Cyber Security Is Not Enough: You Need Cyber Resilience*. Retrieved from http://www.forbes.com/sites/

sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/#2715e4857a0b1bd33e695799

Harris, K.D. (2016, February). CALIFORNIA DATA BREACH REPORT. FEB RUARY 2016. Retrieved from https://oag.ca.gov/breachreport2016#findings

Krebs, B. (2015a). What's Your Security Maturity Level? *Krebs on Security.* Retrieved from http://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/

Krebs, B. (2015b). At Experian, Security Attrition Amid Acquisitions. *Krebs on Security*. Retrieved from http://krebsonsecurity.com/2015/10/at-experian-security-attrition-amid-acquisitions/

Identity Theft Resource Center (ITRC). (2014). *ITRC Breach Statistics 2005 – 2014*. Retrieved from http://www.idtheftcenter.org/images/breach/MultiYear Statistics.pdf

Identity Theft Resource Center (ITRC). (2015). *Identity Theft Resource Center Breach Report*. Retrieved from http://www.idtheftcenter.org/images/breach/ITRCBreach StatsReportSummary2015.pdf

Joyce, R. (2016). *Disrupting Nation State Hackers*. Retrieved from https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce

Korn Ferry Institute. (2014). Adding cybersecurity to the boards risk portfolio. *KFMC 100.* Retrieved from https://www.kornferry.com/media/sidebar_downloads/KFMC-100-Cybersecurity-for-Boards.pdf

KPMG. (2015, December). Cybersecurity: A failure of imagination by CEOs. Retrieved from https://www.kpmg.com/NL/nl/IssuesAndInsights/Articles

Publications/Documents/PDF/IT-Risk-Advisory/Cyber-Security-A-failure-of-imagination-by-CEOs.pdf

KPMG. (2015b). *HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities*. Retrieved from https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

Lobel, M., & Loveland, G. (2012). *Cybersecurity the new business priority*. Retrieved from http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.html

Lute, J.H. (2014, December 29). Is the Sony hack corporate America's cybersecurity wakeup call?. *Fortune*. Retrieved from http://fortune.com/2014/12/29/is-the-sony-hack-corporate-americas-cybersecurity-wakeup-call/

McChrystal, S. (2011, March). *Listen, learn…then lead*. Retrieved from https://www.ted.com/talks/stanley_mcchrystal?language=en

Millican, J.M. (2015). *Twenty Steps To Better Information Security*. Retrieved from http://www.isaca.org/chapters8/Silicon-Valley/Members/Documents/Conferences/2015%20Spring%20Conference/2-3%20John%20Millican%20%20-%20Twenty%20Critical%20Controls%20Overview.pdf

Pell Center for International Relations and Public Policy. (2016). *Cyber Leadership*. Retrieved from http://pellcenter.org/cyber-leadership/

Ponemon Institute. (2015). *State of Cybersecurity in Local, State & Federal Government.* Retrieved from https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-2563enw.pdf

PricewaterhouseCoopers (PwC). (2015). *The Global State of Information Security Survey 2016*. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

RSA. (2015). *Cybersecurity Poverty Index*. Retrieved from https://www.emc.com/collateral/ebook/rsa-cybersecurity-poverty-index-ebook.pdf

Sager, T. (2016, July 7). *Critical Security Controls: A Community Approach to Security Problems*. Retrieved from https://www.youtube.com/watch?v=DG792UjDhuo

SANS. (n.d.) *CIS Critical Security Controls: Guidelines*. Retrieved from https://www.sans.org/critical-security-controls/guidelines

Sileo, J. (n.d.). *Sony Cyber Attack: A Case Study in Cyber Leadership Failure*. Retrieved from http://www.sileo.com/sony-cyber-leadership-failure

Spidalieri, F. (2013, March 13). ONE LEADER AT A TIME: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat. Retrieved from http://www.salve.edu/sites/default/files/filesfield/documents/pell_center_one_leader_time_13.pdf

Splunk. (2014). *Splunk and the SANS Top 20 Critical Security Controls*. Retrieved from http://www.splunk.com/web_assets/pdfs/secure/Splunk-and-the-SANS-Top-20-Critical-Security-Controls.pdf

Tarala, J. (2014, September). *Critical Security Controls: From Adoption to Implementation*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-adoption-implementation-35437

Tenable. (2014). *Council on Cyber Security Critical Security Controls*. Retrieved from http://www.tenable.com/solutions/council-on-cybersecurity-critical-security-controls

The Economist. (2015, November 9). *Cybersecurity: The Cost of Immaturity*. Retrieved from http://ww2.cfo.com/cyber-security-technology/2015/11/cybersecurity-cost-immaturity/

The SANS Institute. (2015). *Security 566: Implementing & Auditing the Critical Security Controls – In Depth (Books 1-5).*

Tripwire. (2014, June 22). *Overcoming Internal Barriers to Adopting Cyber Security*. Retrieved from http://www.tripwire.com/state-of-security/featured/overcoming-internal-barriers-to-adopting-cyber-security-2/

Tripwire. (n.d.). *The Executives Guide to the Top 20 Critical Security Controls*. Retrieved from http://www.tripwire.com/register/the-executives-guide-to-the-top-20-critical-security-controls-key-takeaways-and-improvement-opportunities/showMeta/2/

Trustwave. (2015). *2015 TRUSTWAVE GLOBAL SECURITY REPORT*. Retrieved from https://www2.trustwave.com/GSR2015.html?utm_source=redirect&utm_medium=web&utm_campaign=GSR2015

United States Department of State. (2010, May). iPost: Implementing Continuous Risk Monitoring at the Department of State. Retrieved from http://www.state.gov/documents/organization/156865.pdf

World Economic Forum (WEF). (2014, January). Risk and Responsibility in Hyperconnected World. Retrieved from http://reports.weforum.org/hyper

connected-world-2014/wp-content/blogs.dir/37/mp/files/pages/files/final-15-01-risk-and-responsibility-in-a-hyperconnected-world-report.pdf

Appendix A

- For access to the latest CSCs as well as the latest measurements for the CSCs: https://www.cisecurity.org/critical-controls.cfm
- For access to CSC auditing tools and control mappings: http://www.auditscripts.com/projects/critical-security-controls/
- For training on the CSCs (SEC440 & SEC566): https://www.sans.org/
- For a list of products that support each of the CSCs: https://www.sans.org/critical-security-controls/vendor-solutions
- For possible low cost solutions for implementing the CSCs: https://www.sans.org/reading-room/whitepapers/hsoffice/small-business-budget-implementation-20-security-controls-33744
- For the CSCs Version 6 Poster: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf