Sony Pictures Entertainment, Inc.:  
A Cybersecurity Attack from North Korea (A)

Cyberattack

November 24, 2014 began like most other days for Michael Lynton, Chief Executive Officer of Sony Pictures Entertainment. Upon arriving at the office, Lynton received a call from CFO David Hendler informing Lynton that Sony’s cybersecurity had been compromised. Employees started their computers that morning only to find disturbing images of Lynton’s severed head appear on their screens. Shortly after, Sony shut down all computer systems worldwide, issuing the following statement: “We are investigating an I.T. matter.”¹

The next day, four of the studio’s unreleased movies were posted on pirate Web sites. The hackers also claimed to have stolen approximately 100 terabytes of internal data, including personal and confidential information from thousands of Sony Pictures employees.² Lynton and Sony executives could not have predicted that in three short weeks, the digital attack would be at the center of a global controversy. In total, eight leaks released an estimated 38 million files and thousands of personal, damaging e-mails belonging to Sony Pictures executives.³ According to investigators, the magnitude of the data published was simply unprecedented in U.S. corporate history.

Sony Pictures soon found its brand identity under scrutiny, making headlines in all major news sources. Rich Klein, partner at McLarty Associates advisory firm, called the event “an international crisis, the cyberattack that put Americans’ vulnerability on display, a free speech cause, an Oval Office gut-check, and a cautionary tale for the future of warfare.”⁴

Entering the Motion Picture Entertainment Business

Sony Pictures is a United States based subsidiary of Sony Corporation. Sony Corporation was established in 1946 and based in Tokyo, Japan.⁵ In 1960, Sony Corporation of America was established in the United States and was listed on the New York Stock Exchange in 1970. Late in the Twentieth Century, Sony had become one of the world’s leading consumer electronics manufacturers.

In 1991, Sony acquired Columbia Pictures Entertainment and renamed it Sony Pictures Entertainment, Inc., (SPE). In 2004, Michael Lynton joined SPE as Chairman and Chief Executive Officer. That same year, Amy Pascal was promoted to Chairman of the Motion Picture Group, and to Co-Chairman of SPE two years later. In 2006, SPE crossed the $1 billion mark in domestic box-office receipts for the fifth year in a row.⁶
Sony pledged to operate SPE as independently as possible. The motion picture business represents 10% of revenue for the parent corporation. Although SPE provides just a small fraction of the company’s total income, the motion picture business bears Sony’s name, which carries major implications for the Sony brand.

Size and Scope of Sony Motion Picture Entertainment

The entertainment division is one of the most profitable sectors of the company. Sony Motion Pictures has retained profits between 4% and 7% in recent years, while the electronics divisions have operated consistently in the red. In the fiscal year ending March 31, 2014, Sony Pictures reported $8 billion in revenue. (See Appendix A).

Sony is a major player in the motion picture industry with 199 completed movies. Sony Motion Pictures Entertainment retains an estimated 12.2% of market share, which can be compared to 20th Century Fox (17.3%), Buena Vista (15.6%), and Warner Bros (15.1%). In sum, these four enterprises account for approximately 60% of the total market. Universal and Paramount – other well-known players – both lag behind Sony with respect to market share. (See Appendix B for additional industry information.)

Technology Revolutionizes the Filmmaking Business

New video technology has revolutionized the way movies are made. Historically, 35mm film was the standard for producing, distributing, and displaying motion pictures. This required the physical film to be copied and distributed to theaters. In 2002, Star Wars: Episode II led the charge as the first movie shot entirely on digital video. This helped inspire an entire digital generation of producers and editors, offering cost savings in both time and money and flexibility and simplicity in post-production edits.

Digital movies are essentially very large computer files that theaters are able to play on as many movie screens as they desire. In years past, a theater was dependent on the number of film reels that could be manually delivered to them. Now, via satellite delivery, theaters have much greater flexibility, which affords the capability to match screen decisions to consumer demand. In 2013, the Digital Cinema Distribution Coalition provided digital distribution technologies to more than 1,200 theaters and 17,000 screens.

While digital movie distribution has major benefits, it does not come without its drawbacks and risks. Enhanced security protocols, such as encryption techniques, are necessary to help prevent piracy. Distribution, a critical component of the movie industry, has also changed as a result, requiring theaters to invest in new digital projection equipment. This investment represents a large capital expenditure for theaters, costing as much as $70,000 per screen for a digital cinema retrofit. Fortunately, studios and distributors have helped theaters offset such costs due to the importance of digital distribution. Sony Pictures, for example, relies on exhibitors to generate box office sales. The risk is assumed by exhibitors who choose to turn screens over to Sony and rely on Sony to drive consumer demand and produce box office hits.
2014: The Year of Cybersecurity Attacks

The digital age has led to a new era of crime and theft of corporate assets. Companies now store important data such as corporate assets, company records, and customer information digitally. This lends itself to the possibility that hackers could retrieve this valuable information if proper security standards are not set and followed.

The year 2014 was popular for corporate data theft. Target, Snapchat, Forbes, Michael’s, eBay, Home Depot, and USPS all suffered major data breaches. CNBC has estimated that over one billion personal data records were compromised that year as a result of approximately 1,500 incidents. This is a 78% increase from 2013. Hackers were able to retrieve everything from users’ e-mail messages, passwords, and credit card information, to employee data and phone numbers. The cyberattacks were designed to access customers’ financial accounts, as well as sensitive information that might allow identity theft. The Target hack, for example, resulted in the online auction of 2 million credit cards, allowing hackers to steal some $53 million. Trends in data hacking reveal that cybercriminals are shifting focus from short-term credit card theft to long-term identity theft, which helps to create sustainable revenue streams.

Sony’s Data Protection Controls

Security experts examining Sony’s malware discovered that the hackers were familiar with Sony’s network long before the breach occurred. Evidence suggests that the attackers gained control of Sony’s private cryptographic keys, which secured encrypted information. Control of these keys allowed suspicious movements of data to go undetected.

Historically, Sony has been a popular target for hackers. In 2011, account information of 77 million Sony Playstation users was stolen. It was reported that Sony was threatened in advance of this breach and failed to implement adequate safeguards to protect it, even though it is a company’s responsibility to change their keys frequently, especially after notification of vulnerabilities.

A class-action complaint was filed against Sony in response to the 2014 cyberattack. The complaint alleges that, “Sony failed to secure its computer systems, servers, and databases (‘Network’), despite weaknesses that it has known about for years . . . .” and, “Sony subsequently failed to timely protect confidential information of its current and former employees from law-breaking hackers . . . .”

The Interview: A Comedy

SPE was in the final preparations for launching The Interview to theaters nationwide when the cyberattack occurred. The movie, a fictional comedic film depicting the attempted assassination of North Korean leader Kim Jong-un, starred Seth Rogen and James Franco. It was directed by Evan Goldberg and Seth Rogen. Sony invested $44 million in production, and the movie was
projected to bring in $90 million in revenue, based on a strong record of comedies starring Seth Rogen.\textsuperscript{22} Sony embarked on a major marketing campaign prior to the movie’s winter premiere. Advertising costs were estimated to reach nearly $30 million.\textsuperscript{23}

Sony Corporation CEO Kazuo Hirai voiced concerns soon after learning about the film’s plot because of Japan and North Korea’s tense bilateral relationship. Hirai sent formal demands to Pascal and the team to change parts of the film after receiving warnings from North Korean news agencies in June of 2014.\textsuperscript{24}

Sony executives worked with government think tanks to talk about possible political consequences. The company made some changes, such as using “Columbia Pictures” instead of the Japanese Sony brand. Direct retribution from North Korea was simply not envisioned as a credible threat.\textsuperscript{25} Various entertainment media reported that studio executives questioned whether \textit{The Interview} should refer to the real North Korean regime or, perhaps, a fictitious dictator.\textsuperscript{26} After consulting with several experts, Lynton was told the film was safe to release.

The movie was set to premiere on Christmas Day, December 25, 2014, at all major cinemas across the United States. The launch plan included premieres in 10 other countries within the following eight weeks.\textsuperscript{27} (See Appendix C for the movie poster.)

\textbf{North Korea’s Involvement}

The Democratic People’s Republic of Korea is a rigidly authoritarian state that has been led by the Kim family for more than 60 years.\textsuperscript{28} North Korea maintains strict government controls over its citizens, including many that are thought to violate basic human rights. Draconian laws involving severe punishment enforce citizen loyalty to the North Korean regime. Although North Korea limits access to the Internet, the nation maintains a robust corps of computer hackers.\textsuperscript{29} The North Korean regime chooses some of its best talent for cyberwarfare training and allocates substantial resources to maintain and develop the program. “Cyberwarrior,” in fact, is a highly coveted government position.\textsuperscript{30}

North Korea’s reaction to \textit{The Interview} reflects the unusually strict ideology of the country. The movie parodied the country’s leader and his imagined assassination. The depiction of Kim Jong-un and his dynasty as fallible – an impossible and frightening image to the regime – likely helped to inspire calls for retribution.\textsuperscript{31} Credible, material evidence gathered following the data breach indicates that the hackers engineered the attack to damage Sony’s computer systems and to humiliate the company, thereby proving their loyalty to Kim Jong-un. This objective differs from the majority of corporate hacks, which focus on financial gain.

On December 19\textsuperscript{th}, the United States government was able to confirm that the hack originated in North Korea. Investigators found significant overlap between the digital fingerprints of the Sony attack to other North Korean cyberattacks on South Korean banks. The U.S. stated that it viewed the event as a “serious national security matter.”\textsuperscript{32}
The Aftermath of the Cyberattack

In the immediate aftermath of the cyberattack, Sony’s communication system was shut down. Senior executives quickly implemented alternative communication networks at the company, leveraging phone trees, notepads, and outdated cell phones. The compromised system at Sony Pictures took weeks to restore. The hackers not only stole Sony’s data, but had completely erased it.

The attackers threatened to leak Sony movies as well as thousands of internal documents and the personal information of more than 47,000 people, including employees, freelancers, and movie stars. They did not identify themselves or issue specific demands. Although it was suspected that the hack was perpetrated by North Korean cybercriminals, officials of the DPRK denied all allegations. This made it difficult to communicate details surrounding the attack to employees and external parties.

The crisis-management team at Sony Pictures set up desks to help employees with credit protection and fraud alerts. The team also set up new e-mail accounts and telephone numbers. They were doing what they could to shift all digital systems back to traditional pen-and-paper methods; however, it seemed to be too late. The hackers already had accessed all the data they needed to irrevocably damage Sony’s reputation.

Leadership

Sony Corporation CEO Kazuo Hirai played a negligible media role during the attack, preferring to place his confidence in Lynton and Pascal. However, Hirai claimed he signed off on all external communication and decisions made with regards to the cyberattack.33 CEO Michael Lynton, reserved and analytical, was forced to jump into the spotlight, shadowing Motion Picture Chief, Amy Pascal, who had long been the “face of Sony Pictures.” Pascal’s credibility had deteriorated after several of her e-mails surfaced on December 8th and 10th, which included celebrity insults and racist comments involving President Obama.34

Sony leadership promised employees that they would receive an e-mail outlining steps to sign up for identity protection services. Two days after the promised e-mail, 47,426 unique social security numbers and other personal information of more than 15,000 current and former Sony employees were leaked.35 (Appendix D outlines details of this memo.)

Sony took a gamble when deciding how to respond to the cyberattack. Several employees would later allege that Sony knew about the risks to its digital storage and the geopolitical sensitivity of The Interview but chose to make decisions that were not in the best interest of Sony employees.
In response to the allegations that Sony did not react well to the cyberattack, CEO Michael Lynton said that he felt otherwise. He stated that his top priority was to make important decisions quickly, saying, “You can’t be caught in the headlights doing nothing.” Lynton described the situation as difficult, with no playbook to follow.

**Revenue at Stake as Theaters Cancel Film Showing**

On December 15th, the Guardians of Peace (#GOP) claimed responsibility for the Sony hack and threatened major terrorist attacks on theaters showing the film. Theaters such as Regal Entertainment Group, AMC Entertainment Holdings Inc., Cinemark Holdings Inc., and Carmike Cinemas Inc., as a result, opted out of showing the movie, citing concerns for audience safety.

The Department of Homeland Security said the #GOP’s threats lacked credibility. Due to concerns over box office sales across the industry, theater operators encouraged Sony to delay the opening. After Sony declined, the theaters announced they wouldn’t show *The Interview* until the FBI completed its investigation. (Appendix E shows the effects of this decision on the company’s stock price.) Shortly after this announcement, Sony Pictures decided to cancel its planned release of *The Interview*, a last-minute decision unprecedented in the modern motion picture industry. Entertainment industry sources estimated that damage to the studio and losses incurred from shelving the release would top at least $100 million. As of Thursday, December 18th, Sony had no plans to release the film in any capacity.

**Discussion Questions**

1. How can Sony employ communication strategies to defend its public reputation and improve employee morale?

2. What options are available to Sony to minimize revenue loss on *The Interview*?

3. Is Sony to blame for the cyberattack in the first place? Should the company take the blame?

4. If you were Sony Pictures CEO Michael Lynton, what actions, if any, would you have taken when you first heard about the security breach?

**Appendix A**
## Appendix B

<table>
<thead>
<tr>
<th>Studio</th>
<th>Gross 2014</th>
<th>Gross 2013</th>
<th>Gross Diff</th>
<th>Perc Diff</th>
<th># Movies 2014</th>
<th># Movies 2013</th>
<th># Movies Diff</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>20th Century Fox</strong></td>
<td>$1,790,494,060</td>
<td>$1,064,152,578</td>
<td>+$726,341,482</td>
<td><strong>+68.3%</strong></td>
<td>22</td>
<td>19</td>
<td>+3</td>
</tr>
<tr>
<td><strong>Fox Searchlight</strong></td>
<td>$147,847,784</td>
<td>$114,778,375</td>
<td>+$33,069,409</td>
<td><strong>+28.8%</strong></td>
<td>11</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td><strong>Focus Features</strong></td>
<td>$125,962,060</td>
<td>$101,035,755</td>
<td>+$24,926,305</td>
<td><strong>+24.7%</strong></td>
<td>12</td>
<td>10</td>
<td>+2</td>
</tr>
<tr>
<td><strong>Sony / Columbia</strong></td>
<td>$1,261,543,618</td>
<td>$1,144,579,720</td>
<td>+$116,963,898</td>
<td><strong>+10.2%</strong></td>
<td>22</td>
<td>20</td>
<td>+2</td>
</tr>
<tr>
<td><strong>Open Road Films</strong></td>
<td>$162,652,485</td>
<td>$148,222,661</td>
<td>+$14,429,824</td>
<td><strong>+9.7%</strong></td>
<td>9</td>
<td>8</td>
<td>+1</td>
</tr>
<tr>
<td><strong>Paramount</strong></td>
<td>$1,052,874,509</td>
<td>$966,871,171</td>
<td>+$86,003,338</td>
<td><strong>+8.9%</strong></td>
<td>18</td>
<td>16</td>
<td>+2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Distributor</th>
<th>Market Share</th>
<th>Total Gross*</th>
<th>Movies Tracked</th>
<th>2014 Movies**</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>20th Century Fox</strong></td>
<td>17.3%</td>
<td>$1,790.5</td>
<td>22</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>Buena Vista</td>
<td>15.6%</td>
<td>$1,617.5</td>
<td>17</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>Warner Bros.</td>
<td>15.1%</td>
<td>$1,562.4</td>
<td>31</td>
<td>22</td>
</tr>
<tr>
<td>4</td>
<td>Sony / Columbia</td>
<td>12.2%</td>
<td>$1,261.5</td>
<td>22</td>
<td>19</td>
</tr>
<tr>
<td>5</td>
<td>Universal</td>
<td>10.8%</td>
<td>$1,115.3</td>
<td>18</td>
<td>14</td>
</tr>
<tr>
<td>6</td>
<td>Paramount</td>
<td>10.2%</td>
<td>$1,052.9</td>
<td>18</td>
<td>14</td>
</tr>
</tbody>
</table>
Appendix C
Internal Memo

On the evening of December 2, 2014, sources reported that Sony CEO Michael Lynton and Co-Chairman Amy Pascal at Sony sent an internal memo to 6,500 current employees that confirmed that a “large amount of confidential Sony Pictures Entertainment data has been stolen by the cyberattackers, including personnel information,” stated that “the privacy and security of our employees are of real concern to us,” warned that “we are not yet sure of the full scope of information that the attackers have or might release” and “unfortunately have to ask you to assume that information about you in the possession of the company might be in their possession,” and promised employees that they would receive an email on December 3, 2014 that outlined steps to sign up for identity protection services.
Appendix E
References


38 Ibid.
