Global Information Assurance Certification Paper

Case Study: Critical Controls that Sony Should Have Implemented

GIAC (GSEC) Gold Certification

Author: Gabriel Sanchez, gmgsanchez@gmail.com
Advisor: Richard Carbone

Accepted: June 1, 2015

Abstract

On November 24, 2014, an incident almost pulled right out of a 90's hacker movie transformed into a massive computer hack. A group calling itself The Guardians of Peace (GOP) managed to breach Sony Pictures Entertainment and bring their systems down to a screeching halt. Resulting from this breach the GOP claims to have stolen over 100 terabytes of data containing Social Security numbers, salaries, movies, and other personally identifiable information. Within days, the stolen data was posted on the Internet along with demands from the GOP group that included not releasing *The Interview*. This paper will point out some of the Critical Controls that could have been utilized to minimize the impact the GOP had on the Sony breach. Utilizing even a few of the Critical Controls such as malware defenses, monitoring, audit logs, encryption, controlled use of administrative credentials, and incident response could have provided the necessary implementations required to prevent a 90's hacker movie from turning into reality.

1. Introduction

What would soon characterize one of the worst hacks in recent history began when screenwriter Evan Goldberg and actor Seth Rogen joked about making a comedy about assassinating the leader of North Korea, Kim Jong-un. On March 2013, this joke became reality when Sony Pictures Entertainment announced that both Goldberg and Rogen would direct the comedy movie, *The Interview*. The original release date of *The Interview* was targeted for the end of 2014; however, before the movie could be released an incident occurred that put hackers in complete control of Sony Pictures Entertainment's network. As a portion of the claimed 100 Terabytes of data flooded to the Internet, Sony Pictures Entertainment was forced to take its network offline as Social Security numbers, movies, salaries, and personally identifiable information were released to the Internet. After this incident, observers began to formulate different methods of preventing another hack such as the Sony breach (Zetter, 2014).

Despite concerns over the production of *The Interview* movie Sony Pictures Entertainment decided to open the film in theaters Christmas Day 2014. November 21, 2014, an email addressed to Sony Pictures CEO Michael Lynton, Chairman Amy Pascal, and other executives made vague references to “great damage” and asked for “monetary compensation” to avoid it (Franceschi-Bicchiera, 2014a). November 24, 2014, a Reddit post appeared stating that Sony Pictures Entertainment had been breached and that their complete internal, nation-wide network had signs that the breach was carried out by a group calling themselves the GOP, The Guardians of Peace (RBS, 2014). The hackers claim to have stolen a huge trove of sensitive data from Sony, possibly as large as 100 terabytes of data, which they are slowly releasing in batches.

Judging from the data that the hackers have leaked online, they have obtained usernames, passwords, and sensitive information about Sony's network architecture and a host of documents exposing personal information about employees (Zetter, 2014). December 2, 2014, the FBI sent a confidential “flash” alert to numerous U.S. businesses warning them that hackers have recently launched a destructive “wiper” malware attack. While the alert

does not name the victim, numerous information security experts say that the malware appears to correspond with the malicious code used in the recent hack attack against Sony Pictures Entertainment (Schwartz, 2014).

December 7, 2014, North Korea denied responsibility for hacking the computers of Sony Pictures Entertainment, yet they appeared to relish the attack that crippled the computer systems of the Hollywood company, which was set to release *The Interview* that involved a plot to assassinate its leader, Kim Jong-un (Sang-Hun, 2014). However, the United States public and government have claimed that the North Koreans are responsible for the attack. Although not all the details about the Sony breach have been revealed the following information has come to light due to public sources that seem to serve as a warning of a North Korean attack on Sony Pictures Entertainment. June 26, 2014, a North Korean foreign ministry spokesperson said in state media that the movie's release would be an "act of war" (BBC News, 2014).

The following day, after the United States declared that North Korea was responsible for the breach of December 8, 2014, the CEO of Sony Pictures Entertainment sent a memo to all employees confirming that their information had indeed been compromised. The memo featured a letter by Kevin Mandia, head of the cyber security firm Mandiant, which was hired by Sony to probe the massive and embarrassing film studio hacking (Franceschi-Bicchiera, 2014b). December 10, 2014, after days of review concerning the incredible amount of leaked data, analysis shifted to the contents of Co-Chairman Amy Pascal's emails, Sony Pictures Entertainment, and Steve Mosko, President of Sony Pictures Television (RBS, 2014). Emails from both Amy Pascal and Steve Mosko revealed embarrassing remarks commenting on President Obama's film preferences that had been exchanged via email at Sony Pictures Entertainment.

December 19, 2014, after the FBI formally blamed North Korea for the cyber-attack against Sony Pictures Entertainment, the hack began to spur mounting calls for the U.S. government to purse a tough response against Kim Jong-un's regime (Fox News, 2014). North Korea responded to U.S. accusations over its involvement in a cyber-attack against Sony Pictures Entertainment as "groundless slander" and that it wanted a joint

investigation into the incident with the United States. An unnamed spokesperson of North Korea's foreign ministry said there would be serious consequences if Washington refused to agree to the probe and continue to accuse Pyongyang (Kim, & Holland, 2014).

After the cyber-attack Sony nearly pulled the plug on releasing *The Interview*, however, President Obama's declaration that Sony should move forward with its movie release made Sony reconsider its position; it then proceeded with *The Interview*'s release. January 2, 2015, under a new executive order signed by President Obama, the Treasury Department imposed financial measures against ten North Korean officials and three government agencies (Morello, & Miller, 2015). This incident, besides the release of private information and movies, caused the studio's network to be offline for weeks due to the fact that Sony's technicians were forced to rebuild the network in order to bring it fully online again (Abdollah, 2015).

In a wide-ranging interview, Lynton, Sony CEO, responded to the isolation and uncertainty created by the attack and the unique position the company found itself in which he stated that "there's no playbook for an incident such as this" which created greater hardship for Sony in their recovery after the breach (Abdollah, 2015). While Sony has reported in an earnings report that the hack would cost Sony $15 million "in investigation and remediation costs" for the quarter to December 31, senior general manager Kazuhiko Takeda stated that Sony would lose $35 million for the full fiscal year through March 31 (Hornyak, 2015). This hack has also led to Amy Pascal, one of Hollywood's most powerful movie executives, stepping down as head of Sony Pictures in the wake of a hacking scandal that resulted in her private and damaging emails being leaked (Rushe, 2015).

This paper will point out some of the Top 20 Critical Controls that could have been utilized to minimize the impact that the GOP had during the Sony breach. Utilizing even a few of these Critical Controls, such as malware defenses, monitoring, audit logs, encryption, controlled use of administrative credentials, and incident response could have provided the necessary implementations required to prevent a 90's hacker movie from

turning into reality. The Critical Controls provided can only be successful with the necessary culture shift required from every employee throughout an organization (SANS Institute, 2015). Putting a checkmark in a box or bolting on safeguards, as an afterthought, will only provide a false sense of security against any future attacks.

2. Security

2.1 Critical Controls

The Critical Security Controls focus first on prioritizing security functions that are effective against the latest Advanced Targeted Threats. These security functions strongly emphasize"What Works" (SANS Institute, 2015a). These controls also prioritize and focus on a smaller number of actionable controls with a high-payoff, aiming for a "must do first" philosophy (SANS Institute, 2015a). Currently, there are 20 Critical Controls with various sub-controls that allow for organizations to accomplish tasks in phases. The SANS Institute lists the Top 20 Critical Controls as follows (SANS Institute, 2015b):

Table 1: Top 20 Critical Controls (SANS Institute, 2015b).

Top 20 Critical Controls
1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability

9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Organizations that adopt the Top 20 Critical Controls are left with the best and most timely option to prevent future hacks. Fortunately, dozens of early adopters of the Critical Controls have shared their experiences and lessons learned with the Consortium for Cybersecurity Action (SANS Institute, 2015b). According to the SANS Institute, the pattern that has emerged that allows for substantial progress in reducing risk using Critical Controls are as follows (SANS Institute, 2015b):

Table 2: Steps for Reducing Risk with Critical Controls (SANS Institute, 2015b).

Steps for Reducing Risk with Critical Controls
Step 1: Perform Initial Gap Assessment - determining what has been implemented and where gaps remain for each control and sub-control.

Step 2: Develop an Implementation Roadmap - selecting the specific controls (and sub-controls) to be implemented in each phase, and scheduling the phases based on business risk considerations.
Step 3: Implement the First Phase of Controls - identifying existing tools that can be repurposed or more fully utilized, new tools to acquire, processes to be enhanced, and skills to be developed through training.
Step 4: Integrate Controls into Operations - focusing on continuous monitoring and mitigation and weaving new processes into standard acquisition and systems management operations.
Step 5: Report and Manage Progress against the Implementation Roadmap developed in Step 2. Then repeat Steps 3-5 in the next phase of the Roadmap.

2.2 Culture at Sony

Similarly, three and a half years ago Sony was again in the spotlight with respect to another major breach. April 26, 2011, Sony was reported to have suffered a massive breach in its video game online network that led to the theft of names, addresses, and possibly credit card data belonging to 77 million user accounts (Baker & Finkle, 2011). Several days later on May 4, 2011, Sony revealed that the breach might have affected 24.5 million users of Sony Online Entertainment, making this the largest personal data heist in history (Lavasoft, 2011). Sony's response to this incident has been widely criticized by security experts, consumers, and politicians alike because it took Sony over a week to alert users that their personal details may have been stolen and that Sony stored these details in an unencrypted format (VentureBeat, 2011a, 2011b). According to Stuart Thomas, who previously built the PlayStation 2 network for Sony in 2001, the biggest mistake Sony made that led to the PSN hacks was its organizational complexity and a lack of proper security support at the board level (VentureBeat, 2011c).

May 4, 2011, a Purdue University professor testified to a Congressional committee investigating the massive data breach of Sony Game and Entertainment networks which

revealed that Sony had also failed to use firewalls to protect its networks and was caught using obsolete web applications, which made the company's sites an inviting target to hackers (Rashid, 2011). While Sony declined to appear before the May 4, 2011, hearing convened by the House Committee on Energy and Commerce, the company sent an eight-page letter detailing what it was doing to the Subcommittee on Commerce, Manufacturing, and Trade (Rashid, 2011). This document outlined increased security of data by utilizing encryption along with new tools to defend against future attacks. Other improvements included internal detection mechanisms that would flag unauthorized access or anomalies on the network. Mr. Stinger, Chief Executive of Sony at the time, said that the attacks on Sony had prompted the company to strengthen security across all of its products (Bilton, 2011).

The recent November 24, 2014, breach against Sony by the GOP group left employees and spectators wondering how such a large breach could occur again. Just three weeks later on December 15, 2014, after attackers launched a devastating *wiper* malware attack against Sony Pictures Entertainment and began leaking stolen data, Sony broke its silence by hiring a prominent U.S. attorney to threaten to sue media outlets that reproduce the leaked information and to demand that they delete all leaked-emails, contracts and other information (Schwartz, 2014b). Sony executives failed to take proactive responsibility for the security breach, which resulted in current and former employees' personal information being leaked (Schwartz, 2014c). Sony Pictures executive Amy Pascal told Bloomberg News "I don't think that anybody thinks that this was anyone's fault who works here, and I think continuity and support and going forward is what's important now." Since Sony suffered its hack attack, the company has issued very little information with respect to the breach, except to say that it was "a very sophisticated cyberattack" (Schwartz, 2014c).

3. Applied Security to Sony

3.1 Critical Controls Applied

Implementing even a few of the Critical Controls including certain sub-controls could have greatly assisted Sony with mitigating, or at least detecting the breach sooner. Unfortunately, missed opportunities by Sony resulted in a tragic incident that exposed sensitive documents to the world. Aside from the theft of electronic data, the GOP group made a statement not only to Sony but also to the world that failing to guard one's data could put an organization in the same situation. Although there is no one-size fits all approach to security there does exist foundational concepts that every organization should utilize to help prevent a cyber-attack. The following are the Critical Controls and sub-controls that could have greatly assisted Sony in the breach of November 24, 2014.

3.1.1 Issue 1a

The GOP group was allegedly able to obtain some 100 terabytes of data stolen from Sony servers including sensitive information including Social Security numbers, usernames, passwords, and emails. To put that into perspective, 10 terabytes can hold the entire printed collection of the Library of Congress (Robb, 2014).

3.1.1.1 Remediation 1a: Critical Control #17 - Data Protection

The objective of Critical Control 17 is to protect data regardless if it is internal to the network or is transferred out. In Sony's case, protecting sensitive data from being uploaded to the Internet for the entire world to see was not the ideal situation. It is preferable to detect the exfiltration of data early in the attack; however, if one's data is stolen having it encrypted complicates the attackers' ability to decipher its contents.

Table 3: Sub-Control 17-3 (SANS Institute, 2015a).

Sub-Control 17-3	
Description	**Applied to Sony**
Perform an assessment of data to identity sensitive information that requires the	Identification of sensitive information including Social Security numbers,

application of encryption and integrity controls.	usernames, passwords, and emails give the added mechanism of defense in the event of a breach. Had encryption with Sub-Control 17-3 been implemented on this sensitive information it would have increased the difficulty of uploading these sensitive documents in clear text to the Internet.

Table 4: Sub-Control 17-5 (SANS Institute, 2015a).

Sub-Control 17-5	
Description	**Applied to Sony**
Deploy an automated tool on network perimeters to monitor for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.	A tremendous amount of traffic would have been generated with an alleged 100 terabytes of data being stolen by the GOP. Sony only would have needed to detect a fraction of that in order to be tipped off that their network was under attack. Diligently automating a tool to hunt for unauthorized sensitive information leaving the network could have greatly assisted Sony and prevented the majority of its sensitive information from being stolen.

Table 5: Sub-Control 17-6 (SANS Institute, 2015a).

Sub-Control 17-6	
Description	**Applied to Sony**
Conduct periodic scans of servers using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.	With Sub-Control 17-6 Sony could have actively searched for sensitive information stored in clear text. Although no organization wants their data to be stolen, had the data at least been encrypted it could have greatly hindered the attackers' ability to read the contents.

Table 6: Sub-Control 17-12 (SANS Institute, 2015a).

Sub-Control 17-12	
Description	**Applied to Sony**
Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.	Sony could have established Sub-Control 17-12 to further investigate large amounts of data leaving their network. If Sony was able to differentiate between legitimate encryption channels vs. a possible back channel, it could have forewarned Sony that they were under attack.

3.1.2 Issue 2a

Wiper malware – so called because it erases data from victims' computer drives – played a key part in the costly cybersecurity breach directed against Sony Pictures Entertainment in late 2014 (Robinson, 2015). Given the destructive nature of this malware, early detection of the dropper and its installed files would have been essential to prevent significant data losses (Gallagher, 2014).

3.1.2.1 Remediation 2a: Critical Control #5 - Malware Detection

Malware was a huge contributor of the Sony Pictures Entertainment breach in 2014 where the GOP deleted the contents of hundreds of computers in order to make them unusable by users. Applying malware defenses and detection would have assisted Sony Pictures Entertainment in possibly preventing the *wiper* malware from having spread.

Table 7: Sub-Control 5-7 (SANS Institute, 2015a).

Sub-Control 5-7	
Description	**Applied to Sony**
Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices.	If malware or copying of data occurred via external devices, Sub-Control 5-7 would have notified the security team that something unusual was occurring on Sony systems.

Table 8: Sub-Control 5-9 (SANS Institute, 2015a).

Sub-Control 5-9	
Description	**Applied to Sony**
Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out	Signature-based tools will only catch malware that it already knows about. However, utilizing techniques such as those listed in Sub-Control 5-9 to identify

malicious content before it arrives at the endpoint.	executables in network traffic could have assisted Sony with anomalies in the infrastructure.

3.1.3 Issue 3a

The GOP installed *wiper* malware on computer systems that deleted all the contents on the hard drive.

3.1.3.1 Remediation 3a: Critical Control #8 - Data Recovery Capability

Restore computer systems as quickly as possible from trustworthy backups. Being able to restore data is one major piece to restoring the organizations infrastructure.

Table 9: Sub-Control 8-1 (SANS Institute, 2015a).

Sub-Control 8-1	
Description	**Applied to Sony**
Ensure that each system is automatically backed up at least once a week, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection.	For each day Sony was down it undoubtedly cost the organization more money and time for restoration. Having the capability to quickly restore from malware-free backups for critical systems could have reduced the time Sony Pictures Entertainment systems were kept offline.

All backup policies should be compliant with any regulatory or official requirements.	

Table 10: Sub-Control 8-3 (SANS Institute, 2015a).

Sub-Control 8-3	
Description	**Applied to Sony**
Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	With the use of Sub-Control 8-3 Sony would have been able to properly use protected backups to limit the potential scope of the Sony breach that the GOP gained in its attack. It also could have ensured trust worthy backups.

3.1.4 Issue 4a

The GOP group was able to completely compromise the Sony Pictures Entertainment network.

3.1.4.1 Remediation 4a: Critical Control #12 - Controlled Use of Administrative Privileges

The misuse of administrative privileges is the primary manner in which attackers spread inside a target enterprise (SANS Institute, 2015a). Even one account being compromised by the attacker can lead to a company-wide breach.

Table 11: Sub-Control 12-12 (SANS Institute, 2015a).

Sub-Control 12-12	
Description	**Applied to Sony**
Use multifactor authentication for all administrative access, including domain	Not only did the GOP infiltrate the Sony network, they also embedded legitimate

administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	username and credentials into the malware for a higher success rate of spreading throughout the infrastructure. Providing additional authentication for administrative accounts could have prevented the GOP from compromising sensitive accounts.

3.1.5 Issue 5a

The GOP group dropped the *wiper* malware, which took a foothold within the infrastructure of Sony Pictures Entertainment.

3.1.5.1 Remediation 5a: Critical Control #14 - Maintenance, Monitoring, and Analysis of Audit Logs

Deficiencies in security logging and analysis allowed attackers to hide their location, malicious software, and activities on victim machines (SANS Institute, 2015a).

Table 12: Sub-Control 14-9 (SANS Institute, 2015a).

Sub-Control 14-9	
Description	**Applied to Sony**
Deploy a SIEM (Security Incident and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using a SIEM tool, system administrators and security personnel should devise profiles of common events so that they can tune detection to focus on unusual activity, avoiding false positives, more rapidly identifying anomalies, and prevent overwhelming analysts with	Using Sub-Control 14-9, Sony could have detected that their infrastructure was breached by correlating activities that deviated from their known baseline. Knowing what is normal in one's infrastructure is imperative to detect malicious activity.

insignificant alerts.	

3.1.6 Issue 6a

The GOP group was able to bring down the entire Sony Pictures Entertainment technology infrastructure.

3.1.6.1 Remediation 6a: Critical Control #19 - Secure Network Engineering

Establish network segmentation in order to create the necessary layers for protecting critical systems.

Table 13: Sub-Control 19-4 (SANS Institute, 2015a).

Sub-Control 19-4	
Description	**Applied to Sony**
Segment the enterprise network into multiple, separate trust zones to provide a more granular control of system access and additional intranet boundary defenses.	If Sony had utilized Sub-Control 19-4, and thus had granular segmentation of systems with additional security implemented, it could have lessened, or alerted, Sony to a breach.

3.1.7 Issue 7a

Attackers were able to figure out a way to breach the security of Sony Pictures Entertainment.

3.1.7.1 Remediation 7a: Critical Control #20 - Penetration Tests and Red Team Exercises

Organizations need to be familiar with the different attack vectors and the potential ways attackers can breach their computer infrastructure.

Table 14: Sub-Control 20-1 (SANS Institute, 2015a).

Sub-Control 20-1	
Description	**Applied to Sony**
Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (e.g., the Internet or wireless frequencies around an organization) as well as from within its boundaries (e.g., on the internal network) to simulate both outsider and insider attacks.	Having penetration tests on one's infrastructure can point out many of the ways attackers can breach an organization. More importantly, had Sony established action items to mitigate the highest risks they could have potentially prevented the attack vector utilized by the GOP group.

3.1.8 Issue 8a

Sony admitted to having suffered a major cybersecurity breach; hackers not only erased data from its systems, but also stole and made some of it public, including movie pre-releases, individual's private information, and sensitive documents (Steinberg, 2014).

3.1.8.1 Remediation 8a: Critical Control #18 - Incident Response and Management

Sony did not properly nor effectively deploy incident response during the breach. In the future, Sony needs to be able to quickly involve necessary teams and be familiar with incident response procedures in order to prevent future incidents.

Table 15: Sub-Control 18-7 (SANS Institute, 2015a).

Sub-Control 18-7	
Description	**Applied to Sony**
Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.	Effectively practicing incident response handling could have assisted Sony with being able to recover and bring the organization online quicker. Sony Pictures Entertainment technicians and experts are only now beginning to roll out new computer systems with heightened security safeguards, six weeks after a hack attack crippled operations (Cunningham, 2015).

4. Culture Shift at Sony

The ins and outs of the many cyber-attacks against Sony in recent years – both why and how they have occurred – provide a fascinating look into what happens when hacker and corporate cultures and values collide (Estes, 2014). Unfortunately, this was not the first time Sony has suffered a large security breach within their infrastructure. Just three years earlier, in 2011, Sony provided a document to the Subcommittee on Commerce about increasing security of their data with encryption and mechanisms to detect anomalies on the network. However, none of the security improvements made by Sony Pictures Entertainment over the years proved to be of little use as the GOP group brought down the entire network.

Attempting to apply security controls without ensuring that the organization has the right security culture is similar to utilizing a chain to close one's doors without a padlock. It provides a false sense of security and arguably puts an organization at more risk due to incorrect assumptions. Upper management, including board members, must set the tempo of the organization's culture shift and work with the right people to ensure it is in line

with the best security practices. With the right people taking responsibility and accountability for an organization's security postures, issues can be given the proper attention. Even with support from upper management, the culture shift cannot be forced onto individuals or else organizations will receive minimal complacency. Instead, companies must educate their employees as to why and how the culture must change for the overall good of the individual and the organization.

Organizations, at times, will think of security as an afterthought and instead will focus all their energy on their primary functions of revenue, safety, availability, and other components of the business. The culture shift needed today is one where security is an attribute of the organization's primary functions; thus, it should receive the same amount of attention. A lack of a culture shift when implementing security can lead to scenarios similar to Sony Pictures Entertainment where the entire organization was brought to a standstill. Both security controls and a culture shift will not necessarily guarantee a breach free environment, but it will prepare an organization for the necessary tools and capabilities to prevent, detect, and respond to potential breaches.

5. Conclusion

At any moment, an organization can be attacked by hackers who will attempt, and even succeed, at compromising the computer infrastructure. Sony Pictures Entertainment was one such victim during the massive breach in 2014, but many organizations can easily be in the same scenario. The breach against Sony Pictures Entertainment in 2014 by the GOP brought the entire organization down and led to the leaking of sensitive data on the Internet. Not only was sensitive data leaked but the GOP inserted *wiper* malware into the infrastructure that essentially made bricks out of Sony's computer systems. Sony Pictures Entertainment was forced to scramble to bring the infrastructure back up while dealing with the massive amount of sensitive documents affecting employees and the organization. In addition, Sony's response about suing media outlets for publishing information did not help with their stance of wanting to improve security.

Gabriel Sanchez, gmgsanchez@gmail.com

In many instances a breach is a result of a breakdown or lack of security controls in various areas. With Sony Pictures Entertainment insufficient malware defenses, monitoring, audit logs, encryption, controlled use of administrative credentials, and incident response contributed to the massive breach on the organization. The SANS Top 20 Critical Controls assist with actionable items that allow organizations to mitigate risks quickly and effectively. Not only can organizations implement security changes, but they are also able to audit those changes in order to measure effectiveness.

For every attack, organizations must learn its deficiencies and establish actionable items to constantly improve. This improvement must be supported by the highest level of the organization with a commitment to maintain security as an attribute of the day-to-day functions. However, just wanting to improve security is not enough. It must be supported by proven methodologies such as the SANS Top 20 Critical Controls which provide the framework to technically improve an organization's security posture. Technical controls and the proper culture shift established by upper management give organizations the priorities of aligning security with the business. A lack of one or the other gives a false sense of security and leaves organizations asking why when a major breach occurs. All organizations should look at these common pitfalls so that their organization does not become a national headline with a breach taken out of a 90's hacker movie.

Gabriel Sanchez, gmgsanchez@gmail.com

6. References

Abdollah, T. (2015, January 9). Sony Pictures CEO had 'no playbook' for mega-hack on studio - Yahoo Finance. Retrieved from https://finance.yahoo.com/news/sony-pictures-ceo-had-no-063849901.html

Baker, L., & Finkle, J. (2011, April 26). Sony PlayStation suffers massive data breach| Reuters. Retrieved from http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

BBC News. (2014, June). North Korea threatens war on US over Kim Jong-un movie - Retrieved from http://www.bbc.com/news/world-asia-28014069

Bilton, N. (2011, May 17). Sony Chief Defends Response to PlayStation Data Breach - NYTimes.com. Retrieved from http://bits.blogs.nytimes.com/2011/05/17/sony-chief-defends-response-to-playstation-data-breach/?_r=1

Cunningham, T. (2015, January 9). 45 Days After Hack Attack: What's the State of Sony Pictures. Retrieved from http://www.thewrap.com/45-days-after-hack-attack-the-state-of-sony-pictures/

Estes, A. (2014, December 9). Why Sony Keeps Getting Hacked. Retrieved from http://gizmodo.com/why-sony-keeps-getting-hacked-1667259233

Fox News (2014, December 19). FBI blames North Korea for Sony hack, US weighs response. Retrieved from http://www.foxnews.com/politics/2014/12/19/us-weighs-response-to-attack-on-sony-fbi-prepares-to-implicate-north-korea/

Franceschi-Bicchiera, L., & WARREN, C. (2014a, December 8). Hackers sent extortion email to Sony executives 3 days before attack. Retrieved from http://mashable.com/2014/12/08/hackers-emailed-sony-execs/

Franceschi-Bicchiera, L. (2014b, December 8). Don't believe the hype: Sony hack not 'unprecedented,' experts say. Retrieved from http://mashable.com/2014/12/08/sony-hack-unprecedented-undetectable/

Gallagher, S. (2014, December 3). Inside the "wiper" malware that brought Sony Pictures to its knees [Update] | ArsTechnica. Retrieved from http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/

Hornyak, T. (2015, February 5). Hack to cost Sony $35 million in IT repairs | CSO Online. Retrieved from http://www.csoonline.com/article/2879444/data-breach/hack-to-cost-sony-35-million-in-it-repairs.html

Kim, J., & Holland, S. (2014, December 20). North Korea denies hacking Sony, U.S. stands by its assertion| Reuters. Retrieved from http://www.reuters.com/article/2014/12/20/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141220

LavaSoft. (2011, May 4). Sony's Security Breach May Be the Biggest Personal Data Heist in History | Lavasoft. Retrieved from http://www.lavasoft.com/mylavasoft/company/blog/sony%E2%80%99s-security-breach-may-be-the-biggest-personal-data-heist-in-history

Morello, C., & Miller, G. (2015, January 2). U.S. imposes sanctions on N. Korea following attack on Sony - The Washington Post. Retrieved from http://www.washingtonpost.com/world/national-security/us-imposes-sanctions-on-n-korea-following-attack-on-sony/2015/01/02/3e5423ae-92af-11e4-a900-9960214d4cd7_story.html

Pearson, J. (2014, December 17). Sony Pictures CEO consulted U.S. State Dept on film, leaked emails show | Daily Mail Online. Retrieved from http://www.dailymail.co.uk/wires/reuters/article-2877215/Sony-Pictures-CEO-consulted-U-S-State-Dept-film-leaked-emails-show.html

Rashid, F. (2011, June 5). Sony Networks Lacked Firewall, Ran Obsolete Software: Testimony. Retrieved from http://www.eweek.com/c/a/Security/Sony-Networks-Lacked-Firewall-Ran-Obsolete-Software-Testimony-103450

RBS. (2014, December 5) A Breakdown and Analysis of the December, 2014 Sony Hack. Retrieved from https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#catchingupandclosingout

Robb, D. (2014, December 22). Sony Hack: A Timeline | Deadline. Retrieved from http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

Robinson, R. M. (2015, January 21). Attention Required! | CloudFlare. Retrieved from http://securityintelligence.com/wiper-malware-poses-destructive-threat/#.VVDrgtNVhHw

Rushe, D. (2015, February 5). Amy Pascal steps down from Sony Pictures in wake of damaging email hack | Film | The Guardian. Retrieved from http://www.theguardian.com/film/2015/feb/05/amy-pascal-leaving-sony-pictures-email-leak

Sang-Hun, C. (2014, December 7). North Korea Denies Role in Sony Pictures Hacking - NYTimes.com. Retrieved from http://www.nytimes.com/2014/12/08/business/north-korea-denies-hacking-sony-but-calls-attack-a-righteous-deed.html?_r=0

SANS Institute. (2015a)- Critical Security Controls. Retrieved from https://www.sans.org/critical-security-controls/

SANS Institute. (2015b)- Critical Security Controls: Guidelines. Retrieved from http://www.sans.org/critical-security-controls/guidelines

Schwartz, M. J. (2014a, December 2). Sony Hack: FBI Issues Malware Alert - BankInfoSecurity. Retrieved from http://www.bankinfosecurity.com/sony-hack-fbi-issues-malware-alert-a-7628/op-1

Schwartz, M. (2014b, December 15). Sony Breach Response: Legal Threats - BankInfoSecurity. Retrieved from http://www.bankinfosecurity.com/sony-breach-response-legal-threats-a-7676/op-1

Schwartz, M. (2014c, December 23). Sony's 7 Breach Response Mistakes - BankInfoSecurity. Retrieved from http://www.bankinfosecurity.com/blogs/sonys-7-breach-response-mistakes-p-1785/op-1

Steinberg, J. (2014, December 11). Massive Security Breach At Sony -- Here's What You Need To Know - Forbes. Retrieved from http://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/

VentureBeat. (2011, September 22). Security lessons from the PlayStation Network breach | VentureBeat | News | by VentureBeat. Retrieved from http://venturebeat.com/2011/09/22/security-lessons-from-the-playstation-network-breach/

Zetter, K. (2014, December 3). Sony Got Hacked Hard: What We Know and Don't Know So Far. Retrieved from http://www.wired.com/2014/12/sony-hack-what-we-know/

Last Updated: May 29th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event