Real-World Case Study: The Overloaded Security Professional's Guide to Prioritizing Critical Security Controls

Phillip Bosco

Real-World Case Study: The Overloaded Security Professional's Guide to Prioritizing Critical Security Controls

GIAC (GCCC) Gold Certification

Author: Phillip Bosco, PhillipBosco@gmail.com
Advisor: Stephen Northcutt
Accepted: December 22nd, 2016

Abstract

Using a real-world case study of a recently compromised company as a framework, we will step inside the aftermath of an actual breach and determine how the practical implementation of Critical Security Controls (CSC) may have prevented the compromise entirely while providing greater visibility inside the attack as it occurred. The breached company's information security "team" consisted of a single over-worked individual, who found it arduous to identify which critical controls he should focus his limited time implementing. Lastly, we will delve into real-world examples, using previously unpublished research, that serve as practical approaches for teams with limited resources to prioritize and schedule which CSCs will provide the largest impact towards reducing the company's overall risk. Ideally, the observations and approaches identified in this research paper will assist security professionals who may be in similar circumstances.

Introduction

In a modern world where high-profile breaches occur on a regular basis, more stress is placed on companies and security professionals to prevent their intellectual property and customer data from being plastered across the web or sold to the highest darknet bidder (Levin, 2016). Emerging technologies, such as the Internet of Things (IoT) and the Cloud, further complicate the task of protecting valuable assets. Security professionals are challenged every single day with the daunting task of keeping their networks secured. With the exponential rise in connected devices and sophisticated cyber-attacks, a security professional's ability to protect various systems becomes stunted due to the insufficient resources required for this overwhelming task (Gartner, 2015). Even the most passionate and dedicated security professionals experience difficulty in implementing the 20 Critical Security Controls (CSCs) due to the inundating threats that arise with each passing day.

When correctly applied, these 20 CSCs undoubtedly provide a great benefit to a company's ability to detect and defend against many of the common attacks that systems experience today (Platz, 2016). While steps to implement the CSCs are clear and highly practical, deciding which CSCs to prioritize and work with first becomes a serious challenge. The real-world case study explored in this text will serve as a framework to assist security professionals in determining various methods to prioritize which CSCs to implement that will yield the most mitigation potential for the least amount of precious resources expended. Along the path of prioritization and attempted risk reduction through applying the CSCs, many professionals encounter a series of obstacles that delay or prevent the successful application of security controls entirely (Wilson, 2016). Further utilizing this case study and other real-world examples, security professionals may gain new methods and strategic processes for overcoming seemingly insurmountable and stressful managerial interference.

1. Real-World Case Study

To emphasize the common challenges associated with securing company networks and prioritizing CSCs, analyzing real-world examples of organizations in similar

Phillip Bosco, PhillipBosco@gmail.com

circumstances provide the greatest value with implementing fixes inside of one's methodology and workflow. The company discussed in this text found themselves breached by malicious actors, with their sensitive customer data extracted, customer websites offline, and their production servers wiped. This previously unpublished and original research, paired with the analysis of the struggles faced by a breached company, contribute a fresh perspective in the ongoing battle of securing our most sensitive information.

1.1. Company Background Info

The company, referred to as Portland Design & SEO (Portland Design), contained between 50-100 employees and provided website design, hosting, and Search Engine Optimization (SEO) to their customers. Due to Portland Design's hosting and in-house website building services, they hosted many of their client's sites on their systems that they maintained themselves. While the company employed many website developers and sales engineers, they hired only one individual (Johnson) who served primarily as the go-to security professional. On occasion, Portland Design would contract out some of their work, including as-needed server maintenance.

1.2. The Breach

It was 2 am on a Friday evening when Johnson awoke to the sound of his phone buzzing against his nightstand. After grabbing his phone and focusing his sleepy eyes on the screen, he found a series of missed calls, voicemails, and a sea of emails, which all seemed to indicate a highly urgent situation. Many of Portland Design's customers had begun reporting that their websites were offline and unavailable, which for many, correlated directly with lost revenue. Johnson's other late-night emails and alerts were from Pingdom, the website monitoring service, which stated many of Portland Design's resources were offline (Pingdom, 2016). Initially, Johnson and Portland Design assumed that the issues could be related to a power outage or their ISP encountering connectivity issues. However, when Johnson attempted to authenticate to the remote management host to determine the cause of the outages, he could connect with the host but was denied access.

In a state of panic and confusion, Johnson drove down to the local office where Portland Design's servers were stored and maintained. Johnson used a backdoor account configured on the servers that could only be granted to local users and authenticated to the server successfully. Still unsure of the direct cause of this disruption, Johnson's priority was to restore the affected customer sites as quickly as possible. The web hosting services and processes inside of the server were fully operational, but when Johnson checked the local directories that stored the customer's sites, he found that nearly all websites had vanished. Johnson displayed the running processes and discovered a remotely connected user running the shred command on the directory containing the customers' sites. To reduce the risk of deletion facing the remaining sites, Johnson powered down the server immediately. While this may have temporarily mitigated further damage caused by the breach, it effectively brought down the all the customer sites for Portland Design.

1.3. How Severe was the Damage?

After most of the panic had settled and an investigation took place, Portland Design assessed the damages that occurred during this breach. The realization of actual damages reach beyond the destruction of company property and assets and is not always something tangible. As was the case with Portland Design, the company began assessing damage in short-term, then eventually medium and long-term increments. Depending on the type of breach that a company faces, it may not always be possible to anticipate the long-term damage effects of a compromise until an unknown amount of time passes and the impacts become fully realized.

1.3.1. Customer Sites Offline and Unavailable

It did not take long for Portland Design to find that many of their clients' sites were not only taken offline and unavailable, but the malicious actor also deleted them from the production web server. Johnson caught the breach early enough before all the customer sites faced full deletion, but the malicious actor had already removed over 92% of them.

1.3.2. Customer Sites Deleted and No Recent Backups

The harsh reality of a malicious actor deleting client websites forced Portland Design to rely on backups of the sites, which were scheduled to take place automatically three

times a week. The timestamps on the backed up files showed that they were indeed archived three times a week, but the last successful backup took place over seven months ago. This unfortunate situation occurred due to Portland Design's "hostname overhaul" project from seven months earlier, whereby they wanted to rename all their servers using a predictable hostname scheme. As they changed many of the hostnames, including that of the backup server archive destination, it prevented future backups from taking place. Portland Design had alerts in place sent to Johnson and a few others when successful backups occurred, but not in the case of unsuccessful or failed backups. With an already overwhelming list of responsibilities, Portland Design's employees did not notice the lack of alerts sent to their inboxes, which gave them the incorrect assumption that backups had been occurring automatically over the course of the past seven months.

1.3.3. Customer Data Potentially Stolen

Upon further inspection of the breach, the remote malicious user had moved laterally to a SQL database server. The malicious actor deleted the SQL server logs and bash history; therefore, Portland Design could not confirm whether the malicious actor stole customer data. Fortunately for Portland Design, they did not store customer payment data themselves since they handled all financials via third-party payment vendors, such as PayPal. They did, however, store customer names, email addresses, physical addresses, phone numbers, and information about the services provided to each of Portland Design's customers. While this data was encrypted, a valid SQL user account with the appropriate access permissions can extract decrypted data. At that rate, Portland Design assumed that the malicious actor stole all the stored customer data.

1.3.4. Possible Malware Infection

The user account that the attacker utilized was part of the "super users" group on the web and SQL servers. While Portland Design did not identify irrefutable evidence that the malicious actor installed malware, rootkits, or other backdoors on the system, Portland Design took precaution to ensure any remnants of the threat was eliminated by wiping the system and restoring from old, but known-good backups. If updated backups were available, this would have minimized the impact associated with wholly clearing the systems.

1.3.5. Portland Design Financial Impact and Customer Trust

Portland Design lost revenue and their customers' trust following the breach. Not surprisingly, customers reported dissatisfaction regarding their revenue-generating websites unexpectedly going offline for extended periods of time. Furthermore, when Portland Design eventually brought the sites back online, many of them were outdated, and some customer sites became lost entirely (and had to be haphazardly restored from leftover project files located on various Portland Design employee workstations). These disruptions alone caused Portland Design to lose some of their short and long-term customers. Lastly, once Portland Design alerted their clients that a confirmed compromise occurred, several more customers discontinued their business with the company.

2. Breakdown of Breach Causes

"Those who build walls think differently than those who seek to go over, under, around, or through them." - Paul Wilson (Hadnagy, 2011)

The analysis of the Portland Design breach shed light on a few critical issues that empowered the malicious actor to move through the various servers, wreaking utter havoc effortlessly. Had Portland Design identified and remediated the security problems before the breach, it would have likely assisted Portland Design in resisting the attack at that moment; however, they would still be highly likely to experience the same attack (or a similarly sophisticated attack) at a later date in time. Increasing a company's resistance to cyber-attacks involves more than the ability to identify and remediate individual issues, but instead requires a structured approach and methodology to provide adequate protection continually. The implementation of the CSCs offers a comprehensive, defense-in-depth driven security posture to any company that adopts them. Some information security professionals may not be keenly aware of the CSCs or how to implement them; however, this was not the story for Portland Design. Johnson possessed a complete understanding of the critical controls, but Portland Design just failed to comply with them. If purely knowing the CSCs is half of the battle, having enough resources and knowledge to prioritize implementation of them becomes the tougher second half of this challenge. While the instance of the Portland Design breach may be unique, the

consequences of failing to implement the critical controls is not. Any organization, big or small, has an opportunity to preserve revenue and brand imaging through the successful adoption and appropriate prioritization of the CSCs.

In the primary research leading up to this paper, the author aggregated polling data from 14 different companies after performing a penetration test against their networks. The author conducted all surveys of the tested companies entirely during the year 2016. The post-assessment survey asked participants what the top two reasons were that they considered roadblocks to providing better protection for their networks. Figure 1 displays these results in a pie chart, with each company possessing the ability to place two votes each:

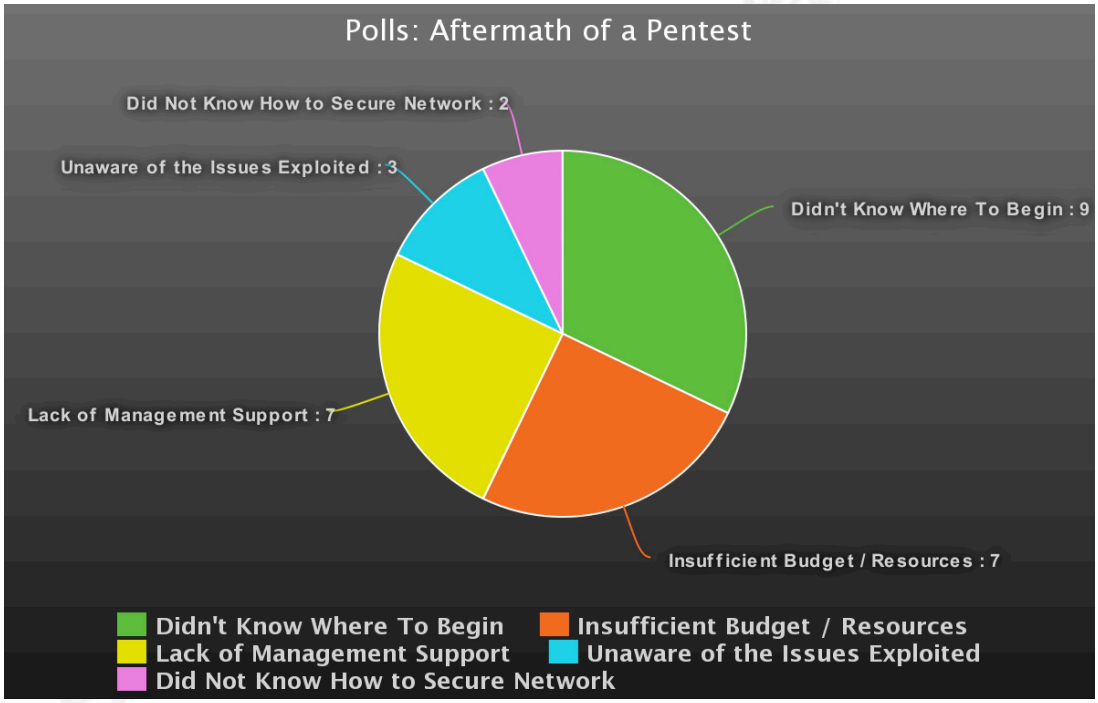

Figure 1: Post-Assessment Survey on Top Two Roadblocks Experienced

While the results of this post-assessment poll are relatively close, it helps to paint the story of the barriers commonly encountered by security professionals. The least referenced issue reported by the surveyed companies stated that they did not know how to secure their networks. The minimal entries for this category indicate that the other 92.9% of participants believed that they possessed the appropriate knowledge to secure their networks, but stumbled on other aspects that prevented them from doing so successfully. Using Portland Design as a framework that mirrors the struggles encountered by many

other similar companies, we can analyze some of these common roadblocks and identify how to overcome many of them.

2.1. Lack of Management Support

In recent years following high-profile breaches, such as the compromises of the United States government's Office of Personnel Management (Koerner, 2016) and Sony Pictures (Elkind, 2016), many companies have been allocating a larger budget and more resources to protecting their networks than ever before (Morgan, 2016). In other cases, budgets are still tight for the information security department, and additional resources cannot be afforded and allocated to the protection of their systems (Ashford, 2016). Irrespective of the exact cause, an information security department's efficacy significantly drops when they do not possess support from management. Management's support, or lack thereof, typically falls into two categories: Inability to Provide Resources or Failure to Provide Support.

2.1.1. Inability to Provide Resources

The Inability to Provide Resources category implies that management backs the information security team on some level, but is seemingly incapable of providing a desired level of support due to circumstances outside of their control. For example, management may fully support the information security team both emotionally and verbally, but may not have the actual budget required to render sufficient operational support. Even with the best intentions, sometimes management find their hands metaphorically tied behind their backs.

2.1.2. Failure to Provide Support

Often confused with the Inability to Provide Resources, management falls into the Failure to Provide Support category when they refuse to support the operations and requirements of the information security team. In many situations, this typically involves the refusal to provide additional resources to the information security team. The lack of support is often due to the management team's disinterest in the information security team regarding the amount of resources required for a department that does not customarily provide direct revenue to the company. Other times, the management team may not understand the critical importance of providing adequate resources to protect their

networks; however, the use of this excuse is dwindling due to the increasing frequency of high-profile attacks. The Failure to Provide Support category can fall into various degrees of intensity, and each organization's management team tends to have thresholds that determine which triggers will prompt them to provide some level of minimal support depending on how dire the impending situation is.

Per the original research conducted for this text and up to 18 months before the compromise, Johnson was on record stating his concerns involving his insufficient resources to protect the network and the sensitive assets thoroughly. He told management that his 14-hour daily schedule was not enough to perform all the duties assigned to him. While management verbally appreciated all his hard work and his passion for the company, they declared that they did not have the resources to allocate more to the information security department. Instead, management decided to invest more in sales, marketing, and website development due to the increasing customer demand, failing to recognize the proportionately rising risks. In this case, management possessed the necessary funds to increase the resources allocated to Johnson's department, but instead focused on growing the company capacity to serve additional customers.

2.2. Insufficient Resources

Usually a byproduct of the previous topic, insufficient resources are frequently a direct result of the lack of management support, as seen in the Failure to Provide Support category. If Johnson did not have management's support but possessed a few additional resources (extra personnel or additional funds), he may have been better equipped to begin implementing some of the CSCs. While an information security team will likely benefit from additional resources, they still might find their hands tied without management's direct support. In other cases, insufficient resources for the information security team may not be directly in management's control, as seen in the Inability to Provide Resources category. If this happens to be the case, it is important to leverage the existing support from management to create a blueprint of how you plan to allocate resources over an estimated future period. Detailing to management how you are using the small quantity of resources that you have control of to the best of your ability and how you are stretching it as far as possible will help give management confidence in you and any future investments in the security department. Additionally, stating all that you

can achieve with current resources and everything that you are unable to complete along with the associated risks is equally as paramount. With any risks that management deems severe enough to tackle, be prepared to detail progressive solutions and the costs involved, even if management provides only a small quantity of funds or other resources. It is just as imperative for management to see how the funds will be used as it is for them to evaluate the outcome if resources are not ultimately provided.

Even when security professionals communicate very clearly and management understands the risks, if the requested resources are non-existent than compromises will likely need to be made on both sides. For example, if one of the most significant risks facing an organization is due to outdated and obsolete software that requires the purchase of more licenses to upgrade, one may consider working with management to update only some of the software in incremental phases. In other words, rather than associating the cost and time of $10,000 and six months with mitigating this risk, a security professional can work with management to reduce some of this risk over the course of 12 months and only on the most sensitive systems. While this is not a replacement for a proper and comprehensive implementation of any security control, having a quality and communicative relationship with management and leveraging their existing support will ultimately minimize the risks linked with failures to implement the CSCs.

2.3. Lack of Communication

Becoming aware of the CSCs and establishing a desire to implement them in your organization is key to hardening your network against common attacks from malicious actors. Unfortunately, a desire to apply the CSCs and having the resources and means to proceed with the deployment plan are two very different things. As outlined earlier, Johnson was aware of Portland Design's lack of security and stressed to his management the unnecessary risk that this placed on the company from the inevitable onslaught of well-documented attacks from opportunistic cyber criminals. Johnson admitted, however, that he could have been more effective at communicating the risk to his management. When management seemed to focus only on business growth and revenue, Johnson states that he could have described the correlation of the overall business growth with the proportionate need for a growing information security team.

Other than resorting to "scare tactics" or encouraging an overly paranoid fear of getting breached, Johnson could have referenced recent breaches and how they had negatively affected customer trust and future business development. When management chooses only to look at the allocation of resources as it corresponds to growing the business in dollars and cents, it is important for security professionals to possess the ability to speak in terms that will resonate most with executives to influence their future decisions on supporting the security team. This robust approach is not a form of trickery or manipulation but serves to improve the quality of communication and overall understanding between the two parties.

3. Prioritizing the Critical Security Controls

To begin the planning stages for implementation of the Critical Security Controls, security professionals must first understand the various controls and the proposed method(s) of implementing them. As seen in the earlier examples, pure awareness of the Critical Security Controls is not enough to secure networks. There are many variables, such as management's support and available resources that come into play when attempting to implement the CSCs across a network. As for Johnson at Portland Design, he was aware of the CSCs but did not have management's support, the appropriate resources to implement them, or the know-how ability to prioritize which of the controls he should initiate before others. Fortunately, several methods are at a security professional's disposal that can be used to assist in the prioritization of Critical Security Controls.

3.1. Knock Out the Easy Ones

"If you can't fly then run, if you can't run then walk, if you can't walk then crawl, but whatever you do you have to keep moving forward." ― Martin Luther King Jr.

With a limited quantity of time and resources, security professionals often wonder which of the CSCs they should implement first to obtain the largest time versus value tradeoff. If unable to prioritize the CSCs by any other means, directly focusing on the controls that will be easiest to implement can put a company on a path to hardening to their network. This method is helpful when a corporation is unsure of the most useful

place to begin implementing controls and does not know where their limited resources would best serve. While this approach should not replace more robust medium and long term solutions, a series of quick and easy CSC wins are still a step in the right direction. Of course, the actual controls that one company might consider an "easy implementation win" might vastly differ from another. To best illustrate the relativity of an easy win for a company, we can compare a similar situation of two different companies.

A tightly-controlled network, like that of a government or hospital network, whereby each device must be registered and approved before being added to the domain might find it beneficial to add host-based antivirus software to each networked system. As this network is well-controlled by IT, it may be a matter of quickly pushing out a GPO that installs the new antivirus software on each of the workstations. Adding antivirus to all workstations may already be a high-priority CSC to implement for one company, but for others, this action item gets lost in the sea of overwhelming security to-dos. Conversely, assume that a second company maintains a more loosely controlled network and encourages a BYOD policy. To implement a compatible and efficient antivirus solution across a variety of devices, workstations, operating system versions, and patch levels could be a daunting task. Even if the security professional found a universal solution compatible with the greater majority of devices, identifying a method for installing and maintaining the solution may prove tedious. Implementation of this particular CSC for the BYOD company would indeed yield a great security benefit, but at the cost of a high quantity of time and resources. Instead, perhaps, the BYOD company could look to another item on their list of actionable security items and identify tasks that are much more manageable considering the resources at their disposal. Of course, if this BYOD company already sees malware on their workstations as a critical risk to their organization, then the substantial time commitment involved with implementing an antivirus solution across all their seemingly rogue workstations would be worth the high level of effort required. However, not all companies have a mature enough security posture to know what the most significant risks are to their organization.

3.1.1. Tackling Known Issues

If a company possesses a mature enough security posture, they may be able to sub-prioritize the implementation of the CSCs by addressing known issues first. Rather than

looking at the 20 CSCs as an intimidating list, a security professional can instead place prioritization on the known issues facing the organization. In the previous example, the mature security posture maintained by the BYOD company allowed them to identify malware on their devices as a significant risk to their business objectives. In this scenario, the company's time would not be best spent by only looking to the CSCs as a linear list of goals with each control carrying equal weights, but instead as a guide for practical implementation of the already-identified risks. These examples should not serve to understate any of the importance of any of the 20 CSCs, as each carries equal importance; However, the unique risks facing your organization will determine which controls security professionals should prioritize. When security professionals cannot utilize any other method of prioritization, moving forward with any actionable plan to mitigate threats becomes more beneficial than blindly walking through each of the CSCs in a linear fashion. Security professionals may identify known risks from a variety of sources, such as compliance audits, vulnerability scans, and penetration testing.

3.2. Penetration Tests, The All-Seeing Eye

Many companies inaccurately place emphasis on what they perceive to be the greatest threat facing their organization, which stems from a few misleading inputs. Some of the most significant contributions that lead to inaccurate assumptions come from the mainstream media, television shows, and movies whereby a massive breach occurs against a high-profile company. Based on which misleading inputs they follow most, they may feel that they need to place more emphasis on updating to the latest Windows security patches, or perhaps utilize their entire annual security budget to procure the newest firewall product to protect their external infrastructure. While patching and newer generations of products can both be potentially good things for companies, their time and effort may better be spent on another aspect of security entirely.

Often misinterpreted, another misleading and overwhelming input comes from a company's internal vulnerability scans. Many security professionals use vulnerability scanning inside of their networks to identify many of the misconfigurations and vulnerabilities that may increase the risk of sensitive data theft or a system compromise. Unfortunately, vulnerability scanning tools tend to lack context with the vulnerabilities that it identifies. Many internal scans may yield thousands of unique vulnerabilities and

70% or more of them may be rated severe or critical by the vulnerability scanning tool. Per the research referenced in Figure 1, the vast quantity of results from the scans leads to security professionals unable to determine where to begin resolving the discovered vulnerabilities. For example, a vulnerability scanning tool might identify two different highly-rated findings, one missing the infamous MS08-067 patch and the other vulnerable to 2014's Heartbleed vulnerability. Each of these vulnerabilities could potentially lead to a full compromise of a company's network, so prioritizing hundreds or thousands of vulnerabilities labeled similarly as "critical" just like these two can be challenging.

Penetration testing provides companies with value far beyond what vulnerability scans can. In the case examined above, a penetration tester might find that the MS08-067 finding is a false positive and the server vulnerable to Heartbleed is for HR's external server that deals with social security numbers and direct deposit data. However, the contrary may also be a reality, where the Heartbleed server hosts content that is only static and non-sensitive making this far less of a priority, while the MS08-067 vulnerability is facing the internet completely unrestricted. These specific details found during penetration tests assist the affected company in the efficient prioritization of which vulnerabilities and misconfigurations a security professional should remediate first (Kostadinov, 2016).

The benefits of using penetration testing go further than just prioritization of vulnerability scanning results, which typically only cover a small number of potential CSCs. In regards to the research conducted in Figure 1, several companies stated that penetration testing exploited issues that were previously unknown. If a company gives the penetration testers access to a broad scope that includes testing items such as electronic social engineering, physical facility testing, wireless testing, external network testing, and so on, penetration testing will assist in identifying which CSCs implementation would yield the most value. Year after year, a company may invest in updated operating systems, new firewalls, and WAFs; but a penetration test may reveal that a compromise of the entire network might be possible via a simple, non-sophisticated email phishing attack due to an overall lack of security awareness training among their employees. These types of penetration tests and scenarios assist in providing the

company feedback on which currently implemented CSCs are operating as intended and which ones are severely lacking. In the previous scenario, the company may now decide to spend their limited time and resources raising security awareness among their employees through training rather than using the funds excessively on a control that is already working as intended.

3.2.1. Gaining Management Support and Resources via Penetration Testing

As seen in the previous section, penetration tests are excellent in helping a company identify the weakest areas in their current security posture and detail which CSC implementations lack the desired efficacy. However, penetration tests can also help security professionals secure additional support from management (Tallent, 2016). If we reflect on Portland Design's breach, Johnson had not received an adequate level of management support and therefore was unable to implement CSCs due to lack of resources to assign to the tasks. Let us consider the effect that a penetration test could have revealed about the Portland Design company. If they had used some of their resources to schedule a penetration test, the assessment might have shown many of the weak areas that allowed the compromise to take place, before the actual breach. Additionally, if penetration testers thoroughly compromised Portland Design's network and demonstrated their ability to destroy the production websites of their clients, this would have served as a wake-up call of sorts to management who were previously hesitant to provide the security team with more resources. Sometimes a penetration test report that details how vulnerable their network is can deliver the concrete realization necessary for management to possess an altered perspective.

4. Conclusion

The task of securing increasingly complicated and diverse systems against a rapidly growing number of cyber-attacks is more challenging than ever before. Unfortunately, many security professionals find that this exponential rise in connected devices and refined attacks has left them with insufficient resources to adequately secure their systems. While the 20 CSCs provide companies with practical steps to protect themselves against various categories of common attacks, the actual ability to implement them is

delayed commonly due to the lack of sufficient resources or management support, as seen in the analysis of the Portland Design breach. While this original research provides recommendations for prioritizing the CSCs and overcoming common roadblocks faced by security professionals, security professionals use this information in parallel with the CSCs. As the CSCs mature one revision after the next with new attack techniques reshaping the way networks are defended, the next update of the CSCs may need to adapt to the difficulties encountered by security professionals by including methods for prioritizing the controls when they cannot apply them due to resource restriction, or other common challenges. Fortunately, a variety of practical methods exists for identifying which of the CSCs will yield the most risk mitigation for the least amount of resources exerted. While the exact approach may be unique, there are a few standard methods that a security professional can utilize to grow the security department of an organization. There are several methods to productively tackling issues related to the lack of management support, obtaining additional resources, and making strategic compromises to continually improving a company's security posture when lacking the proper assets. Some methods stressed the importance of enhancing the quality of communication between the security department and management. Other methods included completing some of the easier to implement CSCs as a way of continually moving forward with hardening the network and using penetration tests to identify which CSCs are working as intended and to provide valuable context to existing vulnerability scan data.

There is not a one-size-fits-all solution that can be recommended or implemented across the board; however, using strategic approaches and remedies to common problems faced by security professionals on a regular basis will help to grow the security posture of any company consistently. Many of the explored strategies involved overcoming obstacles when working with fewer resources than what is necessary and making compromises along the way. Possessing a realistic and practical plan, even when it may not be an entirely ideal solution, is far more effective than not having a solid plan or approach of any kind. With many of the challenges faced, appropriate prioritization of the overwhelming risks and endless security to-do lists is key to success. Ultimately, a less-than-ideal plan that strategically utilizes all available resources and adheres to a schedule agreed upon by the security team and management is superior to a full-blown theoretical

solution that never receives full support or the necessary funds, which never actually gets implemented. As demonstrated by the lone security professional who was equipped with all the right knowledge, but lacking the proper support, companies will succumb to cyber-attacks unless that think and act with security serving as their North Star. In many cases, adopting and, most importantly, effectively prioritizing the Critical Security Controls (CSCs) can fill the role of this North Star.

Phillip Bosco, PhillipBosco@gmail.com

References

Ashford, W. (2016, March 22). Cyber security budgets not rising in line with threats, say security pros. Retrieved from http://www.computerweekly.com/news/4500279662/Cyber-security-budgets-not-rising-in-line-with-threats-say-security-pros

Elkind, P. (2015, June 25). Sony Pictures: Inside the hack of the century. Retrieved from http://fortune.com/sony-hack-part-1/

Gartner. (2015, November 10). Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015. Retrieved from http://www.gartner.com/newsroom/id/3165317

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Indianapolis, IN: Wiley.

Koerner, B. (2016, October 23). Inside the OPM hack, the cyber attack that shocked the US government. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Kostadinov, D. (2016, October 5). Penetration testing benefits: Pen testing for risk management. Retrieved from http://resources.infosecinstitute.com/penetration-testing-benefits-pen-testing-for-risk-management/

Levin, A. (2016, July 28). 5 reasons you can't ignore this new rise in cyber crime. Retrieved from http://www.inc.com/adam-levin/5-reasons-you-cant-ignore-this-new-rise-in-cyber-crime.html

Morgan, S. (2016, January 27). Bank of America's unlimited cybersecurity budget sums up spending plans in a war against hackers. Retrieved from

Phillip Bosco, PhillipBosco@gmail.com

http://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#38dc1b9e434b

Pingdom. (2016). Pingdom Uptime Monitoring. Retrieved from https://www.pingdom.com/product/uptime-monitoring

Platz, J. (2016, May 18). Top 20 CIS Critical Security Controls (CSC) through the eyes of a hacker. Retrieved from https://www.optiv.com/blog/top-20-cis-critical-security-controls-csc-through-the-eyes-of-a-hacker-csc-1

Tallent, R. (2016, September 13). 10 reasons to pen-test your network. Retrieved from https://www.coresecurity.com/blog/10-reasons-to-pen-test-your-network

Wilson, T. (2016, July 15). Poor priorities, lack of resources put enterprises at risk, security pros say. Retrieved from http://www.darkreading.com/vulnerabilities---threats/poor-priorities-lack-of-resources-put-enterprises-at-risk-security-pros-say/d/d-id/1321308

Phillip Bosco, PhillipBosco@gmail.com

Last Updated: September 21st, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Cairo October 2019	Cairo, EG	Oct 19, 2019 - Oct 24, 2019	Live Event
Purple Team Summit & Training 2019	Las Colinas, TXUS	Oct 21, 2019 - Oct 28, 2019	Live Event
SANS Santa Monica 2019	Santa Monica, CAUS	Oct 21, 2019 - Oct 26, 2019	Live Event
SANS Training at Wild West Hackin Fest	Deadwood, SDUS	Oct 22, 2019 - Oct 23, 2019	Live Event
SANS Orlando 2019	Orlando, FLUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Amsterdam October 2019	Amsterdam, NL	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Houston 2019	Houston, TXUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS DFIRCON 2019	Coral Gables, FLUS	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Paris November 2019	Paris, FR	Nov 04, 2019 - Nov 09, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, COUS	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS Sydney 2019	Sydney, AU	Nov 04, 2019 - Nov 23, 2019	Live Event
SANS Mumbai 2019	Mumbai, IN	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS London November 2019	London, GB	Nov 11, 2019 - Nov 16, 2019	Live Event
SANS Dallas Fall 2019	OnlineTXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced