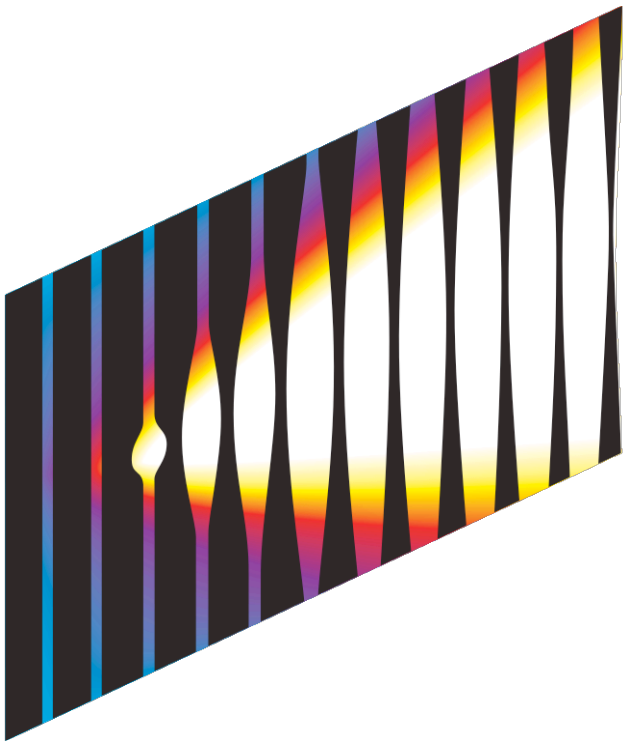


SONY
PICTURES

Hacked!
A Strategic Communication Analysis of the Cyberattack of Sony Pictures

2016 Arthur W. Page Society Case Study Competition

Table of Contents

Overview of Case 1

Company Background 2

The Problem 2

Cyberterrorism 2

Sony's Case 3

Timeline of Events 4

Sony's Crisis Communication 5

Internal Communications 5

External Communications 6

Media Relations 7

Stakeholders Affected 8

Employees 8

Partners 9

Crisis Outcomes 11

Sony's Reputation 11

Financial Impact 12

Value and Significance 12

Cyber Security 12

Lessons Learned 13

References 15

Appendices 19

Overview of Case

In 2014, Sony Pictures Entertainment (SPE) planned on releasing a comedy motion picture, *The Interview,* on Christmas Day. In the film, two journalists, played by Seth Rogen and James Franco, are sent on an assignment by the CIA to assassinate the leader of North Korea, Kim Jong Un. Prior to the film's release, a team of hackers from North Korea referring to themselves as the Guardians of Peace (GOP), sent several warnings to SPE not to release the "terrorism film." When the threat was sent out to news sources and theater chains, several major chains (AMC, Regal, Cinemark, Cineplex, and Carmike) refused to screen the movie, eventually causing SPE to cancel its release. After much scrutiny and criticism from multiple stakeholders regarding this decision, SPE reversed its decision and decided to release the film in select theaters and through video on-demand websites on its original date of December 25, 2014.

On November 24, 2014, a massive cyberattack struck SPE's systems that erased over half of its global network, erasing everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers (Elkind, 2015 a). The attack ensured that nothing could be recovered after the hacking team uploaded a special deleting algorithm that overwrote the data several different ways (Gaudiosi, 2014). Over the course of several weeks prior, attackers had also been collecting personal employee information and confidential files and placed them on shared public websites in the subsequent weeks following the initial attack. This stolen information included social security numbers of nearly 50,000 employees, movies that had not yet been released, a list of studio salaries of company executives, and personal email messages between employees and celebrities (Elkind, 2015 c).

The data dump proved SPE lacked basic security features to effectively protect personal employee data, proprietary company information, and its internal communication systems. The situation was even more embarrassing for the studio after emails were released detailing specifics about film production and strong personal opinions of employees about other individuals within the film industry. The scope and breadth of the cyberattack made the SPE hack a landmark case in the world of corporate cybersecurity, drew attention to the way a company reacts to massive information theft, and further proved that cyberterrorism is an increasingly significant global issue.

Company Background

Sony Pictures Entertainment is a subsidiary of the Japanese conglomerate Sony Corporation. Founded as Columbia Pictures in 1924, the production company was a force in movie making for decades before falling on hard times and pushed close to bankruptcy in the early 1970s. Purchased by Coca-Cola Company in 1982, Columbia had the financial backing to undergo rapid expansion, buying multiple smaller production companies and even moved into television production after purchasing Merv Griffin Enterprises. In 1987, Coca-Cola executives became weary of the volatile nature of the film industry, selling Columbia Pictures to Tri-Star Pictures, thus creating Columbia Pictures Entertainment (CPE). In 1989, controlling interest in CPE was sold to Sony Corporation. The studio officially changed its name to Sony Pictures Entertainment (SPE) in 1991. Today, SPE is one of the most well-known film and television production companies in the world, doing over $8 billion dollars worth of sales in 2014. This revenue from SPE accounted for nearly 11 percent of the Sony Corporation's total revenue. Most people recognize SPE for successful film franchises like *Spider-man* or *Men In Black* (see Appendix A).

The Problem

Cyberterrorism

Late in the 20th century, the rise of the Internet age ushered in a rise in digital exploitation. Cybercrime was a term coined to include acts like computer hacking, email phishing, and other online exploits designed to target the online systems of a person or company. By 2000, experts began to use the term "cyberterror" to describe online crime designed to disrupt systems versus crime specifically designed to steal assets or enrich the perpetrators.

By 2005, nearly 60% of surveyed businesses had detected multiple instances of cyberattack, with the average system downtime ranging from 90 minutes to 24 hours. Nearly half of victimized businesses detected 10 or more cyberattacks per year (Bureau of Justice Statistics, 2010).

The numbers have continued to grow as the ease with which a person can commit cybercrime has developed. In 2007, there were 12,000 reports of cyber incidents in the United States. That number had quadrupled by 2012. In 2013, reports from the Pentagon show that it experiences nearly 10 million attempts at intrusion every day (Government Accountability Office, 2013). Nationally, the U.S. Intelligence Committee considers the threat of cyberterrorism a greater threat to our national security than physical acts of terrorism (Clapper, 2013).

Sony's Case

Unlike most stereotypes related to cyberterrorism and cybercrime, the Sony Pictures Entertainment (SPE) data breach was a new milestone in the world of cyberterrorism. Previously, most attempts to breach companies were done with the intent of monetary gain. Typically, criminals were specifically after personal information for other crimes, like fraud. However, high-profile instances like WikiLeaks and the Edward Snowden leak showed that releasing internal data could be just as damaging and embarrassing to an entity - in those cases the Federal Government.

An issue with SPE was the ease and simplicity in which thieves were able to find sensitive information. A security audit conducted July 14 - August 1, 2014, by PriceWaterhouseCoopers (PWC), reported that one firewall and more than 100 other devices were not being monitored by SPE's in-house security team, and was an issue PWC warned could slow SPE's response time in a crisis situation. "Security incidents impacting these network or infrastructure devices may not be detected or resolved timely," warns PWC (Chmielewski, 2014) in its report. Over the 10-month analysis, PWC had alerted the studio to 193 security "instances" (Elkind, 2015 b). The final audit report released to SPE's General Counsel Leah Weil on September 25, 2014, just under two months prior to the attack, included recommendations for strengthening the company's security.

Following PWC's audit of SPE, Norse Corporation, a small threat intelligence firm, visited the SPE studio on November 3, 2014, to pitch its cybersecurity protection services to SPE executives and warned the company of its vulnerability of an attack. Norse Corporation also reported walking straight into the unlocked first floor of SPE's information security department containing unattended, logged-into computers, with no receptionist or security guard present at the door-- a display of SPE's overall sloppy security practices (Eklind, 2015 a).

On December 29, 2014, Norse executives delivered findings of their investigation, followed by the FBI issuing a public statement, "insisting there was 'no credible information' to implicate anyone but the North Koreans" (Elkind, 2015 c). It is now concluded that North Korea likely had the assistance of former SPE employees as well.

Timeline of Events

In highlighting the chain of events of the SPE hack, a pattern emerged of the way communication was handled in the months following the cyberattack. All communication was reactive in nature without initiative placed on getting ahead of potential stories or strategically moving forward with a proactive communications plan, both internally and externally.

(Robb, 2014)

Sony's Crisis Communication

Internal Communications

SPE seemed unprepared in its internal crisis communication efforts. Employees were left uninformed of the extent to which their data was leaked, and in the overall state of the company. "We got more information from blogs and websites than we did from Michael [Lynton, CEO of SPE] and Amy [Pascal, co-chair of SPE]," (Marikar, 2014) recalls an employee in an interview with *Fortune* on December 20, 2014.

Immediately after the hack, SPE was at a loss. With the control of their digital networks completely taken over, SPE employees and executives had minimal forms of communication—no email, no phones—which left the company in a state of crisis with drastically hindered communication ability. SPE executives circulated archived company Blackberrys to communicate with each other (Abdollah, 2015). *The Wrap* reported that "One of the insiders said the studio is '100 percent' shutdown, with staff using whiteboards to try to figure out what they've lost and what they need to try to do to bring themselves back online, to be able to function at all" (Cunningham & Waxman, 2014). In an effort to continue with their work, employees brought in personal laptops, and used personal email accounts and flash drives to share information. Employees resorted to colleagues passing along information to one another and relied on news updates from the media before any temporary email system was able to be set up for formal SPE internal communication (anonymous SPE employee, personal communication,November 15, 2015).

On November 30, 2014, six days after the attack, employees received the following email from SPE's IT department forwarded to them on personal accounts by their managers (names and emails have been removed for privacy) with the one word subject line, "Monday".

Hello - latest update from it-

A message from Sony Pictures: IT Disruption Update
This is a message from Sony Pictures. A Message From Michael Lynton and Amy Pascal.We want to give you an update on the progress that has been made in response to the system disruption that occurred last week. While our network remains offline, we have taken several important steps to assure on-going business continuity. On Monday we expect to be up and running with email and Wi-Fi access. This week we will also begin collecting and testing S P E-issued laptops and desktops. In the meantime, we will also provide new computers and will be distributing them on a prioritized basis for critical business needs. In light of recent news stories referencing the potential theft and disclosure of various Sony Pictures documents, we recognize that some of you are concerned about the confidentiality of your personal information. While we do not know whether such information has been taken, and we have no evidence of disclosure, we want to help address these concerns by making certain services available to you. You will receive more information on these services shortly. We also are recommending that you change the passwords on all online accounts, in particular for accounts you access from your office computer. We have asked our business leaders to connect with their teams on Monday to answer some of the questions we are hearing most frequently. We hope this open line of communication is helpful even though we don't yet have all of the answers, and we welcome any additional questions that you may have. We know this issue is causing certain day-to-day challenges, and we appreciate your continued patience and creative efforts to enable us to carry out our business as usual.

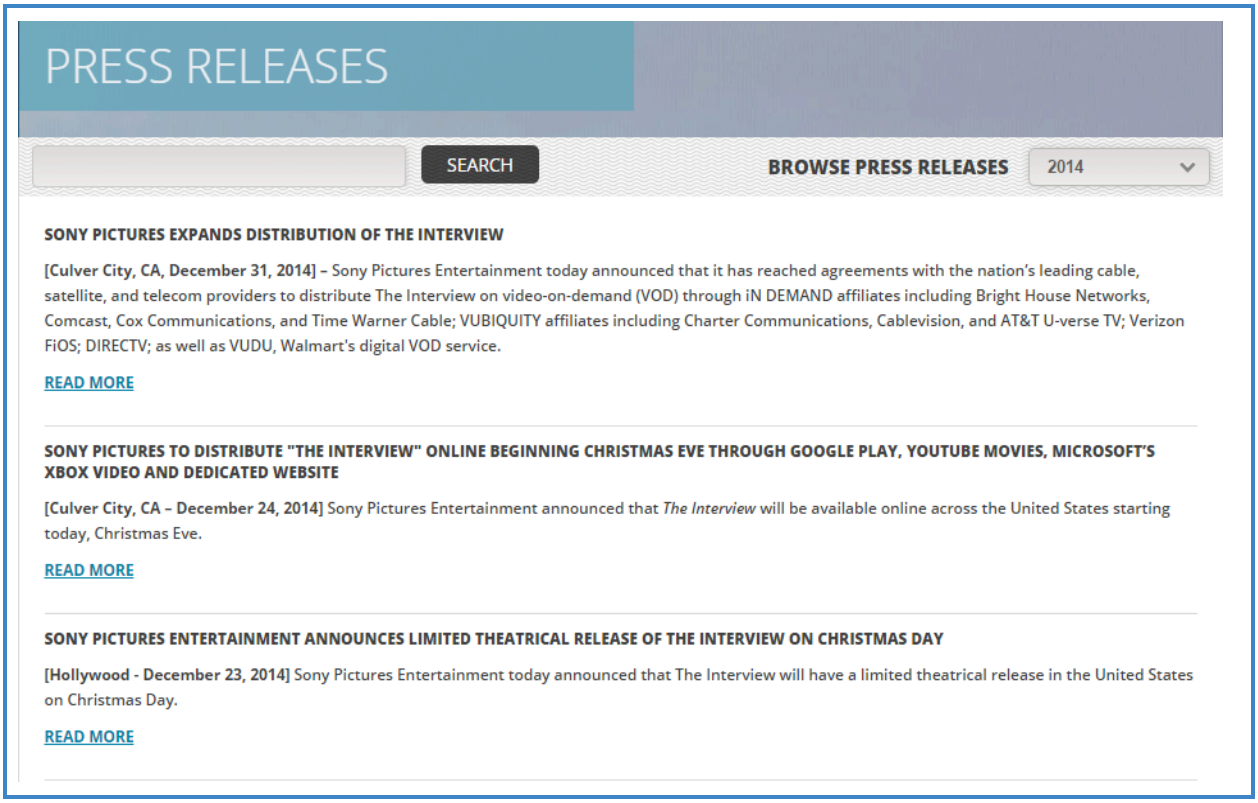
(anonymous SPE employee, personal communication, November 15, 2015)

Throughout the first few days after the cyberattack, SPE executives tried to keep employees informed by calling meetings to explain any bit of information they knew at the time, but struggled in providing answers and a way of releasing information to the company with SPE computers and social media accounts completely shut down. While a formal email announcement (see Appendix B) was not released until 10 days after the cyberattack once the company email was back up, in the interim, CEO Michael Lynton visited each department to provide an update to employees, letting them know the company was investigating the situation, and that its priority was keeping its employees safe. “The visit from the CEO definitely made everyone feel more at peace with the situation, and assured employees that their safety was a priority of the company,” recalled a current SPE employee who has been with the company since before the cyberattack. “People were really shaken up and felt that Sony did not communicate the situation well to employees—but all forms of communication were also shut down for so many days.”

However, the lack of communications implementation within the company during SPE’s major crisis could be attributed in part to not having a chief communications officer (CCO) on staff. It was not until May 2015 that Robert Lawson was named CCO of SPE. Lawson had worked closely with SPE during the security breach crisis while he was executive vice president at the strategic communications firm, Rubenstein PR. Prior to this, SPE had the misfortune of losing Senior Vice President of Communications Scott Sipkins shortly before the initial data breach. This resulted in no strategic guidance when dealing with the situation (Lang, 2015).

External Communications

For outward facing communications, SPE took a decidedly quiet approach. The company chose not to directly confront or address news outlets of the data breach. Without formally confirming the cyberattack, the only communications released through the SPE public relations team were press releases related to the *The Interview*. SPE decided not to even acknowledge the previous cancellation, or the reasoning behind the new release date.



PRESS RELEASES

SEARCH

BROWSE PRESS RELEASES 2014

SONY PICTURES EXPANDS DISTRIBUTION OF THE INTERVIEW

[Culver City, CA, December 31, 2014] – Sony Pictures Entertainment today announced that it has reached agreements with the nation's leading cable, satellite, and telecom providers to distribute The Interview on video-on-demand (VOD) through iN DEMAND affiliates including Bright House Networks, Comcast, Cox Communications, and Time Warner Cable; VUBIQUITY affiliates including Charter Communications, Cablevision, and AT&T U-verse TV; Verizon FiOS; DIRECTV; as well as VUDU, Walmart's digital VOD service.

READ MORE

SONY PICTURES TO DISTRIBUTE "THE INTERVIEW" ONLINE BEGINNING CHRISTMAS EVE THROUGH GOOGLE PLAY, YOUTUBE MOVIES, MICROSOFT'S XBOX VIDEO AND DEDICATED WEBSITE

[Culver City, CA – December 24, 2014] Sony Pictures Entertainment announced that *The Interview* will be available online across the United States starting today, Christmas Eve.

READ MORE

SONY PICTURES ENTERTAINMENT ANNOUNCES LIMITED THEATRICAL RELEASE OF THE INTERVIEW ON CHRISTMAS DAY

[Hollywood - December 23, 2014] Sony Pictures Entertainment today announced that The Interview will have a limited theatrical release in the United States on Christmas Day.

READ MORE

(sonypictures.com)

Beyond this, there was no effort made to externally communicate or acknowledge that the data breach or information theft had occurred. Though SPE maintained active social media accounts during this time, there was never mention of the hack. When the situation was brought up by outside observers through posts or comments, SPE chose not to respond.

Media Relations

Throughout the aftermath of the attack, SPE never publicly addressed the crisis with the media aside from its initial public announcement on November 24, 2014, stating that the company was investigating "an IT matter" (Elkind, 2015 c). The company considered the cyberattack an internal matter in nature, as it pertained to the private information of the company. The only outward action SPE took was an effort to bar media outlets from covering the hack and its embarrassing aftermath by having its law firm send a letter demanding the media destroy any company information obtained after the cyberattack, and to stop publicizing the company's stolen property (Feeny, 2014) (see Appendix C).

On December 14, 2014, SPE attorney, David Boies, wrote a letter to multiple news outlets stating, "We are writing to ensure that you are aware that SPE does not consent to your possession, review, copying, dissemination, publication, uploading, downloading or making any use of the stolen information." If journalists refused SPE's request, the company said it "will have no choice but to hold you responsible for any damage or loss" (Barnes, 2014). The

move was seen as one likely to fail by many First Amendment scholars and was criticized by multiple crisis management specialists (Hamedy, 2014).

Stakeholders Affected

The SPE security hack did far more to the company than stop the release of *The Interview* in theatres. The data compromised in the breach affected multiple stakeholders starting with the heart and soul of the company—its employees. Data security software firm, Identity Finder, showed that the 33,000 leaked files included the personal information, salaries (see Appendix D), and home addresses for employees and freelancers who worked for the company (Musil, 2014). Among the most important data exposed was 47,000 U.S. social security numbers belonging to celebrities, freelancers, and current and former SPE employees.

Employees

For internal employees of the company, SPE's cyberattack afflicted terror and confusion on the morning of November 24, 2014. The computer screens of SPE employees displayed the following message from the Guardians of Peace (GOP), warning SPE to cooperate by not releasing the film, *The Interview*.

(Picture provided following personal interview with SPE employee)

With the release of the following email warning, from the GOP directly to SPE employees, a few days after the initial attack, many employees feared for their personal safety and the safety of their families.

> "Please sign your name to object the false (sic) of the company at the email address below if you don't want to suffer damage. If you don't, not only you but your family will be in danger" (McNary, 2014).

In the time after the attack, "the FBI also visited the employees to discuss the safety of their personal information and general security after the attack. There was also heightened security on the [SPE] lot," explained the SPE employee. While SPE executives tried to recover

from the initial attack and reassure employees of their safety, the GOP released yet another warning email on December 16, 2014, to all employees, specifically referencing *The Interview*.

> "We will clearly show it to you at the very time and places *The Interview* be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to. Soon all the world will see what an awful movie Sony Pictures Entertainment has made. The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time. (If your house is nearby, you'd better leave.) Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment. All the world will denounce the SONY" (Boot, 2014).

Following the email threats and the compromising of all employee information, SPE provided employees (and former employees) with services from All Clear ID, an identity protection company, and promised to pay up to $10,000 in any potential damages. Still, employees continued to think about the effects of the data hack on them personally.

> "It's taken a toll, mentally—do I have to worry about someone getting a random medical procedure with my benefits? And there's the frustration at the way the top, top brass handled the situation. Why didn't they provide more for the employees? Why didn't they bring in security consultants?" (Marikar, 2014).

Partners

Undoubtedly, the impact of the SPE hack on its employees was unprecedented. However, gaining the most media attention during SPE's unfolding crisis, while causing the largest amount of controversy, was a series of leaked emails regarding some of Hollywood's A-list celebrities.

In an exchange of emails between producer Scott Rudin, and SPE's Co-Chairwoman Amy Pascal, Rudin expressed his disdain for Hollywood star Angelina Jolie over the use of director David Fincher who wanted to use Fincher for a project at the same time. Rubin responded to an email from Pascal with the following:

> "She'll survive it. I don't want to waste my time on this… I'm not destroying my career over a minimally talented spoiled brat who thought nothing of shoving this off her plate for eighteen months so she could go direct a movie… YOU BETTER SHUT ANGIE DOWN BEFORE SHE MAKES IT VERY HARD FOR DAVID TO DO JOBS."

Other celebrities who found themselves "targeted" in the leaked emails included Leonardo DiCaprio and comedian Kevin Hart. Perhaps the most notable, however, was Pascal's email referencing President Barack Obama. Before attending what was referred to in an email as a "stupid" fundraiser, Amy Pascal and producer Scott Rudin exchanged ideas as to what Pascal should talk to Obama about and referenced films about slavery. Shortly after the emails were leaked, both Pascal and Rudin publicly apologized stating:

> "The content of my emails to Scott were insensitive and inappropriate but are not an accurate reflection of who I am." -Amy Pascal (Reuters, 2014)

> “To anybody I’ve offended, I’m profoundly and deeply sorry, and I regret and apologize for any injury they might have caused” -Scott Rudin (Reuters, 2014)

Several days after the initial cyberattack, referencing a 9/11 type attack, another threat from the GOP was made targeting any theater that screened *The Interview*. Included were several major movie theatre chains (AMC Entertainment, Regal Entertainment and Cineplex Cinemas), all of which decided to pull out from screening the film. In response, each issued the following statements:

"Due to the wavering support of the film *The Interview* by Sony Pictures, as well as the ambiguous nature of any real or perceived security threats, Regal Entertainment Group has decided to delay the opening of the film in our theatres." - Regal Entertainment Group

"The recent cancellation of *The Interview*'s premiere and publicity appearances by its leading talent, and the overall confusion and uncertainty that has been created in the marketplace, brings into serious doubt whether the movie will open at all next week. At this time, to best enable AMC guests to plan their holiday movie-going with certainty and confidence, AMC is programming its theatres without *The Interview*." - AMC Theatres

"Cineplex takes seriously its commitment to the freedom of artistic expression, but we want to reassure our guests and staff that their safety and security is our number one priority." -Cineplex

(*Kilday,* 2014)

Motivated by the theater’s decision to not screen the movie, SPE decided against the release of *The Interview*. The decision to “give in” to the hackers did not sit well with Hollywood, or the American public. Many took to Twitter and other social media platforms to vent their disappointment and frustration. The following is an Internet poll by CNET.com, gathering the general public’s response.

HACKER PRESSURE

Was Sony right to cancel "The Interview”

- Ø Yes. It was necessary due to the threats. **14%**
- Ø No. Sony shouldn't bow to hacker threats. **73%**
- Ø Maybe. It depends on how credible the threats are. **7%**
- Ø Other. (Expand in comments.) **7%**

CAST YOUR VOTE

(Kooser, 2014)

Crisis Outcomes

Sony's Reputation

As part of a larger company with a history of cybersecurity breaches, and after suffering what experts have called the worst cyberattack in American corporate history, SPE's reputation was left battered at best. The goal of the attack, confirmed 25 days after the hack to have been launched by North Korea (Elkind, 2015 c), was to thoroughly embarrass the company, humiliate its executive management team, and shame the American film industry—and that is just what the hackers achieved. The SPE cyberattack was an extortion of its informational intelligence, sensitive employee files, and the company's business and communication practices. The "hack of the century" left the company in complete deflation.

CEO Michael Lynton told the *Associated Press*, "There's no playbook for this, so you are in essence trying to look at the situation as it unfolds and make decisions without being able to refer to a lot of experiences you've had in the past or other peoples' experiences," he said. "You're on completely new ground" (Donnelly, 2015).

Following the cyberattack, the SPE brand was irreparably damaged by the disclosures of sensitive employee information. The hack paralyzed the company for days as the media swarmed to pick up any information as it was released. "Essentially, this leak has left SPE out of control of their own brand. They no longer hold the capacity to drive the ship of company property and information dissemination, and now must deal in damage control," (Torossian, 2015), wrote Ronn Torossian, Public Relations Executive and CEO of 5W Public Relations, about the hack.

SPE suffered extreme criticism for its crisis response efforts. Aside from addressing the media demanding that the company's stolen information not be circulated, SPE never formally addressed the public following the cyberattack. Because SPE took this approach, it appeared very reactive to its crisis situation. PR professionals criticized SPE in its weak effort to stand up for itself. Torossian writes, "It's hard for the public to rally behind a brand that lets itself be pushed around and victimized" (Comcowich, 2015).

In the aftermath of deciding against the release of *The Interview*, SPE came under scrutiny and backlash from the White House. President Obama called the decision a "mistake." "If we set a precedent in which a dictator in another country can disrupt through cyber a company's distribution chain or its products, and as a consequence we start censoring ourselves, that's a problem," President Obama said (Comcowich, 2015).

Other celebrities took to social media to voice similar concerns as shown below.

Bill Maher @billmaher: #TheInterview Is that all it takes - an anonymous threat and the numbers 911 - to throw free expression under the bus? #PussyNation

Rob Lowe @RobLowe: Wow. Everyone caved. The hackers won. An utter and complete victory for them. Wow.

Critics also scrutinized SPE's security practices. "The company came across as unapologetic for their sloppy security and IT standards," commented Torossian. "Taken in conjunction with their recent PlayStation hack, the public is both unsympathetic and suspicious of the company's level of competence" (Comcowich, 2015). In SPE's view, the company was a blameless victim. Following the cyberattack in December 2014, CEO Michael Lynton, contended that his company was "extremely well prepared for conventional cybersecurity," but faced "the worst cyberattack in U.S. history" in an interview with National Public Radio, and described it as a "highly sophisticated attack" (Elkind, 2015 a). Because Sony's assailant was confirmed to be a foreign government, with far more resources than a typical band of hackers, SPE considered what happened to be unstoppable. "The studio simply faced an unfair fight" (Elkind, 2015 a).

Financial Impact

The cost of the SPE hack on the company is a complicated matter, as the effects took months to calculate. As of December 31, 2014, the company estimated in its preliminary third quarter financial results that it would spend $15 million to cover "investigation and remediation costs" related to the breach (Musil, 2015). On February 16, 2015, the company requested an extension to March 31, 2015, to report its third-quarter results since the "company was still working on key computer applications after 'a serious disruption of [the SPE] network systems occurred, including the destruction of network hardware and the compromise of a large amount of data on these systems'" (Musil, 2015). However, in that same month, SPE's senior general manager, Kazuhiko Takeda stated that the figure would be close to $35 million for the full fiscal year ending March 31, 2015 (Hornyak, 2015). As of November 2015, one year after the cyberattack, SPE has reported a loss in excess of $100 million due to the hack (Geraci, 2015).

In addition to financial hits to the company operations and sales, SPE also faces lawsuits by employees and former employees, alleging that the company failed to adequately secure its servers and protect its employee data. An article released by the *Associated Press* in October 2015, estimates lawsuit settlements for SPE employees and former employees could cost the company up to $8 million dollars for damages related to the hack, including losses, preventative measures and legal fees (*NBC News*, 2015).

Value and Significance

Significance of Cyber Security

The SPE hack was no insignificant security issue for the company, and is an eye-opener to other large companies whose security practices may not be up to industry standards and able to withstand theft by cybercriminals. While corporate America has become no stranger to security breaches in recent years, a cyberattack such as this demonstrates the power and capability to inflict damage beyond physical proximity. While it is not actively visible, cyberterrorism is a top global security threat with the potential to cause more damage than espionage or weapons of mass destruction. In this case, SPE was made an example to others as the attack was meant more for embarrassment and exposure than a major

debilitation to the company. As the need to share information grows every day, cyberterrorism is an evolving issue and everyone should be active in preventing it (Elkind, 2015 c).

Cybercrime is also not limited to large public corporations. “According to the National Cyber Security Alliance, one out of every five small businesses is a victim of cybercrime each year; and of those hit, 60% go out of business” (Brown, 2015). Combined with IBM estimating that the average number of cyberattacks on a single corporation over one week is 1,400, it is safe to say that no organization or company is too small to be a target. As more and more companies move their resources to servers and digital platforms, security practices are imperative to protecting data, proprietary information and intellectual property. According to Bloomberg *Businessweek*, “today cybercrime costs businesses $450 billion globally, and $100 billion in the U.S. each year,” with those numbers continually rising (Geraci, 2015).

In the past, business leaders did not spend a lot of time understanding cybercrime and security protocol, but now with the rise of digital sharing of information, there is a much greater awareness of security on multiple levels. Today, CIOs and CEOs are required to have a certain level of knowledge about cybersecurity and the effects it could have on their companies; and this level of knowledge is constantly increasing (Bussey, 2015).

Not only should companies address cybersecurity efforts within their own companies, but they should also assess the practices and processes of third party service providers that handle sensitive information for the company.

Lessons Learned

As the aftermath of SPE’s unprecedented cyberattack has been analyzed, there are many lessons to be learned. SPE, a company that received multiple warnings prior to November 2014 and had also been hacked previously (with the most notable hack being Sony’s Playstation Network in 2011 that cost the company $171 million), could have benefitted from a full investigation and analysis of its security practices. Companies that fall victim to cyberattacks should conduct an internal crisis analysis to see what went wrong and how future issues can be avoided. However, SPE proved not to have learned from its past mistakes in managing for the future.

The SPE hack was significantly worsened because of poor security protocols practiced by virtually every level of employee in the company. The hack is arguably the worst attack a company has experienced to date, and is a reminder to all companies to reassess their security practices by identifying and properly addressing every stage of risk to their digital assets, to evaluate their crisis communication plan, and to assign roles to C-Suite officers to properly execute a crisis management plan in the time of need.

This calls for proper attention given to security practices from all levels of employees, under the leadership of the executive team. In the November 2015 issue of Bloomberg *BusinessWeek*, Davis Hake, Director of Cybersecurity Strategy for Palo Alto Networks, a leading cybersecurity firm in California, explains that gaining a “bottom up view” of a company’s cybersecurity risks should be the primary focus of executives. Most importantly, companies should not forget about their director of corporate communications or chief communication officer. “If you've faced a significant breach, corporate communication is key because public response will dramatically affect your brand perception,” says Hake (Geraci,

2015). While employees should be effectively trained in security measures, proper communication of those protocols is critical.

In today's business world, the center of communication efforts within a company, the CCO, must be an 'integrator' of knowledge and awareness across the company, bridging the C-Suite with the rest of the employees, especially when it comes to addressing critical issues with potentially crisis-causing results. Doing this will ensure the company thinks like and performs like its corporate character, something of utmost importance in upholding its reputation. In today's competitive business environment, all stakeholders notice an organization's corporate character and social responsibility efforts. Management of corporate character involves the integration of the organization's reputation and culture," (Arthur W. Page Society, 2012) and should, therefore, be implemented throughout company processes and protocols.

In the event of a crisis, the CCO of a company should actively participate in executive meetings so as to have the knowledge to effectively communicate to the public on behalf of the company. In the event of a cyberattack, does a company want to be known for its inadequate security practices, poor internal and external crisis communications and have its embarrassing personal secrets aired to the public? How a company handles a crisis situation will effectively showcase its true character.

References

Abdollah, T. (2015, January 9). Sony CEO breaks down hack response, Google role in 'The Interview' release. *Mercury News*. Retrieved November 23, 2015, from http://www.mercurynews.com/business/ci_27290586/sony-ceo-breaks-down-hack-response-google-role?source=infinite-up

Arthur W. Page Society (2012). Building Belief: A News Model for Activating Corporate Character & Authentic Advocacy. Retrieved November 23, 2015, from http://www.awpagesociety.com/wp-content/uploads/2012/11/Building-Belief-New-Model-for-Corp-Comms.pdf

Barnes, Brooks (2014 December 14) Sony Pictures Demands That News Agencies Delete "Stolen" Data. *The New York Times*. Retrieved November 22, 2015 from http://www.nytimes.com/2014/12/15/business/sony-pictures-demands-that-news-organizations-delete-stolen-data.html?_r=0

Boot, W. (2014, December 16). Sony Hackers Issue 9/11 Warning. *The Daily Beast*. Retrieved November 23, 2015, from http://www.thedailybeast.com/articles/2014/12/16/sony-hackers-issue-9-11-warning.html

Brown, R. (2015, March/April). Solving the complex riddle of CYBERSECURITY. *Rural Telecommunications*, 34(2), 20-23. Retrieved November 23, 2015, from http://ezproxy.depaul.edu/login?url=http://search.proquest.com/docview/1672176017?accountid=10477

Bureau of Justice Statistics (BJS) (2010). *Cybercrime*. Retrieved November 23, 2015, from http://www.bjs.gov/index.cfm?ty=tp&tid=41

Bussey, J. (2015, February 9). How the Sony Breach Changes Cybersecurity. *Wall Street Journal.* Retrieved November 23, 2015, from http://www.wsj.com/articles/how-the-sony-data-breach-signals-a-paradigm-shift-in-cybersecurity-1423540851

Chmielewski, D., & Hesseldahl, A. (2014, December 12). Sony Pictures Knew of Gaps in Computer Network Before Hack Attack. *Re/Code*. Retrieved November 23, 2015, from http://recode.net/2014/12/12/sony-pictures-knew-of-gaps-in-computer-network-before-hack-attack/

Clapper, J. (2013, March 12). *Worldwide Threat Assessment of the US Intelligence Community*. Retrieved November 23, 2015, from http://www.odni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf

Comcowich, William (2015 January 16). Key PR Lessons from the Sony Hacking Nightmare. *Cyber Alert*. Retrieved on November 22, 2015, from http://www.cyberalert.com/blog/index.php/key-pr-lessons-from-the-sony-hacking-nightmare/

Cunningham, T., & Waxman, S. (2014, November 28). Sony Struggles to Fight #GOP Hackers Who Claim Stolen Data Includes Stars' IDs, Budget and Contract Figures. *The Wrap*. Retrieved November 23, 2015, from http://www.thewrap.com/sony-execs-working-on-chalkboards-while-hackers-claim-stolen-data-includes-stars-ids-budget-and-contract-figures/

Donnelly, Matt (2015 January 6) Sony's Michael Lynton Promises to "Renew and Redefine. *The Wrap*. Retrieved on November 21, 2015, from http://www.thewrap.com/sonys-michael-lynton-promises-to-renew-and-redefine-read-internal-staff-memo/

Elkind, P. (2015). Sony Pictures: Inside the Hack of the Century; part 1. *Fortune*. Retrieved November 23, 2015, from http://fortune.com/sony-hack-part-1/

Elkind, P. (2015). Sony Pictures: Inside the Hack of the Century; part 2. *Fortune*. Retrieved November 23, 2015, from http://fortune.com/sony-hack-part-two/

Elkind, P. (2015). Sony Pictures: Inside the Hack of the Century; part 3. *Fortune*. Retrieved November 23, 2015, from http://fortune.com/sony-hack-final-part/

Feeny, N. (2014, December 15). Sony Asking Media Outlets to Stop Covering Hacked Emails. *TIME*. Retrieved November 23, 2015, from http://time.com/3633385/sony-hack-emails-media/

Gaudiosi, J. (2014, December 24). Why Sony didn't learn from its 2011 hack. *Fortune*. Retrieved November 23, 2015, from http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/

Geraci, R. (n.d.). CEOs and Cyber Defense:The New Reality. *Bloomberg Media*. Retrieved November 23, 2015, from http://www.bloombergmedia.com/assets/pdfs/custom-publishing/151102_Cyber_Security_2.pdf

Government Accountability Office. (2013) *CYBERSECURITY A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*. Retrieved November 23, 2015, from http://www.gao.gov/assets/660/652817.pdf

Hamedy, S. (2014, December 14). Sony calls on media to stop publishing hacked documents. *The Los Angeles Times*.Retrieved November 23, 2015, from http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-boies-20141215-story.html

Hornyak, T. (2015, February 4). Hack to cost Sony $35 million in IT repairs. *Network World*. Retrieved November 23, 2015, from http://www.networkworld.com/article/2879814/data-center/sony-hack-cost-15-million-but-earnings-unaffected.html

Kilday, Gregg (2014, December 17). Top Five Theater Circuits Drop 'The Interview' After Sony Hack. *The Hollywood Reporter*. Retrieved on November 20, 2015, from http://www.hollywoodreporter.com/news/source-top-five-theater-circuits-758843

Lang, B. (2015, May 12). Sony Pictures Entertainment Taps Robert Lawson as Chief Communications Officer. *Variety*. Retrieved November 23, 2015, from http://variety.com/2015/film/news/sony-pictures-entertainment-taps-robert-lawson-as-chief-communications-officer-1201493370/

Marikar, S. (2014, December 20). I work at Sony Pictures. This is what it was like after we got hacked. *Fortune*. Retrieved November 23, 2015, from http://fortune.com/2014/12/20/sony-pictures-entertainment-essay/

McNary, D. (2014, December 5). Hackers Threaten Sony Employees in New Email: 'Your Family Will Be in Danger'. *Variety*. Retrieved November 23, 2015, from http://variety.com/2014/film/news/hackers-threaten-sony-employees-in-new-email-your-family-will-be-in-danger-1201372230/

Musil, S. (2014, December 4). Sony hack leaked 47,000 Social Security numbers, celebrity data. *CNET*. Retrieved November 23, 2015, from http://www.cnet.com/news/sony-hack-said-to-leak-47000-social-security-numbers-celebrity-data/

Musil, S. (2015, February 4). Sony Pictures hack has cost the company only $15 million so far. *CNET*. Retrieved November 23, 2015, from http://www.cnet.com/news/sony-pictures-hack-to-cost-the-company-only-15-million/

NBC News (2015, October 20). Sony Hack Lawsuit Settlement Could Cost Company Up To $8 Million. Retrieved November 23, 2015, from http://www.nbcnews.com/tech/security/sony-hack-lawsuit-settlement-could-cost-company-8-million-n447896

Reuters (2014, December 11). Sony co-chair apologizes for 'insensitive' emails about Obama's race. *Fortune*. Retrieved November 20, 2015, from http://fortune.com/2014/12/11/sony-co-chair-apologizes-for-insensitive-emails-about-obamas-race/

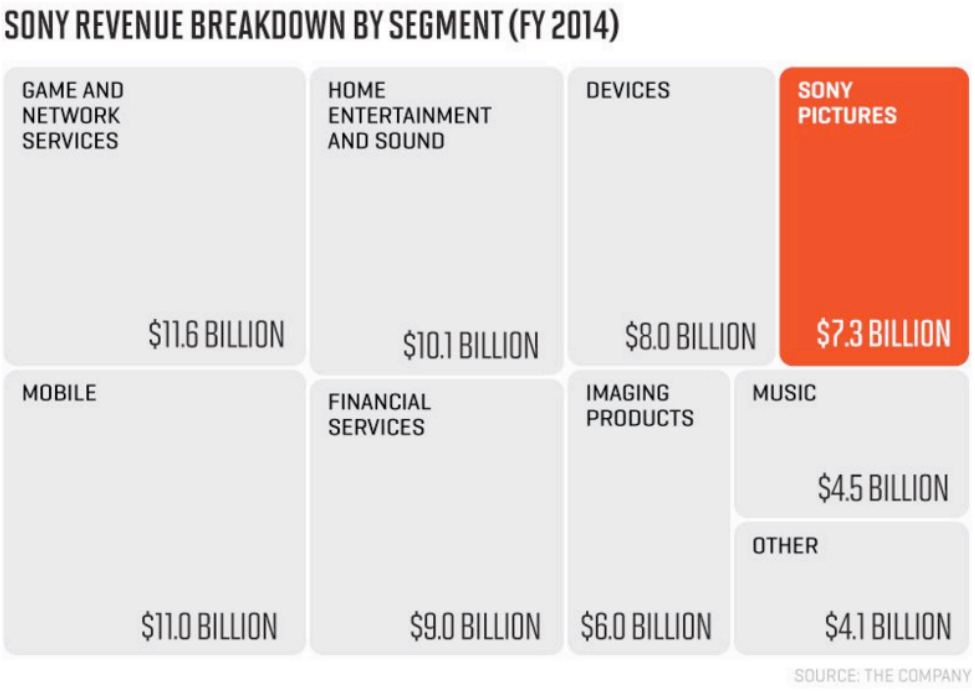
Robb, David (2014 December 22). Sony Hack: A Timeline. *Deadline*. Retrieved November 21, 2015 from http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

Torossian, R. (2014, December 23). Public Relations & Damage Control in the Aftermath of the Sony Hack. *Business 2 Community*. Retrieved November 23, 2015, from http://www.business2community.com/crisis-management/public-relations-damage-control-aftermath-sony-hack-01104738#l5rkQbTrAc1FVkjU.97

Appendices

Appendix A

A visual representation of SPE's revenue contribution to Sony Corporation as a whole. Retrieved from: http://fortune.com/sony-hack-part-two/



Appendix B

A formal letter from SPE to its employees addressing the cyberattack. Retrieved from: http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf

10202 West Washington Boulevard
Culver City, California 90232-3195

December 8, 2014

Dear SPE Employee:

Sony Pictures Entertainment ("SPE") is writing to provide you with a summary of SPE's prior communications regarding the significant system disruption SPE experienced on Monday, November 24, 2014, as well as to provide you with additional detail.

As you know, SPE has determined that the cause of the disruption was a brazen cyber attack. After identifying the disruption, SPE took prompt action to contain the cyber attack, engaged recognized security consultants and contacted law enforcement.

SPE learned on December 1, 2014, that the security of personally identifiable information that SPE received about you and/or your dependents during the course of your employment may have been compromised as a result of such brazen cyber attack. Although SPE is in the process of investigating the scope of the cyber attack, SPE believes that the following types of personally identifiable information that you provided to SPE may have been obtained by unauthorized individuals: (i) name, (ii) address, (iii) social security number, driver's license number, passport number, and/or other government identifier, (iv) bank account information, (v) credit card information for corporate travel and expense, (vi) username and passwords, (vii) compensation and (viii) other employment related information. In addition, unauthorized individuals may have obtained (ix) HIPAA protected health information, such as name, social security number, claims appeals information you submitted to SPE (including diagnosis and disability code), date of birth, home address, and member ID number to the extent that you and/or your dependents participated in SPE health plans, and (x) health/medical information that you provided to us outside of SPE health plans.

As SPE previously notified you, SPE has made arrangements with a third-party service provider, AllClear ID, to offer all employees and dependents twelve (12) months of identity protection services at no charge. As a reminder, to obtain credit monitoring and identity theft insurance, you will need to enroll. On Wednesday, December 3, 2014, you received an email from SonyPictures@AllClearID.com. This email contained your unique, nontransferable activation code for enrolling in the AllClear identity theft protection services. In addition, since December 3, 2014, you have had access to identity repair assistance. AllClear ID's multi-language call center is available to respond to your questions and assist you Monday-Saturday, from 8 am to 8 pm CST. You may also email AllClear ID's support center at support@allclearid.com.

For your security SPE encourages you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. Neither SPE nor anyone acting on its behalf will contact you in any way, including by email, asking for your credit card number, social security number or other personally identifiable information. If you are asked for this information, you can be confident SPE is not the entity asking. To protect against possible identity theft or other financial loss, SPE encourages you to remain vigilant, review your account statements, monitor your credit reports and change your passwords. SPE is providing the following information for those who wish to consider it:

- You may wish to visit the web site of the U.S. Federal Trade Commission at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or reach the FTC at 1-877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.

- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus are listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

    - Experian: (888) 397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
    - Equifax: (800) 525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
    - TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Please contact us at (855) 731-6013 should you have any additional questions.

Appendix C

Copy of letter from Sony's lawyer, David Boies, to the media. Retrieved from: https://assets.documentcloud.org/documents/1380456/sonyletter.pdf

BOIES, SCHILLER & FLEXNER LLP
333 MAIN STREET • ARMONK, NY 10504 • PH. 914.749.8200 • FAX 914.749.8300

December 14, 2014

Via Email and Courier

The Hollywood Reporter
770 Broadway
New York, NY 10003
ATTN: General Counsel/Legal Department

RE: Your Possession of Privileged and/or Confidential Information Stolen From Sony Pictures Entertainment

Dear General Counsel:

As you are no doubt aware, Sony Pictures Entertainment (SPE) has been the victim of a theft of data stored on its computers. As you may also be aware, in an on-going campaign explicitly seeking to prevent SPE from distributing a motion picture, the perpetrators of the theft have threatened SPE and its staff and are using the dissemination of both private and company information for the stated purpose of materially harming SPE unless SPE submits and withdraws the motion picture from distribution.

We have reason to believe that you may possess, or may directly or indirectly be given, illegally obtained documents or other information stolen from SPE (the "Stolen Information"), pursuant to the perpetrators' scheme. The Stolen Information includes, but is not limited to, documents and information protected under U.S. and foreign legal doctrines protecting attorney-client privileged communications, attorney work product, and related privileges and protections, as well as private financial and other confidential information and communications of SPE's current and former personnel and others, confidential personnel data, intellectual property, trade secrets and other business secrets and related communications, and other confidential information. We are writing to ensure that you are aware that **SPE does not consent to your possession, review, copying, dissemination, publication, uploading, downloading, or making any use of the Stolen Information, and to request your cooperation in destroying the Stolen Information**.

As soon as you suspect that you may have possession of any of the Stolen Information, we ask that you promptly:

(1) notify us using the contact information provided below;

(2) take all reasonable actions to prevent your company and any of your employees, independent contractors, agents, consultants, or anyone who may have access to your files from examining, copying, disseminating, distributing, publishing, downloading, uploading, or making any other use of the Stolen Information;

(3) arrange for and supervise the destruction of all copies of the Stolen Information in your possession or under your control, particularly information protected under U.S. and foreign legal doctrines protecting attorney-client privileged communications, attorney work product, and related privileges and protections, as well as private financial and other confidential information and communications of SPE's current and former personnel and others, confidential personnel data, intellectual property, trade secrets and other business secrets and related communications; and

(4) confirm that such destruction has been completed.

In addition, if you have provided the Stolen Information to anyone outside of your company, we ask that you provide them with a copy of this letter, and request the destruction of the Stolen Information by the recipient.

To discuss matters concerning the Stolen Information, please contact me at dboiesspe@bsfllp.com or (914) 749-8245.

If you do not comply with this request, and the Stolen Information is used or disseminated by you in any manner, SPE will have no choice but to hold you responsible for any damage or loss arising from such use or dissemination by you, including any damages or loss to SPE or others, and including, but not limited to, any loss of value of intellectual property and trade secrets resulting from your actions.

If you have previously had access to or received Stolen Information and have exercised restraint with regard to its publication, use or dissemination, SPE and its employees are sincerely grateful to you and ask for your continued exercise of restraint.

Please note that this letter is provided to you without prejudice and does not purport to address all facts and issues concerning the Stolen Information. SPE expressly reserves all rights, remedies, claims and defenses available to it under applicable law.

Thank you for your anticipated and immediate cooperation regarding this important matter.

Sincerely yours,

David Boies

David Boies

cc: Leah Weil, Esq.
Michele Singer, Esq., General Counsel, Prometheus Global Media

Appendix D

Salaries of SPE's top executives leaked in the cyberattack. Retrieved from: http://www.businessinsider.com/hacked-sony-docs-top-execs-paychecks-2014-12#ixzz3KqaE1HCX

Name	Newest Hire Date	Orginal Hire Date	Job Code Title (Default)	Business Title	Annual Rate
Lynton, Michael	1/5/04	1/5/04	CEO, SCA, Chairman and CEO, SPE	CEO, Sony Corporation of America, Chairman and	3,000,000.00
Pascal, Amy B	1/13/97	12/14/87	Co-Chair SPE (10)_Corp_LA	Co-Chairman SPE & Chairman MPG	3,000,000.00
Mosko, Stephen M	11/18/91	11/18/91	Pres SPT (10)_SPT_LA	President, SPT	2,800,000.00
Belgrad, Doug	9/13/89	9/13/89	Pres Theatrical Films (10)_MPG_LA	President, Columbia Pictures	2,350,000.00
Culpepper, Clinton R	3/30/92	3/30/92	Pres Screen Gems (10)_MPG_LA	President, Screen Gems	1,800,000.00
Singh, Man Jit	3/19/07	3/19/07	Pres SPHE (10)_SPHE_LA	President, SPHE Worldwide	1,800,000.00
De Luca, Michael	3/1/14	3/1/14	Pres Prod (09)_MPG_LA	President of Production	1,500,000.00
Van Amburg, Zackary A	9/6/96	9/6/96	Pres Prog (09)_SPT_LA	Pres Programming	1,500,000.00
Erlicht, Jamie B	7/8/02	8/25/97	Pres Prog (09)_SPT_LA	Pres Programming	1,500,000.00
Kaplan, Andrew J	9/23/02	2/25/87	Pres Networks (09)_SPT_LA	President, Worldwide Networks	1,380,000.00
Osher, Robert	5/17/04	5/17/04	Pres Digital Prod (10)_SPDP_LA	President, Digital Production	1,250,000.00
Weiser, John	3/7/88	3/7/88	Pres TV Dist (09)_SPT_LA	President, Distribution	1,175,000.00
Bersch, Steven N	1/31/08	1/31/08	Pres Acquisitions (09)_MPG_LA	President, WW Acquisitions Group	1,150,000.00
Caines, Dwight R	2/18/97	2/18/97	Pres Mktg (09)_MPG_LA	President, Sony Pictures Entertainment Theatrical	1,050,000.00
Bernard, Tom	1/27/92	1/27/92	Co-Pres SP Classics (10)_MPG_NY	Co-President, SP Classics	1,000,000.04
Barker, Michael	1/27/92	1/27/92	Co-Pres SP Classics (10)_MPG_NY	Co-President, SP Classics	1,000,000.04
Pavlic, Michael	1/26/09	8/4/03	Pres Creative Svcs/Ad (08)_MPG_LA	President, Worldwide Creative Advertising	1,000,000.00