School of International and Public Affairs
Case Consortium @ Columbia
Columbia University

SIPA-21-0023.1

The Hacking of Sony Pictures:
A Columbia University Case Study

Executive Summary

In 2014, Sony Pictures suffered a devastating and highly publicized cyberattack related to its planned release of the controversial film *The Interview*, which intelligence reports later attributed to a nation-state attacker. As employees were locked out of thousands of company computers and hundreds of servers, their systems' memory was wiped clean while sensitive personal information and valuable corporate assets were stolen and eventually released online. In time, questions concerning the adequacy of Sony's cybersecurity program became a prominent topic for cybersecurity experts as well as business leaders, as its IT decisions left the company and its stakeholders vulnerable.

This Columbia University case study explores this landmark attack, which underlined the importance of a well-coordinated cyber crisis management and public relations response following a cyber attack as much it reaffirmed the need for strong information security programs and investments prior to its occurrence. This case also highlights the growing variety of cyberthreats major companies face as they become increasingly viable targets of state-sponsored hackers.

The case includes the following elements;

a) Video Intro and Discussions – Available Online

b) Written Case Study (This Document)

c) Annex A – Original Documents

This case was written by Sean Steinberg, Adam Stepan and Kyle Neary for the Picker Center Digital Education Group at Columbia's School of International and Public Affairs (SIPA). The faculty sponsors are Greg Rattray and Jason Healey.

Sony: Background

In 2014, Sony Corporation was a tech and media giant with over 130,000 employees and nearly $70 billion in annual revenue.[1] Between its electronics, media, gaming, music, mobile, and other divisions, Sony had grown from its founder's preceding radio repair business – a small, post-war shop set up in Japan in 1946 – into a dominant player in the global consumer electronics market, and Japan's 21st largest company in 2014.[2] Yet despite its media and technology expertise, the global corporation had earned a reputation within the hacking community for poor information security. Denizens of online message boards even coined a term coined at the company's expense: "Sownage," which loosely translates to an act of defeat – getting 'owned' in Internet parlance – comparable to Sony's own cyber humiliations. [3]

In 2011 alone – the same year the company declared its infamous "War on Hackers" – Sony's various divisions saw their networks breached more than 20 times. This trend began after Sony sued 20-year-old George Hotz, the first to devise code to "crack" Sony's flagship PlayStation 3 gaming console, as part of its campaign against hackers,.[4] As Hotz's story gained traction in the media, Sony fell into the crosshairs of Anonymous, a decentralized "hacktivist" collective, which inflicted on PlayStation one of the most high-profile breaches of a year-long hacking blitzkrieg against Sony. Company websites crashed under distributed denial of service (DdoS) attacks, which overwhelmed the sites with traffic; PlayStation's online gaming hub was taken offline for weeks; and personally identifiable information belonging to over 75 million PlayStation users were stolen from Sony's servers, along with 10 million customers' credit card information. This single breach alone carried a price tag of $171 million for Sony. Although company executives defended the quality of the company's cyber defenses while trying to paint themselves as victims of a "highly sophisticated attack," they failed to elicit pity from British regulators, who added to Sony's injury additional fines for failing to secure the sensitive data of its customers.[5]

The weaponization of lawsuits in Sony's "war" represented a legal escalation of its controversial anti-piracy efforts during the decade prior. In 2005, it was reported that Sony's music division had embedded hidden software – which some critics decried as malware – onto some 20 million CDs purchased by unwitting consumers. This "rootkit" software scanned customers' computer systems for illegal downloads of the company's intellectual property, prevented users from copying CDs, and even reported on their listening habits. As an unintentional side effect, it also created vulnerabilities' in the user's system that could later be exploited by unrelated malware.

Besides the toll on the company's public image, this scandal generated boycotts of Sony products, class-action lawsuits and lawsuits by states attorneys general, as well as charges by the U.S. Federal Trade Commission. As news coverage around the scandal grew, so did Sony customers' vulnerability as third-party attackers discovered the tool and repurposed it to conceal their own programs.. In the weeks following the initial reports, anti-virus firms discovered a new virus known as "Stinx" spreading across

[1] Hill, J.J. "Form 20F for the Fiscal Year Ended March 31, 2015." Sony Corporation. Jun. 23, 2015.

[2] Murphy, A., Tucker, H., Coyne, M., Touryalai, H. "GLOBAL 2000: The World's Largest Public Companies." *Forbes.* 2014.

[3] Elkind, P. "Sony Pictures: Inside the Hack of the Century." *Fortune*. Jun. 25, 2015.

[3] Murphy, A., Tucker, H., Coyne, M., Touryalai, H. "GLOBAL 2000: The World's Largest Public Companies." *Forbes.* 2014.

[4] Kushner, D. "Machine Politics." *The New Yorker*. Apr. 30, 2012.

[5] Elkind.

the Internet, infecting computers and using them to send spam emails en-masse, [6] while less malevolent hackers used the rootkit to hide rule-breaking software exploits from an anti-cheating program installed in the popular video game World of Warcraft.[7]

All of this led Sony Corporation in 2011 to hire a former senior U.S. Homeland Security cyber leader, Philip Reitinger, as its first-ever "global chief security information officer." However, by the time he stepped down three years later, few substantive changes had been made to the corporation's lax IT practices, according to many experts. Some attributed Reitinger's resignation to his frustrations with corporate decisionmakers in Tokyo, who appeared unreceptive to his proposals for a more centralized cyber security program with tighter controls in business units.[8]

The company's film and TV division, Sony Pictures Entertainment, appeared no more receptive to these changes than its parent. While auditors had warned the company's executive director of information security, Jason Spaltro, of these risks in 2005, Spaltro said he preferred to protect the company's bottom line by focusing investments on "the most important" security protocols "that are absolutely required by law." Suggesting the costs of patching the holes outweighed the risks posed by their exploitation, Spaltro said in a 2007 interview that he would "not invest $10 million to avoid a possible $1 million loss."[9] Years later, the same issues persisted. In 2014, months before the North Korean attack, a PricewaterhouseCoopers audit commented on the weak internal security of the studio network, and found a firewall and 100 computers being monitored by studio employees rather than the corporate security team.[10]

The Interview: The Match in Sony's Tinderbox

In 2014, Sony Pictures was losing the race against its competition after reigning supreme for years atop the box office throne. After its two most-hyped films of the summer flopped in 2013, the studio found itself hounded within the industry for its poor performance, and Sony Pictures' executives feared they were slipping out of the good graces of their Japanese parent company, which had long taken a hands-off approach to the California-based subsidiary.

Despite remaining one of Sony Corp's few profitable divisions, Sony Pictures soon found itself under siege by an activist investor who wanted to spin off some of its assets, claiming the studio was "famously bloated" and "poorly managed." Desperate to fend off the attack, Sony Pictures' CEO Michael Lynton made a public pledge of fiscal responsibility and promised to generate positive revenue, declaring that "no cost is too sacred to cut." Meanwhile, Sony's studio chief Amy Pascal sought a redeeming box office hit after the industry press held her personally liable for the company's slump.

[6] Roush, W. "Three Arrested in Sony Rootkit Virus Case." *MIT Technology Review*. Jun. 27, 2006.

[7] Lemos, R. "World of Warcraft hackers using Sony BMG rootkit." *SecurityFocus*. Nov. 3, 2005.

[8] Elkind.

[9] Holmes, A. "Your Guide To Good-Enough Compliance." *CIO*. Apr. 6, 2007.

[10] Chmielewski, D., Hesseldahl, A. "Sony Pictures Knew of Gaps in Computer Network Before Hack Attack." *Re/code*. Dec. 12, 2014.

Pascal turned to comedy writer/actor/director Seth Rogen, a reliable revenue source who'd brought the company critical and box office success in the past. Since 2013, Sony Pictures had been working with Rogen to produce *The Interview*. The comedy film starred James Franco and Rogen as a talk show host/ producer duo recruited to assassinate North Korea's real-life leader, Kim Jong-Un, under the pretense of a TV interview. Complemented by the star appeal and box office track record of its leads, the film's controversial subject was sure to generate publicity. But Sony was not prepared for its reception on the international stage.

In June 2014, days after the film's first trailer was released, the North Korean government released a statement threatening "a merciless counter-measure" for the film, which it deemed not only offensive, but "the most blatant act of terrorism and war."[11] While many dismissed the North Koreans' inflammatory comments as empty threats, Sony Corp's CEO, Kazuo Hirai, expressed concern to Lynton that releasing the film in its current state would further sour relations between Japan and North Korea. Hirai had good cause for concern: the nuclear-armed nation-state was infamously thin-skinned when it came to reputational challenges, was not shy about making threats (nuclear or otherwise), and had just been blamed for directing cyber attacks against South Korean banks and broadcasters the year prior, causing $700 million in damages.[12] The question Sony executives faced was whether it was worth calling North Korea's bluff.

On one hand, by cancelling the release, the studio faced a $75 million hit to its bottom line,[13] and risked burning a bridge with an important collaborator in Rogen. On the other, even though past threats by the regime often turned out to be bluffs, the consequences could be catastrophic if the threats were carried out. Ultimately, Sony Pictures settled for toning down some of the film's more offensive elements in the editing room, such as reducing the amount of gore in Kim's death scene. Yet even that half-measure fueled heated exchanges between Rogen and Pascal, as the comedian felt betrayed by the studio's capitulation to the dictator his film meant to satirize. Meanwhile, Sony Corporation scrambled to distance itself from the toxic product, removing its logo from marketing for the film, taking the trailer down from YouTube, removing its promotional materials from company sites, and pulling the plug on the film's theatrical release in Asia.[14]

What Sony Pictures did not do, however, was improve upon the weak points of its cybersecurity in anticipation of a possible cyber attack retaliation by a nation-state. While such a response may have seemed unprecedented for a private company, let alone a film studio whose only crime was producing a raunchy comedy, at least one North Korea expert at the Rand Corporation consulted by Lynton claimed to have alerted him to this risk. Lynton denied having any prior awareness of the threat.[15]

The Attack: Infiltration and Reconnaissance

Outdated information security practices, combined with employees' poor digital hygiene, made Sony particularly vulnerable to the tactics the North Koreans would later reportedly use to compromise its networks. For instance, the company failed to implement a basic, industry-standard security practice known as two-factor authentication which requires users to verify their identities by entering a unique

[11] Reuters staff. "North Korea slams U.S. movie on leader assassination plot." *Reuters*. Jun. 25, 2014.
[12] Elkind.
[13] Lang, B. "Sony Could Lose $75 Million on 'The Interview.'" *Variety*. Dec. 18, 2014.
[14] "Sony on shelving 'The Interview': 'We had no choice.'" *AP News*. Dec. 19, 2014.
[15] Elkind.

numerical code sent to their mobile device or digital keychain. Passwords belonging to Sony employees frequently were not comprised of randomized sequences of numbers and letters, but rather based on personal information, making them both easier for employees to memorize and for attackers to surmise.[16] Emails were also stored unencrypted on Sony's servers for up to seven years, providing a wealth of information for those who could infiltrate the servers.

With Sony still set to push forward its theatrical release plans – albeit on a more limited scale – the attackers made their first moves, compromising the company's internal networks as early as September, according to the FBI. Attackers broke through the network's security perimeter using a common tactic known as "spearphishing": Sony employees – including Lynton – received emails containing false Apple ID verification links which directed them to a fake Apple sign-in page, unaware they were being manipulated by the attackers to hand over their Apple account passwords.[17] With these passwords in hand, the attackers simply had to test them against the employees' Sony network accounts until they found a match.

Eventually, the attackers are believed to have obtained the credentials of a "top-level information technology employee."[18] U.S. intelligence agencies have claimed these credentials were not acquired through willing insider assistance, as was done in the Snowden leaks, though they have never revealed their alleged proof to the public, possibly out of fear that doing so would compromise U.S. cyber-operations against North Korea which may have generated the evidence. In either case, the acquisition of top-tier credentials granted the attackers unhindered access to the entire Sony network, in part because Sony eschewed the practice of data segmentation, instead storing many types of data on the same servers regardless of sensitivity.

Because the company's antivirus program only recognized previously deployed malware registered in its system, the attackers avoided detection by modifying the code used to infected Sony's systems. Moving laterally undetected across the network undetected, the attackers scouted it out to identify valuable information before exfiltrating the data to attacker-controlled servers. By restraining the bit-rates of these uploads, these transfers went undetected for months among Sony's legitimate digital media transfers until they held terabytes of company data in their possession.

The Attack: The Hackers Go Public

On the morning of November 24, 2014, the attackers finally made their presence known. About a month before *The Interview*'s planned Christmas release, Sony Pictures' employees received a chilling morning welcome as they logged onto their corporate network: sounds of gunfire erupted from their computer speakers as a macabre red skeleton hovered over Photoshopped images of Lynton's and Pascal's severed heads on their monitors. Proclaiming that the network was under attack, a line of vague-but-threatening text read: "If you don't obey us, we'll release your data shown below to the world." (see Annex A-2). The message also praised "God'sApstls," a pseudonym that had appeared several days earlier in an email sent to Lynton, Pascal, and others demanding "monetary compensation" for "great damage by Sony Pictures."

[16] Ibid.

[17] Bisson, D. "Sony Hackers Used Phishing Emails to Breach Company Networks." *The State of Security*. Apr. 22, 2015.

[18] Brown, P., Sciutto, J., Perez, E., Acosta, J., Bradner, E. "Investigators think hackers stole Sony passwords." *CNN Politics*. Dec. 19, 2014.

But without any specific references to *The Interview*, or any obvious order to "obey," it was not immediately clear what had motivated the attack.

Meanwhile, malware leapt from one Sony system to the next, ignoring continental divides as it erased every byte of data on nearly half of the 6,800 personal computers and more than half of the 1,555 servers comprising the studio's global network. The malware also "bricked" infected systems, frying them so deeply that they could not even initiate their start-up sequences. Within an hour, Sony was thrown "back into the era of Betamax," fax machines, Post-It notes, and paper checks.[19] The company faced operational challenges in its day-to-day business as its systems were taken offline, either disabled by the attack or preventatively shut down by Sony IT to contain the spread of the virus. Employees would not regain access to company machines for at least a week, and Sony Pictures spent over two months rebuilding the national network for Sony Pictures.[20, 21] Recovering compromised data would be impossible or prohibitively expensive, but in time the data loss would be dwarfed by a surprisingly personal public relations crisis.

Leaks, Threats of Violence & Fallout

In the weeks that followed the network meltdown, stolen Sony files ranging from valuable intellectual property to extremely sensitive personal information was dumped onto public-facing filesharing websites where anybody with an internet connection could view and download them. Proprietary properties like films and scripts were widely pirated almost as quickly as they were leaked. *Fury* – a World War 2 action/drama starring Brad Pitt which was still playing in theaters at the time – was downloaded over 1.2 million times in a mere four days, while the movie *Annie* was leaked before it had even been released. Both leaks cost Sony an unknown amount of forgone revenue in lost ticket sales.[22, 23] Additionally, employees' compensation information, performance evaluations, criminal background checks, company disciplinary histories, and even medical data suddenly became public record. Many also faced the risk of identity theft after 47 thousand Social Security Numbers belonging to former and current employees were released by the attackers.

As news outlets honed in on the unsavory and embarrassing revelations of leaked emails belonging to Sony executives, the reputations of the organization and its leadership were dragged through the court of public opinion. The world became privy to Sony's office politics, executives' gripes with Hollywood A-listers, and even an email spying operation an executive launched against Sony's own employees. But perhaps nobody bore the brunt of the scrutiny more than Pascal. One particular email which stood out during coverage showed Pascal joking with a producer that then-President Barack Obama would be most interested in black films such as *Django Unchained* or *Twelve Years a Slave* while she was discussing an upcoming fundraiser

[19] Elkind.

[20] Cunningham, T., Waxman, S. "Sony Struggles to Fight #GOP Hackers Who Claim Stolen Data Includes Stars' IDs, Budget and Contract Figures." *The Wrap*. Dec. 16, 2014.

[21] "A Breakdown and Analysis of the December, 2014 Sony Hack." Risk Based Security, Dec. 5, 2014.

[22] Wallenstein, A., Lang, B. "Sony's New Movies Leak Online Following Hack Attack." *Variety*. Nov. 29, 2014.

[23] Miller, D., Hamedy, S. "Cyberattack could cost Sony Pictures tens of millions of dollars." *Los Angeles Times*. Dec. 5, 2014.

for the politician.[24] Her public humiliation, combined with the studio's anemic performance under her leadership during the preceding two years, likely contributed to her resignation as studio chief.

The leaks also publicly undermined Sony leadership's professed commitment to the film's bold premise, the creative integrity of the filmmakers, and to free speech principles more broadly, as emails sent as recently as two days prior to the system meltdown revealed attempts to appease the Kim regime by making the film less offensive. This in turn spawned a deeper, national conversation over the role and responsibility Sony and other private actors ought to assume in protecting and restricting free speech within the U.S., especially at the behest of a foreign, authoritarian government .

On December 16th, the risk escalated out of cyberspace and into the physical world when a message appeared online threatening moviegoers who attended screenings of the film with a "bitter fate," drawing direct parallels to the 9/11 terror attacks.[25] Major American theater chains, skittish after a mass shooting of moviegoers in Colorado two years prior, pulled out of their arrangements to screen the film. With their most financially promising distributors out of play, Sony announced that it would cancel the film's planned Christmas release, for which it was once again publicly critiqued over its perceived lack of commitment to free speech.

Though North Korea's link to the attack was reported in the media days after Sony's machines were knocked out, the attack was formally attributed to North Korea by the FBI on December 19. This marked the first time the U.S. had ever directly attributed a particular cyber attack to a nation-state. President Obama promised the same day to "respond proportionally" and expressed disappointment in Sony's decision to shelve the film.[26] Facing public and commercial pressure to release the film, Sony Pictures reneged on its decision once more shortly before Christmas Day and announced it would screen the film in a few hundred arthouse theaters alongside a simultaneous Christmas Day digital release on Google and Microsoft's streaming platforms.

While *The Interview* managed to recoup its production budget, the studio lost millions in marketing costs, not to mention the costs of recovering its compromised network and settling class-action lawsuits with employees whose information it failed to secure.

Recovery

Given the amount of time the attackers had spent exploiting the network, Sony's IT team was concerned over how deeply ingrained their attack tools may have been in its backups, and feared other backdoor access might be present.[27] To ensure no malicious remnants of the infected network were able to compromise its new set up, the team spent months poring over the old backups before copying anything

[24] Rushe, D. "Amy Pascal steps down from Sony Pictures in wake of damaging email hack." *The Guardian*. Feb. 5, 2015.

[25] Peterson, A. "Sony Pictures hackers invoke 9/11 while threatening theaters that show 'The Interview.'" *The Washington Post*. Dec. 16, 2014.

[26] By Holland, S., Spetalnick, M. "Obama vows U.S. response to North Korea over Sony cyber attack."

[27] Peterson, A. "Why it's so hard to calculate the cost of the Sony Pictures hack." *The Washington Post*. Dec. 5, 2014.

onto its new network.[28] By Sony's own estimates, the company lost $35 million "in investigation and remediation costs" following the attack," a figure which the company said was "primarily" aimed at "restoring [its] financial and IT systems.[29] Beyond that, however, the company almost certainly suffered additional losses due to business disruptions imposed by the loss of its network capabilities.

Sony Pictures took additional steps to improve its cyber defenses, some of which it has been argued were long overdue. For instance, the company adjusted its data storage practices so that, rather than storing all data on its main network, Sony would instead only retain information in current-use for projects on its network. The rest was to be encrypted and stored in separate, siloed servers which were kept offline. By doing this, the company hoped to prevent would-be attackers relying on tactics similar to those used in 2014 from accessing their files. In addition, by downgrading administrators' privileges and making their network presence less ubiquitous, attackers who managed to obtain their credentials would no longer have an all-purpose skeleton key to Sony's network. Further, the company reduced the length of time that emails could be archived to a matter of weeks from its previous seven-year limit, which allowed employees to use their inboxes as de-facto digital storage units.

Sony IT also restricted Internet access to employees' endpoints in the network, directly impacting their ability to do their jobs, until the company had rebuilt a more secure network. They then switched the studio firewall to its most restrictive setting and enacted greater controls on employees' ability to install new programs on their systems, reducing future attackers' prospects for gaining a foothold on company systems. Finally, Sony Pictures began to monitor for irregular login patterns that could indicate unauthorized access. Given the number of separate accounts used by attackers to steal files, Sony might have detected the 2014 intrusion had such detection protocols been in place.[30]

Summary

Its political motivations, as well as its implications for freedom of expression, make the 2014 Sony Pictures hack unique among cyber attacks on private sector actors of the time. Unlike the typical assailants of corporate networks, those credited with the 2014 attack appeared to be motivated not by the profits of intellectual property or credit card theft, but by political retaliation and deterrence. This prompted the attackers to retrieve personal data belonging to employees that may not have been particularly valuable to a dark web buyer, but could be used to humiliate, discredit, and threaten individuals within the target organization.

The personal-level of this targeted information campaign, and the resulting fallout suffered by individual victims, appears to have been eye-opening for the C-suite community, especially for those working in industries that did not grant high priority to cybersecurity previously. The attack's aggressive nature, which saw not only data theft but also the destruction of data and hardware, also helped set it apart from financially-motivated cybercrimes. All of these factors go to show that as businesses and geopolitics continue to collide in this 21st century cyber landscape, private companies must brace themselves to deal with threat actors boasting the resources and objectives of nation-states.

[28] Elkind.
[29] Hornyak, T. "Hack to cost Sony $35 million in IT repairs." *Network World*. Feb. 4, 2015.
[30] "The Sony Pictures Hack: Two Years Later." Harvard Business School Digital Initiative. Nov. 17, 2016.

As could be expected of any film studio in the mid-2010s, particularly one belonging to an electronics conglomerate, Sony Pictures had increasingly taken to digitizing its assets. As such, protecting its intellectual property increasingly demanded a more robust information security strategy, with a higher claim on budgetary and human resources. Sony, however, did not make these investments and downplayed the risks of an attack. Given the financial losses Sony incurred as a result of the 2014 attack – which we estimate may have topped $150 million – the heightened stakes of such attacks ought to be taken into account in justifying increased information security expenditures moving forward. The financial damages Sony might have prevented – which could affect any company facing similar digital risks – included legal fees and lawsuit settlement costs; foregone revenue from *The Interview's* botched release as well as the leaks and pirating of other Sony films; the costs of operational disruptions experienced during the network rebuild; and the direct costs of repairing the IT infrastructure damaged by the attack.

Sony Pictures might have reduced the damage it suffered, if not repelled the attack, through several technical and operational steps. To better inoculate itself against intrusion via phishing campaigns, Sony might have employed common password-protection best practices, such as prohibiting easy-to-surmise passwords like "sony12345," for accounts with network access, or requiring unique passwords for work devices which did not match those of employees' personal devices .[31] Nonetheless, the scale of Sony's losses should not be blamed on the initial breach of its network perimeter, as even the most even the most security-conscious organizations can fall prey to phishing. That being said, Sony's inability to detect and remove the intruders from the network in timely fashion gave the attackers months to steal data and destroy hardware.

Had studio executives operated under the assumption that their digital communications carried some degree of exposure risk, studio executives might have chosen not to share sensitive and/or embarrassing communications via email. In addition, implementing more judicious email storage practices, such as reducing the length of time that emails were allowed to remain in inboxes before being automatically archived, or discouraging the use of email for record-keeping and data storage, might have prevented the exposure of controversial remarks by Pascal and other executives, which brought the company and the individuals public rebuke. The company's decision not to encrypt sensitive and/or valuable data or store them on separate servers segmented from those accessible to the wider employee population also made this information more accessible to network intruders.

The Sony Pictures hack also exemplifies the importance for private companies to diligently monitor evolving cyberthreats. Despite several high-profile and costly attacks on its sister companies, Sony Pictures' executives apparently underweighted the risk that a costly cyber attack would occur against their own division. Had they deemed a North Korean retaliatory attack more likely following the government's threats – an oversight likely driven by the lack of precedence for nation-state cyber attacks against private actors – they may have generated greater buy-in to increase their cybersecurity investments, which could have mitigated the vulnerabilities which the company had been made aware of years prior to the attack.

Finally, the attack underlined the need for companies to anticipate high-profile digital breaches by pre-emptively crafting effective public relations strategies to deal with the fallout. In addition to the typical legal liability and negative publicity Sony faced for its security failures, the company and its personnel faced the consequences arising from weeks of sensitive, compromising information leaks. Meanwhile, Sony's inconsistent decisions with regard to its release of a politically-sensitive media product called into question its commitment to free speech values. This caused particular harm to the studio's public image in

[31] Risk Based Security.

the U.S. and its media industry, both of which are deeply intertwined with free speech values legally and ideologically.

Taken together, implementing improved these practices may have better ensured employee privacy, reduced the risk and scale of data theft and financial losses, sidestepped legal woes, and protected Sony Pictures from a tarnished public image.

ANNEX A: Original Documents

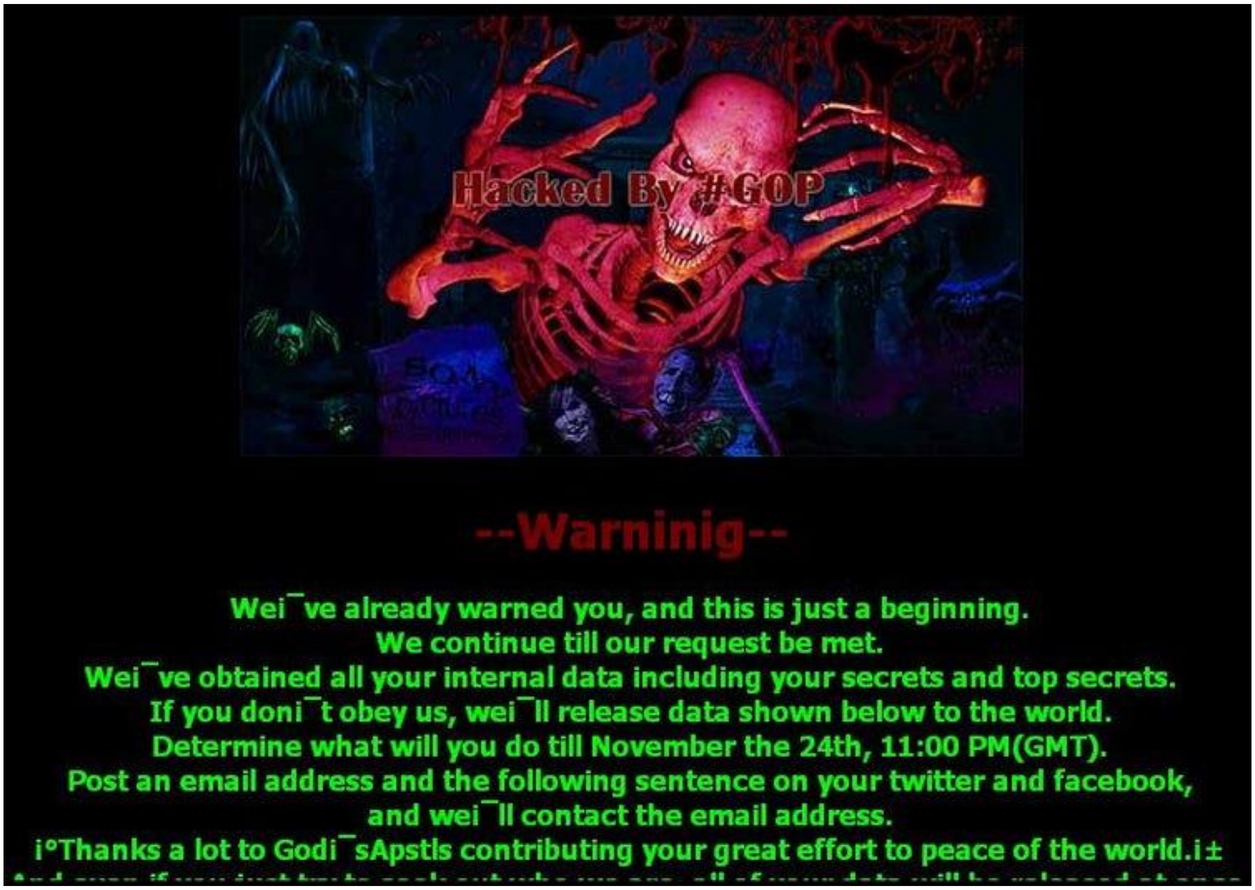
Annex A-1:	TABLE: Sony financial losses associated with hack
Annex A-2:	Message on affected Sony computers’ screens during attack
Annex A-3:	Promotional poster for *The Interview*
Annex A-4:	Warrant issued by F.B.I. for one of the alleged hackers

Annex A-1

Loss Type	Cost
Investigation + Remediation	$35 Million
Legal	$8 – 15 Million
Lost revenue (*The Interview)*	$30 Million
Additional film assets write-offs	$82 – 95 Million
Other (Reputational, etc.)	Unknown
Total	**$155 – 175 Million**

Annex A-2

The threatening screen that employees first saw when they tried accessing their computers. The message attributes responsibility to "GOP," or "Guardians of Peace," but similarities to an attack on South Korean banks suggest the attack was a North Korean operation. Available from Business Insider here.

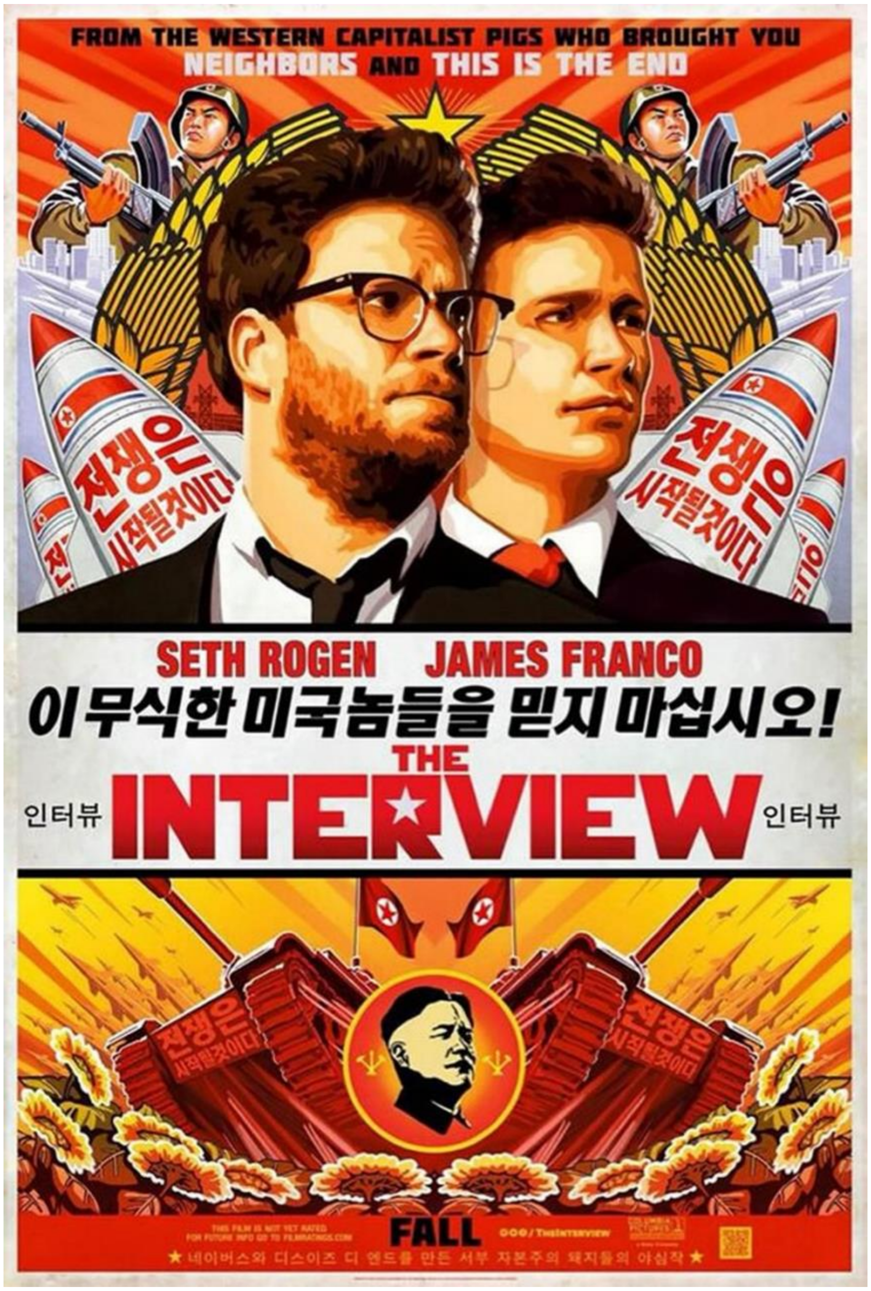


--Warninig--

Wei¯ve already warned you, and this is just a beginning.
We continue till our request be met.
Wei¯ve obtained all your internal data including your secrets and top secrets.
If you doni¯t obey us, wei¯ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook,
and wei¯ll contact the email address.
i°Thanks a lot to Godi¯sApstls contributing your great effort to peace of the world.i±

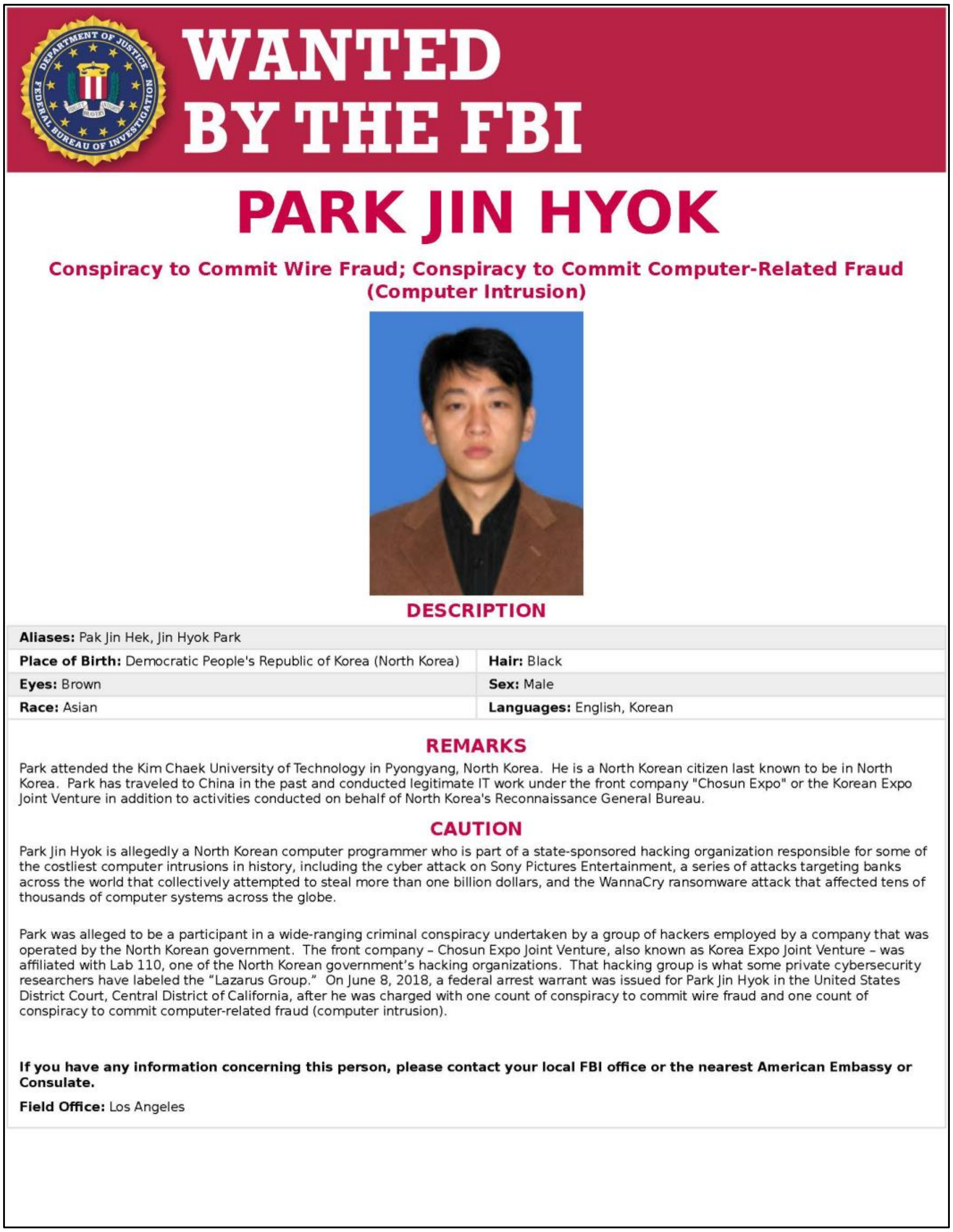
Annex A-3

A promotional poster for *The Interview* parodying the typical style of North Korean propaganda. The central text reads “Don’t trust these ignorant Americans!” in Korean. Available from the *Rolling Stone* here.


FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU
NEIGHBORS AND THIS IS THE END
전쟁은 시작될것이다
전쟁은 시작될것이다
SETH ROGEN
JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오!
THE
INTERVIEW
인터뷰
인터뷰
전쟁은 시작될것이다
전쟁은 시작될것이다
THIS FILM IS NOT YET RATED
FOR FUTURE INFO GO TO FILMRATINGS.COM
FALL
/TheInterview
COLUMBIA PICTURES
★ 네이버스와 디스이즈 디 엔드를 만든 서부 자본주의 돼지들의 야심작 ★

Annex A-4

The warrant issued by the F.B.I. for one of the alleged hackers. The warrant describes Park's association with the North Korean government through a company called Chosun Expo Joint Venture. Some cybersecurity experts, however, contend the U.S. government has overstated North Korea's role in the attack. Available from the Federal Bureau of Investigation here.



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company – Chosun Expo Joint Venture, also known as Korea Expo Joint Venture – was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles