The Hollywood Reporter

WORLD PREMIERE OF
THE INTERVIEW
#THEINTERVIEWMOV

Five Years Later, Who Really Hacked Sony?

by Tatiana Siegel

November 25, 2019, 6:00am PST

The massive cyberattack just before Thanksgiving 2014 crippled a studio, embarrassed executives and reshaped Hollywood. The FBI blamed a North Korea scheme to retaliate for the comedy 'The Interview,' but many whose lives were upended have doubts. Says Seth Rogen: "The fact that [co-director Evan Goldberg and I] were never really specifically targeted always raised suspicions in my head."

On Jan. 23, 2015, a manager at Sony Pictures Entertainment shot off an email to a group of 12 in the studio's distribution department that offered intel about an upcoming film from rival Disney. "Midwest exhibitors went into McFARLAND USA expecting a boring track & field movie but came away pleasantly surprised," the manager noted about the sports drama that had been screened the day before. It was a mundane missive: a Hollywood executive sizing up the competition.

What is extraordinary about the email is what sources say it reveals about the 2014 Sony Pictures hack — and the official FBI narrative that pins it on North Korea. The email was drafted nearly nine weeks *after* the now infamous cyberattack ostensibly had been contained. It was passed along to a U.S. cyber researcher in February 2015 by a Ukrainian hacker as alleged proof that his Russian associate had breached Sony and could still do so at will. Despite FBI director James Comey's "very high confidence" that Kim Jong Un was to blame, the Ukrainian source was maintaining that hackers were still accessing Sony's system — and they weren't North Korean.

Exactly five years have passed since the Sony hack, a seismic event that announced itself just before the Thanksgiving holiday on Nov. 24, 2014, when a menacing skeleton simultaneously popped up on thousands of Sony computer screens with the message: "We've obtained all your internal data including your secrets."

That was followed by 22 days of massive data dumps that exposed embarrassing executive email exchanges (like one between then-co-chairman Amy Pascal and producer Scott Rudin in which he refers to Angelina Jolie as "a minimally talented spoiled brat"), trade secrets (including overtures from Marvel to bring Sony-owned Spider-Man into its universe) and five upcoming full-length films (such as Brad Pitt's *Fury*). The breach, which former National Intelligence director James Clapper dubbed "the most serious cyberattack ever made against U.S. interests," rocked the industry and forever altered how studios think about cybersecurity and the global impact of their content. In the aftermath, nearly all of Sony's top management was swept out.

Although the FBI's North Korea attribution was swift (it took just 25 days) and has never wavered, many of those impacted still harbor questions about what exactly happened when a previously unknown hacker group named Guardians of Peace decimated Sony's computer infrastructure and brought one of the six major studios to its knees. *THR* spoke to more than two dozen insiders and executives who worked at Sony at the time, including some who still do, and more than half say they harbor doubts about the FBI's official narrative, which maintains that the hack was a response from North Korea because leader Kim Jong Un objected to his depiction in Seth Rogen's comedy *The Interview*.

Ed Araquel/Sony Pictures

A scene from Seth Rogen's 2014 comedy *The Interview*, which co-stars James Franco as a TV talking head recruited by the CIA to assassinate North Korean leader Kim Jong-un.

KCNA/AFP via Getty Images

North Korean leader Kim Jong-un

"I never believed it had anything to do with *The Interview*," says former Sony Pictures Television head Steve Mosko, who along with former CEO Michael Lynton and Pascal, witnessed his entire email account dumped into public view by GoP.

Mosko, now CEO of Village Roadshow, declined to say exactly why he is personally so skeptical of the FBI's account. But he's hardly alone. Rogen himself remains uncertain. For him, there was one glaring red flag in the North Korea narrative. In the wake of the breach, he hired a cyber risk team at the private investigative firm Kroll, Inc. to comb through all his devices and accounts as well as those of the film's co-director Evan Goldberg. Not only did they find no breaches, but they discovered that no hack attempts had been made. That offers a peculiar twist given that Rogen was by far the highest-profile person associated with the movie, which he starred in, directed, produced and co-wrote.

"I've got to say, the fact that we were never really specifically targeted always raised suspicions in my head," Rogen tells *THR*.

The FBI declined to comment, noting that the hack remains the subject of an active investigation. Meanwhile, North

Korea continues to deny any involvement in the attack, even as it proudly boasts each time it launches a ballistic missile into the sea.

Many, including Lynton, who left the studio in 2017 and now is chairman of Snap Inc., do accept the official explanation. "I believe the experts, and the experts told me it was North Korea. I have no reason to believe otherwise," he says. Through a studio spokesperson, Sony says, "We have no reason to suspect anything other than what the FBI concluded based on their investigation. The studio has moved on."

Still, alternate theories and conspiracies circulate widely among former and current executives. Some believe it was the work of Russian hackers hired by a Sony investor looking to profit from a post-hack stock collapse. Others speculate it was a disgruntled former employee who specifically targeted top executive brass. Perhaps the wildest rumor that still enjoys traction involves the wife of a former head of a rival studio, who is said to have helped her friend land a job at Sony sometime before the hack — and that friend turned out to be a Russian honeypot who gave hackers entry into the system.

If a Russia connection seems far-fetched, there's at least some reason to indulge a closer look. Max Popov, a Soviet-born hacker and former FBI informant, claimed in early 2015 that a Russian cyber associate gave him a cache of documents from Sony that were dated both before and after the hack, but were never released in the public dumps. (They included the *McFarland, USA* email referenced earlier.)

At the time, Popov sent the cache to Jeffrey Carr, a researcher and the author of *Inside Cyber Warfare: Mapping the Cyber Underworld* (Seattle-based Carr had been communicating online with Popov in Ukraine for years). Carr, who has provided intelligence briefings to the CIA and is the founder of the annual Suits & Spooks summit, passed along the emails and documents to the FBI in early 2015.

"I said, 'Look, before you jump on the North Korea bandwagon, I'm getting these documents from a Russian hacker who seems to have unlimited ability to pull more documents, even after Sony's network was down.' Literally after their network was in shambles, this guy was still able to send me documents," says Carr. As for the government's reaction, Carr notes: "The FBI doesn't give you a response. They say, 'Oh, thanks for sharing this information with us,' and that's the last you hear about it."

Former FBI agent E.J. Hilbert, who ran Popov as a source for years in the early aughts, says the hacker might very well have been telling the truth. "With any attack, and very likely with the Sony attack, they thought they had full containment, and they probably did not, and therefore information could have continued to have been extracted by the bad guys from various methodologies," says Hilbert, who now works in cybersecurity in the private sector. "It is very likely that Mr. Popov got his hands on it. He knows people."

Although Popov, who lived in the U.S. for two and a half years, was well connected in cybercrime circles, Hilbert says he knows of no instance in which he liaised with North Koreans. "With North Koreans, no. With Iranians and Russians, yes," he says.

Lynton says he was never made aware of any Russian hackers having access to Sony's then-crippled system. That point was echoed by a number of top executives who were in contact with law enforcement at the time. Adding further intrigue, one former executive recalls being bombarded with emails written in Cyrillic beginning in the summer of 2014.

It is, of course, very possible that Russian hackers never actually breached any Sony corporate accounts and instead these additional emails were stolen from employees' personal accounts (some staffers were using Gmail for work in the hack's aftermath). There also was at least one other break-in of the studio's system nine months before the infamous public hack in 2014. According to leaked emails, vp legal compliance Courtney Schaberg briefed general counsel Leah Weil about a breach in February of that year, noting that "credentials ... for an SPE system may have been obtained by an unauthorized party, who then may have uploaded malware." (The leaked emails show that Sony decided to keep that breach quiet.)

Popov isn't likely to step forward to clarify why he believes Russian contract hackers attacked Sony. Carr says Popov enlisted with the Ukrainian military and has since been deployed to the eastern front.

***

All GoP communications stopped Dec. 20, 2014, with a final missive that mocked the FBI: "The result of investigation by FBI is so excellent that you might have seen what we were doing with your own eyes. We congratulate you [sic] success. FBI is the BEST in the world."

In 2018, the U.S. Department of Justice finally laid out its 179-page criminal complaint, naming North Korea's Park Jin-hyok as the key player behind the attack. According to the document, the programmer also lived in China before the Sony breach, which FBI special agent Nathan Shields pinpoints as having happened in late September 2014, after the undisclosed February breach.

The idea of Russians idling in the system before and after the hack is never mentioned. The complaint concedes that "because of the harmful nature of the attack on SPE in which vast amounts of data were overwritten and computers were rendered unrecoverable, a complete reconstruction of the [hackers'] activities during the period of the intrusion was not possible through a forensic analysis."

North Korea maintains Park does not exist.

Naysayers remain unimpressed by the government's evidence. "The Sony attack was just so loud and so clownish," says Carr, who sees "weaknesses" in the attribution. "There was nothing sophisticated about it. It's not what you think about with a nation-state that has a military arm that does cyberattacks."

Former News Corp. chief security officer Hemanshu Nigam says there are major holes in the theory that North Korea carried out the hack as payback for *The Interview*. "North Korea would have needed someone on the ground — an almost impossible-to-imagine scenario that also contradicts the criminal complaint — in order to exfiltrate that much data, including at least five full-length movies, without anyone noticing at Sony," he says. "From day one, I didn't believe this had the hallmarks of a nation-state, and I still don't. Pointing the finger at an enemy is the easy way out."

Also, as many former and current executives note, GoP never attempted to retaliate further with additional leaks when *The Interview* was released in theaters (albeit at small art houses rather than cineplexes) on Christmas Day 2014 and on streaming platforms. North Korea skeptics find that odd, given that the group threatened 9/11-style attacks on movie theaters just days earlier.

(At the time, President Obama said the studio "made a mistake" when it pulled *The Interview* from theaters. "That statement from Obama was erroneous," says one former executive, noting that the studio was actively negotiating with smaller theaters to carry the movie at the time. "It was very difficult for people to hear that.")

Rogen finds the poorly worded GoP threat that invoked 9/11 to be off-key for a nation-state.

"That didn't seem like North Korea's M.O. That seemed more like young, amateurish hackers than like a foreign government launching a systematic attack on another country," he says, floating the possibility that someone used the North Korea narrative as cover. "What if it's someone started robbing a bank and someone else saw it was happening and decided they would jump in on it and weaponize it in a different way than it was meant to be weaponized? That's a conversation that we've had in trying to hypothesize what the fuck might've happened here."

While it's true that the crime itself was unsophisticated — a semi-competent hacker could have done it, given that servers had passwords like "sonypictures" — the rollout of the info indicated someone who understood showbiz players and practices well. Despite the hackers' broken English (which could have been intentional), the media acumen on display strikes some as exceeding that of the hermit kingdom. "They would have needed someone with exceptional insider tribal knowledge of Hollywood in order to know what would damage reputations. You can't google that," says Nigam, who was once a federal prosecutor of online crime and now has his own firm that advises Hollywood entities.

The hackers knew exactly which journalists to approach and seemed to anticipate the media's reaction. The rollout of leaks also appeared to be strategically planned, peaking with the release of Mosko's and Pascal's inboxes followed by the movie theater threat.

Some skeptics say that pushing back on the government's narrative came with a reputational cost. Marc Rogers, who is head of security at famed hacking conference Defcon and a consultant on *Mr. Robot*, says he took heat from the government for knocking down the Pyongyang angle and noting that North Korean proxy IP addresses don't necessarily translate into a smoking gun.

"At least one official described me as either an idiot or someone trying to sell something," he says. "I literally have no dog in the fight. But when people start making statements about things that I know to be factually questionable, I find it often difficult to keep my mouth shut, so that's why I piped up. My original statements weren't to say, 'No, the FBI is completely wrong.' It was to say, 'No, the evidence the FBI is pushing does not say what they're claiming it says.' "

In late December 2014, Kurt Stammberger, then senior vp at cybersecurity company Norse, was making the rounds of the news shows with findings from his firm's report that the attack was an inside job. "The thing that really lifted our eyebrows was, I was giving an interview on CNN, and [the anchor] says, 'I've talked to the FBI and the National Security director, and they say this report's a load of BS,' " Stammberger recalls. "I said, 'That's really interesting because we haven't even transmitted it to them yet.' They started basically trashing us before they had even seen the data."

Although the disgruntled-staffer angle generated headlines back in 2014, less explored is the prospect of someone using the hack as a weapon to manipulate the Sony share price. A number of investors sold large chunks of stock in 2014 between the supposed late September breach and the day the world learned of the attack on Nov. 24. There was also one spike in short-selling activity in the weeks leading up to Nov. 24. It is unclear if the SEC ever looked into Sony shortings or sell-offs given that SEC investigations are confidential unless it files an action in court.

Gabelli & Company's John Tinker, a Wall Street analyst who covers Sony, says the nefarious investor angle is possible and that it's happened before. For instance, there was an attempted bombing against publicly traded German soccer team Borussia Dortmund. "It was originally said to be terrorism," says Tinker. "But [investigators later said] it was someone who shorted the stock and had basically hoped to kill the team. The stock would collapse. There's some pretty weird people out there. You never know the lengths to which people will go."

In any case, the hackers appeared to be bent on humiliating Sony, particularly Pascal, who was in the middle of negotiating her contract renewal at the time of the hack. (Leaked emails showed Pascal making inappropriate jokes about President Obama and later fighting with Rudin.)

Sony fought to keep its composure as executive and talent salaries became public (the fact that Amy Adams and Jennifer Lawrence made less than their male co-stars in *American Hustle* became a Hollywood rallying cry). Internally, fear reigned. Top executives were given old BlackBerrys that had been stored in the basement of the Thalberg Building. Pascal enlisted a nurse to give sleep-deprived staffers B12 shots. Another former executive says he hired a private investigator after being hacked multiple times following the 2014 incursion.

Rival studios shunned Sony executives and wouldn't take their calls, one former president notes. "They wouldn't open our emails," he says. "They thought they'd be infected."

As a sign of their resilience, staffers created a video of how they were carrying on, in which they extolled the virtues of going back to basics and having face-to-face conversations. The Sony legal team advised that it should not be released to the public. "It was extraordinary that every single employee stepped up, and in the end, we got through it. In a strange way, it was our finest moment," says Mosko. "But the video was buried. No one wanted to tell that story."

The studio has never assigned a final dollar figure to losses from the attack, but in a 2015 earnings report, Sony said it would cost $35 million for the "investigation and remediation" for the full fiscal year (that tally did not include lawsuits). SPE's Japanese parent company finally seems to have gotten its groove back (the stock is now triple what it was at the time of the hack, trading at $62.13). But in an increasingly data-driven industry, the attack provided a wake-up call for the rest of Hollywood. Timothy Toohey, who heads up Greenberg Glusker's cybersecurity practice, says the studios all the way down to the smallest vendors have strengthened their firewalls in response to the Sony fallout. "Reporting structures have improved. The internal management of security and privacy issues has improved. They've devoted more resources to the issue. But there's no such thing as perfect security," he says. "Could it happen again? Absolutely."

Attorney Bryan Freedman, who represented several parties affected by the Sony hack, says studios share an ethical responsibility to work together to prevent it from happening again. "From an industry standpoint, I'm not sure enough has been done in terms of collective coordination," says Freedman. "While you do hear more about cybersecurity, it's not a topic that's readily discussed as a group with law firms, studios, talent agencies and management companies all participating."

Whether or not the government ever arrests Park (if he exists), there likely will always be those who hold on to their doubts.

For his part, Rogen has moved on, even if he's still a bit curious about what really went down. "It would be nice to know the truth," he says. "I don't think I would feel drastically different on a personal level if it was or wasn't North Korea. I do think other people would probably feel vindicated."

***

The Hack Was Just The Start: Legal Fallout

As if the damage done by the hack wasn't severe enough, Sony was then sued for negligence by its employees and by one of its partners for breach of contract.

Angry Employees

The multiple lawsuits filed by current and past Sony employees in late 2014 and early 2015 were consolidated into a class action led by Michael Corona, who worked for the company from 2004 to 2007. The employees claimed the studio's negligence compromised their private information, including Social Security numbers, account routing information and medical records, leaving them vulnerable. Sony settled after losing a bid to get it tossed. As part of the deal, Sony created a $2 million fund to reimburse employees (up to $1,000 each) for preventative measures they took to protect against identity theft. The company also agreed to provide identity protection services for two years and to reimburse another $2.5 million (a max of $10,000 per person) for those who could show unreimbursed loss as a result of the hack. Sony also had to foot the bill for more than $2.5 million in attorneys' fees.

Piracy Problems

In July 2016, *To Write Love on Her Arms* producer Possibility Pictures sued Sony, claiming the film was illegally distributed online as a result of the hack. Possibility claimed Sony violated a provision in its contract that requires it "to protect the Picture worldwide on the internet directly or through third party vendors, representatives or agents." That dispute settled in early 2018, and the details weren't released.

USA v. North Korea

The DOJ in September 2018 charged North Korean national Park Jin-hyok with conspiracy to commit computer fraud and conspiracy to commit wire fraud. They allege he was not only involved in the Sony hack, but also the 2017 WannaCry 2.0 global ransomware attack and "numerous other attacks or intrusions" on industries including entertainment, defense and utilities. Park, who also is alleged to be part of a government-sponsored hacking team known as the Lazarus Group, is on the FBI's most wanted list. North Korean officials have denied Park's existence and any responsibility for the hack.

***

3 Other Big Hollywood Hacks

Although many Hollywood breaches never come to light, with companies quietly paying the ransoms demanded by the criminals, several are known.

UTA

On April 11, 2017, UTA's IT department discovered that a cyber intruder had hacked the voicemail system and computer network, and the agency quickly shut down its systems, sending agents to conduct business on their iPads. Soon a demand from a hacker arrived: Pay a ransom or watch the agency's most confidential data be posted online. It was said to be one of at least a half-dozen extortion attempts against Hollywood firms around that time. UTA says no personal data of its clients or employees had been compromised.

Netflix

Sometime in late 2016, a hacker collective known as

TheDarkOverlord breached the network of postproduction facility Larson Studios and stole unaired episodes of Netflix's *Orange Is the New Black*, CBS' *NCIS: Los Angeles*, Fox's *New Girl* and IFC's *Portlandia*. In March 2017, TheDarkOverlord demanded a ransom of 50 bitcoin (roughly $60,000 at the time) by an April 30, 2017, deadline. Netflix never responded to the hackers (it's unknown if the other networks paid up), and two days before the deadline, TheDarkOverlord posted the first of 10 episodes of season five of *Orange Is the New Black* on Pirate Bay.

HBO

On July 27, 2017, HBO became the victim of a coordinated cyberattack in which a staggering 1.5 terabytes of data was pilfered from the company's servers. In a letter addressed to former CEO Richard Plepler, the hackers warned: "We successfully breached into your huge network. ... HBO was one of our difficult targets to deal with but we succeeded (it took about 6 months)." Going by the name of Mr. Smith, the hackers demanded money (though the figure was redacted in the version of the letter *THR* viewed at the time) and claimed that HBO was their 17th target. Mr. Smith released everything from a script summary of an upcoming *Game of Thrones* episode to a month's worth of emails from the inbox of one of the company's production executives, as well as unaired episodes of *Ballers*, *Insecure* and *Room 104*. Nearly five months later, federal prosecutors pinned the theft on an Iranian military hacker.

This story first appeared in the Nov. 25 issue of The Hollywood Reporter magazine. To receive the magazine, click here to subscribe.

Main Image: Illustration by: Lincoln Agnew

The Hollywood Reporter

© 2019 The Hollywood Reporter
All rights reserved.

The Hollywood Reporter, LLC is a subsidiary of Prometheus Global Media, LLC.