2014 Sony Pictures Entertainment Cyber Attack: A Case Study

INTRODUCTION

On November 24, 2014, a hacker group identifying itself as "Guardians of Peace" leaked a release of confidential data from the film studio Sony Pictures Entertainment (SPE). The data included personal information about Sony Pictures employees and their families, emails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, plans for future Sony films, scripts for certain films, and other information The perpetrators then employed a variant of the Shamoon wiper malware to erase Sony's computer infrastructure

During the hack, the group demanded that Sony withdraw its then-upcoming film *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-un, and threatened terrorist attacks at cinemas screening the film. After many major U.S. theater chains opted not to screen *The Interview* in response to these threats, Sony chose to cancel the film's formal premiere and mainstream release, opting to skip directly to a downloadable digital release followed by a limited theatrical release the next day.

United States intelligence officials, after evaluating the software, techniques, and network sources used in the hack, concluded that the attack was sponsored by the government of North Korea, which has since denied all responsibility

THE SONY PICTURES CYBER ATTACK

On the day of the attack (November 24th, 2014) there were just weeks before the release of the Seth Rogen and James Franco comedy, The Interview. Financed and developed by Sony, the film is a fictionalized attempt on Kim Jong Un's life, and portrays the dear leader as an unstable and slightly buffoonish maniac. The project was always considered potentially sensitive, and prior to Sony's greenlight had been passed on by other studios- fear of a possible North Korean reprisal hung around the project, and given North Korea's previous abductions of famous Japanese filmmakers and international assassinations, they weren't completely unfounded. Yet surprisingly it's Sony pictures- a Japanese owned company, and one of North Korea's most hated international rivals- who greenlighted the film and helped develop it.

That morning Sony employees showed up to work much like normal only to find themselves locked out of their computer network by a screen filled with a glowing red skeleton and the following message: **“Hacked by #GOP”.**
The screen cryptically stated Sony had already been warned, and that “this is just the beginning.” The hackers also claimed to have obtained all their internal data including “your secrets and top secrets”, then a final warning that if they don't obey, they'll release the data to the world.

A deadline offered by the hackers- 11:00 pm that same day- was ignored, which led directly to a massive dump of internal documents, unreleased films, and very embarrassing emails.

Components of the attack included a **listening implant, backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool**.

NORTH KOREA

A few days after the breach initially took place, sources told *Re/code* that Sony was worried North Korea was behind the attack. Why North Korea, though? Well, the timing coincides with the release of *The Interview*, an upcoming comedy about two journalists who attempt to assassinate the Supreme Leader of North Korea, Kim Jong Un. Strangely enough, back in August, *The Hollywood Reporter* wrote that the studio was digitally altering the film, as it looked to keep it from "igniting a tinderbox." The tweaks, which were "precipitated by clearance issues," included the deletion of a scene in which Kim's face was melted. Meanwhile, the stars of *The Interview*, Seth Rogen and James Franco, have put a humorous spin on the matter by releasing a number of racy pictures from the set -- in typical Rogen/Franco fashion.

North Korea, for its part, denied having a role in any of this, referring to the allegations as nothing more than a "wild rumor." However, state news outlet KCNA did express that the cyberattack on Sony could be a "righteous deed" from "supporters and sympathizers" of the country. No, North Korea won't take the blame for the harmful actions on Sony Pictures, but it is very, very happy that someone did -- especially after being extremely outspoken about its opposition to the release of *The Interview*.

"Stop the terrorist film!" the attackers wrote in a message recently posted to GitHub.

Accusations against North Korea

There's a fair amount of circumstantial evidence linking the North Korean regime to the attacks. But the best evidence that Pyongyang is responsible may not be publicly available — it's reportedly in the hands of the National Security Agency.

North Korea's anger over *The Interview* gives North Korea a clear motive for the attacks. This summer, it vowed a "resolute and merciless" response if the film was released as planned, though it frequently issues such threats with little consequence.

There's also circumstantial evidence linking the attacks to the North Koreans. Some of the malware used in the attack seems to have been written in Korean. The attacks also use tactics similar to those used against targets in South Korea in 2013 and Saudi Arabia in 2012.

On December 19, the FBI announced that it "has enough information to conclude that the North Korean government is responsible for these actions." But security experts were unimpressed with the information the FBI released publicly.

In January, the New York Times reported, based on information from anonymous sources, that the National Security Agency has been monitoring North Korean networks for years. According to these sources, the NSA was able to directly observe North Korea's hacking activities and confirm that they were responsible for the Sony attacks.

Of course, releasing the full details of this evidence could compromise the NSA's access to North Korea's network. To some extent, Americans are forced to take the NSA's word for it (or not) that North Korea is responsible.

Information obtained by the hackers

According to a notice letter dated December 8, 2014, from SPE to its employees, SPE learned on December 1, 2014, that personally identifiable information about employees and their dependents may have been obtained by unauthorized individuals as a result of a "brazen cyber-attack", including names, addresses, Social Security numbers and financial information. On December 7, 2014, C-SPAN reported that the hackers stole 47,000 unique Social Security numbers from the SPE computer network

Although personal data may have been stolen, early news reports focused mainly on celebrity gossip and embarrassing details about Hollywood and film industry business affairs gleaned by the media from electronic files, including private email messages. Among the information revealed in the emails was that Sony CEO Kazuo Hirai pressured Sony Pictures co-chairwoman Amy Pascal to "soften" the assassination scene in *The Interview* Many details relating to the actions of the Sony Pictures executives, including Pascal and Michael Lynton, were also released, in a manner that appeared to be intended to spur distrust between these executives and other employees of Sony

Other emails released in the hack showed Pascal and Scott Rudin, a film and theatrical producer, discussing Angelina Jolie. In the emails, Rudin referred to Jolie as "a minimally talented spoiled brat" because Jolie wanted David Fincher to direct her film *Cleopatra*, which Rudin felt would interfere with Fincher directing a planned film about Steve Jobs. Pascal and Rudin were also noted to have had an email exchange about Pascal's upcoming encounter with Barack Obama that included characterizations described as racist, which led to Pascal's resignation from Sony. The two had suggested they should mention films about African-Americans upon meeting the president, such as *Django Unchained*, *12 Years a Slave* and *The Butler*, all of which depict slavery in the United States or the pre-civil rights era.Pascal and Rudin later apologized. Details of lobbying efforts by politician Mike Moore on behalf of the Digital Citizens Alliance and FairSearch against Google were also revealed.

The leak revealed multiple details of behind-the-scenes politics on Columbia Pictures' current *Spider-Man* film series, including emails between Pascal and others to various heads of Marvel Studios. Due to the outcry from fans, the Spider-Man license was eventually negotiated to be shared between both studios. In addition to the emails, a copy of the screenplay for the *James Bond* film *Spectre*, released in 2015, was obtained. Several future Sony Pictures films, including *Annie*, *Mr. Turner*, *Still Alice* and *To Write Love on Her Arms*, were also leaked. The hackers intended to release additional information on December 25, 2014, which coincided with the release date of *The Interview* in the United States.

Conclusion

This can happen to any organization big or small. The hacker community is skilled and well-funded. Organizations need to use a multi-layered defense-in-depth approach to protect their territory by adopting strong security practices that weave policies, people, regulations, and technology. Some of these include – educating the employees about security best practices – using strong passwords and changing them per company policy, using technologies like firewall and VPN, performing periodic risk assessments to understand one’s security posture – which controls are effective and which are failing. Performing a penetration test is important to see where you are vulnerable. Continuously monitoring and responding to the alerts will help you be ready to prevent, detect, and respond in a timely manner.

To conclude the cost of repairing after a security incident is 10 to 100 times higher than preventing it in the first place. Deploy the Defense-in-depth approach. Prevention, Detection and Response is the key.