# Fool Me Once: A Look at the 2011 and 2014 Sony Hacks

Matthew Sullivan
CSCI 5742

**Abstract.** In April of 2011, Sony experienced multiple Denial of Service attacks, culminating in a breach that saw the leak of personal information of over 100 million Sony Playstation and Sony Online Entertainment users, as well as a small number of credit cards. This breach caused the Playstation network to be down for 23 days and cost Sony an estimated 170 million dollars. Sony, reacting to accusations of delayed notification of its userbase, reassured its members and investors that they were enhancing security. However, just 3 years later, in December of 2014, Sony experienced another massive breach that saw the loss of employee information, intellectual property, and sensitive technical information, as well as the destruction of a sizable portion of their computer systems with a wiperware attack. Were the attacks so different that there was no defense against them? Or did Sony not effectively employ the standards that they claimed to have adopted in 2011?

## 1 Summary of Case Study

On April 19th, 2011, Sony detected unauthorized activities on their networks, leading to them to monitor the activity and to shut down both the Sony Playstation Network and their Qriocity networks on April 20th when they determined that data had been transferred off of the servers[1]. They also hired a security and forensic analysis firm to analyze the breach on the 20th, and a second team on the 21st. They contacted the FBI on April 22nd., but declined to inform the public until April 26th when they had more information on the data that was taken. The data included the personal information on 77 million Playstation network members and 24 million Sony Online Entertainment members. Their passwords, while hashed, were not encrypted, and the information for 12,700 credit cards and 10,700 direct debit records were taken from an “outdated” server.[2] Sony was unable to identify the actors behind this attack (Anonymous denied it was them, though they didn't discount the possibility of members acting independently), and, while they were able to identify the access method, they did not disclose it in the interest of preventing future breaches.

The United States House of Representatives subcommittee on Commerce, Manufacturing, and Trade launched an inquiry on the data breach, the storage of sensitive information without encryption, and the slow notification of the customers. On May 3rd, Sony responded in the form of a letter, pledging new security measures in response to the breach, including new automated software monitoring, more levels of encryption, enhanced network monitoring, additional firewalls, implementing a new move to a data center with enhanced protocols, and the naming of a new CISO (Chief Information Security Officer).[1]

After these security measures were implemented, Sony brought the networks back up on May 15th. Almost a month of down time prompted Sony to offer a “Welcome Back” package as a way of apologizing to their users. The cost of the new security measures, identity protection for customers, and lost revenue ended up costing Sony an estimated 171 million dollars, not inclusive of the settlement in a 15 million dollar class action lawsuit in 2014[3].

The second incident this case study examines took place in November of 2014. Sony Pictures Entertainment was getting ready for a Christmas release of a film offensive to the current North Korean regime called “The Interview”. On November 24th, it was leaked to the internet that there was a breach on many computers at Sony. A group of hackers calling themselves the Guardians of Peace (or GOP) had infiltrated Sony Picture Entertainment's network, stolen a great deal of data, and installed wiperware on their machines. This severely crippled Sony Picture's operations. Two days later, the GOP released high quality copies of several upcoming Sony pictures to torrent sites.  For the next 3 weeks, the GOP released a series of leaked files, totaling in the hundreds of gigabytes.[4] The first leak included personal information for employees (47,426 social security numbers in the first leak alone), while the second included plaintext credentials for social media accounts, major news and media sites, as well as FTP servers. It also included server information, internal IP addresses, and info on the company's PCs, Linux and Windows servers. The 3rd leak included financial reports, contracts, and tax documentation revealing even more employee personal information. The 4th leak included the email records for Steve Mosko (President of Sony Pictures Television) and Amy Pascal (Co-Chairman, Sony Pictures Entertainment and Chairman, Sony Pictures Entertainment Motion Picture Group), which detailed everything from personal emails to upcoming movie deals. The group went on to release the personal information of thousands of employees, Sony internal documents, as well as several more highly placed members of Sony Pictures Entertainment, for a total of 9 leaks.

While no details about the definite origin of the attack, it appears that the malware that wiped Sony Picture's computers was tailored to target Sony, indicating that either the hackers had  prolonged access to the network, or they had help from the inside[5]. While there are several different theories about the identity of the GOP, the FBI concluded on December 19th that North Korea was behind the attack. This goes against the analysis of several security firms, who believe that it is more likely an attack by former Sony employees, Russia, or China. After consulting with the security companies, the FBI declined to change their conclusion, and President Obama imposed sanctions on several parties belonging to the North Korea government on January 2nd.

Timeline for 2011 Incident:
April 19th: Anomalous activity detected
April 20th: Data transfer discovered, networks shut down.
April 21st: Sony retains security firm services
April 22nd: Sony informs FBI of breach
April 26th: Sony informs the public of the breach
April 29th: US Congress writes letter to Sony questioning their response and lack of notification.
May 3rd: \Sony responds to Congressional letter.
May 15th: Sony brings its network back up, starts “Welcome Back” Program

Timeline for 2014 Incident:
November 24th: Sony Pictures computers are found to be compromised by wiperware.
November 25th: High quality unreleased movies released to torrent sites.
December 1st: 1st leak, 24.87GB (Employee information)
December 3rd: 2nd leak, 35MB. (Network/Technical information)
December 7th: 3rd leak, 100GB. (Financial and contract data)
December 8th: 4th leak, 7GB (Steve Mosko and Amy Pascal's emails)
December 10th: 5th leak, 5GB(employee information and business data)
December 10th: 6th leak, 3.8GB(Leah Weil's emails)
December 13th: 7th leak, 6.4 GB (internal documents)
December 14th: 8th leak, 5.5GB (O'Dell Steven's emails)
December 16th: 9th leak, 1GB (Michael Lynton's emails)
December 17th: Sony cancels theatrical release of The Interview, due to threatening messages from parties claiming to be GOP
December 19th: FBI concludes that North Korea is behind the attack.
January 2nd: President Obama invokes sanctions on North Korean parties in response to the attack.

## 2 NIST 800-53A Controls

In this section, we will examine some NIST Controls that apply to these two incidents.

### 2.1 Control Family #1 Access Control

While it is unknown exactly how the network was breached in 2011 and in the 2014 attacks, it is a given that unauthorized users were able to gain access and were also able to manipulate information flow inside the network. With more secure policies for AC-3 (Access Security) and AC-4 (Information Flow Enforcement), it's possible that some of the information would not have been leaked.

### 2.2 Control Family #2 Awareness and Training

As stated above, it is unknown how the network in 2014 was compromised, however, the fact that the malware seemed tailor made for Sony suggested either previous access to the network by a watering hole or spear phishing attack, or an inside job[5]. The best way to prevent watering hole or spear phishing is by educating employees as outlined in control AT-2 (Security Awareness Training). If this was implemented, it may have become more difficult for the GOP to get the information required to so completely disrupt the Sony Pictures Entertainment network.

### 2.3 Control Family #3 Security Assesment and Authorization

In the 2011 incident, good implementation of continuous monitoring policy (CA-7) allowed Sony to detect unusual activity on their network, though they did not shut it down until it was confirmed data was taken and therefore it was too late. However, the fact that they realized that they were unsecure allowed them to mitigate the damage, possibly preventing further loss of data. In contrast, in the 2014 incident, Sony Pictures was completely unaware of the breach until the wiperware spread throughout its computers and announced that it had been hacked. While Sony is a big corporation, clearly the Pictures division did not follow the lead of the Playstation Network division when it came to setting up security protocols, and it cost them greatly.

### 2.4 Control Family #4 Incident Response

While Sony was criticized for the delay in reporting the breach of data to consumers in 2011, it pales in comparison to the haphazard method of damage control the Pictures division attempted in 2014. I was unable to cover Sony's full response in the 2014 case, but reading it seems borderline insane. They attempted everything from threatening news outlets with legal action to keep quiet on the emails, to denial of service attacks on the hosting websites themselves. In the end they ended up canceling the release of the Interview. Their response (at least outwardly) in 2011 was slow and angered their userbase, but in 2014 it was almost embarrassing. It must be assumed that a new policy was drawn up (IR-1), as their incident response was a disaster.

### 2.5 Control Family #5 System and Services Acquisition

The malware that spread throughout Sony Pictures' entire network in 2014 was able to do so due to a lack in control SA-8(Security Engineering Principles), which dictates that the network be segmented and layered so that it is more secure. Clearly the Sony Pictures network was not, and was still down 6 weeks after the incident occurred[7].

### 2.6 Control Family #6  System and Communication Protection

Obviously, Sony did not have adequate protections under SC-5 (Denial of Service Protection) in 2011. While they took the servers down themselves, they had been plagued all year by hackers doing widespread DoS attacks.

Also, while it is unknown how the network was breached, clearly even Sony admitted that their SC-7 (Barrier protection) was inadequate, as it was expressly called out in the letter to Congress[1].

While the breach of 2011 had more user personal data leaked, the breach in 2014 was much larger, with more long reaching consequences for the company. Sensitive trade information, contracts, and personal emails only scratch the surface of what was taken. A great deal of this information was released because the company was using email as a long term storage solution, rather than a secure database. This should have been covered under SC-28 (Protection of Information at Rest). Also relevant to this control is also where the policy should have been implemented to store passwords (from the 2011 attack) in an encrypted form rather than a weak cryptographic hash, as well as any number of sensitive documents, credentials, or passwords from the 2014 attacks, many of which were stored in plaintext[7].

### 2.7 Control Family #7 System and Information Integrity

Clearly, the two incidents that happened at Sony show a resounding failure of control SI-3 (Malicious Code Protection), SI-4(Information System Monitoring) and SI-7(Software, Firmware, Information Integrity). It is difficult to ascertain how much of this is Sony's fault, as they actually did (belatedly) detect the abnormal traffic in 2011 (SI-4), and the malware used to wipe their computers seems to be of a new kind (based on the FBI Flash[5]) and would therefore probably be undetectable by normal antivirus/anti-malware. However, it should still have been possible to detect unauthorized network activity in that case, as was done in 2011. Some experts concluded that much of the reason Sony was vulnerable was due to bad IT practices, including not installing security updates (SI-3)[6]. They should also have prevented the malware from making modifications to the computers throughout the network (SI-7).

## 3 Prevention and Detection Tools

Here I will attempt to cover some prevention and detection tools and practices. While many of these are covered above, I'll try to hit the highlights. Also, I can give a rough estimate when I can, but I don't have any idea of the ballpark of costs for some of these.

### 3.1 Practice #1 Information Security

This practice boils down mostly to policy. Personal information should be encrypted, not in plaintext. Long term storage of documents, especially sensitive ones, should be in a secure server potentially off site, not in an email inbox. Outdated information should be secured in an off-site secured server or destroyed. Sony dropped the ball by having the personal information accessed in 2011, and the breach in 2014 was even more damning because of it. To implement these practices, it's mostly a matter of education, not allowing laziness because it's easy or convenient, and some new secure servers. The monetary cost should be minimal, and the real cost will be in the effort and manpower to properly train and enforce such procedures, and to update the old information into more secure formats.

### 3.2 Tool/Practice #2 Advanced Network Monitoring Software

This practice would implement state of the art network monitoring techniques to ensure that anomalous traffic is detected and stopped. While the Playstation division detected the hack in 2011, the Pictures division was caught completely by surprise in 2014. It may be necessary to enhance the cybersecurity division, and the licensing fees on the software itself (there are many out there) are expensive, but if the employees were able to detect the abnormal traffic and stop it, they would have clearly not cost as much as the hundreds of millions of dollars in lost productivity, intellectual property loss, trade secrets, settlements, and fines that these two incidents have cost Sony.

### 3.3 Practice #3 Become a Harder Target

While unfortunately I had to stick to the more technical side due to space constraints, it was no secret in the many articles I found that Sony did little to make itself a hardened target. [6][8][9][10] This would generally apply to most of the controls above that I have not covered yet, but also applies to the business and legal practices of Sony. On the business side, not angering Hactivist groups such as Anonymous, or active state level cyberthreats such as North Korea might be a good start. On the technical side, everything that makes you a harder target than your neighbor decreases your risk. Enhanced firewalls and network architecture, increased cybersecurity staff, penetration testing, secure information, all would enhance security. Unfortunately, this is the most costly of the proposed practices in money and manpower, and as such is least likely to be implemented properly.

### 3.4 Practice #3 Clear Incident Response Policy

Since the response from the company in both of these cases was inadequate (the first needing a letter from Congress, the second a giant mess of legal threats, hacking, and blame). A clear and appropriate response plan should be written up and employed. While the policies and tools above will hopefully not cause it to be necessary, it is important for the company, the customers, and the stockholders that an appropriate response is made.

## 4. Lessons Learned

While it is true that there is no such thing as a perfectly secure system, especially when someone is specifically targeting you, it's clear that at the very least, the different departments of Sony didn't communicate the lessons learned in the 2011 attack. If anything, the attack in 2011 was better handled, despite the “verify then communicate” attitude of Sony in that situation. The continued practice of unsecured sensitive information of all kinds, as well as the non-implementation of better security practices outlined in the letter to Congress, show that Sony, while not intentionally malicious, were definitely negligent. The cost to repair the infrastructure alone in the 2014 attack was estimated at $35 million, and Sony settled with employees for an additional $15 million, to say nothing of the loss of the intellectual property and the sensitive business documents. All of this because of bad security practices on a lesson that should have been learned back in 2011. To ensure that this never happens again, Sony needs to start taking information security seriously, hopefully enhance its infrastructure while rebuilding, and communicate the lessons learned through the entire corporation. Has Sony learned from the past this time? Only time will tell.

## References

1. Hirai, Kazuo. 2011. *Letter to Honorable Mary Bono Mack & Honorable G.K. Butterfield* (5/3/2011) Retrieved 11/15/18 https://www.flickr.com/photos/playstationblog/5686965323/in/album-72157626521862165/

2. Pearson, Dan. 2015. *24.6 Million SOE accounts potentially compromised* (5/3/2015) Retrieved 11/15/18 https://www.gamesindustry.biz/articles/2011-05-03-24-6-million-soe-accounts-potentially-compromised

3. Buckley, Sean. 2014. *Sony's $15 million PSN hacking settlement pays out in free games* (7/23/14) Retrieved 11/15/18 https://www.engadget.com/2014/07/23/playstation-lawsuit-settlement/

4. Risk Based Security Staff. 2014. *A Breakdown and Analysis of the December, 2014 Sony Hack* (12/5/2014)Retrieved 11/15/18 https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

5. Gallagher, Steve. 2014. *Inside the "wiper" malware that brought Sony Pictures to its knees[Update]* (12/3/14)Retrieved 11/15/18 https://arstechnica.com/information-technology/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/

6. Elkind, Peter. 2015. *Inside the Hack of the Century*, Fortune Magazine (July 2015) Retrieved 11/15/18 http://fortune.com/sony-hack-part-1/, http://fortune.com/sony-hack-part-2/, http://fortune.com/sony-hack-part-3/

7. Sanchez, Gabriel. 2015. *Case Study: Critical Controls that Sony Should Have Implemented*, SANS Case Studies (2015) Retrieved 11/15/18 https://www.sans.org/reading-room/whitepapers/casestudies/paper/36022

8. Alvarez, Edgar. 2014. *Sony Pictures hack: the whole story* (12/10/14) Retrieved 11/15/18 https://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/

9. Olaniran, Bolanle, Potter, Andrew, Ross, Katy, Johnson, Brad. 2014. *A Gamer's Nightmare: An Analysis of the Sony Playstation Hacking Crisis*, Journal of Risk Analysis and Crisis Response, Vol. 4, No. 3 (September 2014), 151-159 https://www.atlantis-press.com/journals/jracr/14335

10. Xiao-Feng (John) Hsu, Shawn Do. 2012. *Stoppage of Play: The Sony Playstation Network Crash*, 2012 Case Study Competition in Corporate Communications, The Page Society (2012) https://docs.google.com/gview?url=https://page.org/attachments/531a5a9d74ec8d8f3e12e4874720d547bb7037b0/store/3a7855b5e2628d6f1e1cf998bd4d1ab31f2b89a12adb6e029ce836a26f72/Sony-PSN-Case-A11.pdf

https://docs.google.com/gview?url=https://page.org/attachments/2577e10d938f904a71f8fe0c6e6bd5ef7641589d/store/fe2436c67064f55d9c7829282bd48d59729e60d937a8724a91f7a0f4efd7/Sony-PSN-Case-B.pdf