

[Risk Based Security](#)

Not just security, the right security.

Call Us! (855) RBS-RISK

- [About RBS »](#)
- [News](#)
- [Products »](#)
- [Services »](#)
- [Research](#)
- [Contact Us](#)

Not Just Security, the Right Security.

- [Home](#)
- [Security Intelligence »](#)
- [Industry Solutions »](#)
- [Compliance »](#)
- [Cyber Liability »](#)

A Breakdown and Analysis of the December, 2014 Sony Hack

December 5, 2014 By [RBS](#)

[The Beginning \(November 24\)](#)
[Second Round of Leaks \(December 3\)](#)
[The Analysis Game \(December 4\)](#)
[The Next Chapter \(December 5\)](#)
[The Analysis Continues \(December 7\)](#)
[Fifteen Days Under Siege \(December 8\)](#)
[Reality and the Blame Game \(December 9\)](#)
[My Life At The Company, Part 1 \(December 10\)](#)
[Another Day, Another Email Spool \(December 10\)](#)
[Celebrity Gossip and Hacking Back \(December 11\)](#)
[Debates, Goliath, and Apologies \(December 12\)](#)
[My Life At The Company, Part 2 \(December 13\)](#)
[GOP at Christmas, Part 2 \(December 14\)](#)
[Cyber Insurance, Copyright, Parody \(December 15\)](#)
[Lawsuits, Terror, War, and we hope Hyperbole \(December 16\)](#)
[Leaks, Blame Game Redux, and Caving In \(December 17\)](#)
[Attribution is Hard, the Guessing Game, and Perspective \(December 18\)](#)
[Proportional Response, Fallout, and Politics \(December 19\)](#)
[Attribution Dilemma Continues and Weekend Roundup \(December 21\)](#)
[Holidays, A Time To Reflect \(December 26\)](#)
[Ex-Sony Employees, Russia, NK, Anonymous, and Sanctions \(January 5th\)](#)
[Insurance Claims, Money and Pranks \(January 6th\)](#)
[Attribution, Someone Is Wrong, and Lulz! \(January 12th\)](#)
[Catching Up and Closing Out! \(February 22nd\)](#)

On November 25, a new chapter was added to the chronicles of data theft activity. A group calling itself GOP or The Guardians Of Peace, hacked their way into Sony Pictures, leaving the Sony network crippled for days, valuable insider information including previously unreleased films posted to the Internet, and vague allegations it all may have been done by North Korea in retribution for the imminent release of an upcoming movie titled “The Interview”.

While politically motivated attacks and theft of intellectual property is nothing new, this incident certainly stands out for several reasons. First, via a Pastebin link, the group released a package and links to torrent files hosted on four sites consisting of 26 parts, broken out into 25 1GB files, and one 894 MB rar file. The files were also uploaded to the file sharing giants MEGA and Rapidgator, but removed by site managers shortly after. The researchers at RBS were able to access the files and analyze the content prior to the information going off-line, as well as reach out to GOP.

The results of the analysis provide unprecedented insight into the inner workings of Sony Pictures and leaked the personal information of approximately 4,000 past and present employees. As if the sensitive employee information wasn't troubling enough, the leak also revealed curious practices at Sony, such as money orders used to purchase movie tickets that were apparently re-sold back to Sony staff.

The Guardians Of Peace made their contact information available for a brief time. RBS researchers used that opportunity to contact the group seeking comment and received the following response:

I am the head of GOP.
 I appreciate you for calling us.
 The data will soon get there.
 You can find what we do on the following link.

The link provided only led to a Facebook page that was not in use. The following time line gives more perspective and analysis of the details of the intrusion based on information made available via public sources.

The Beginning (November 24)

On November 24th, [a Reddit post appeared](#) stating that Sony Pictures had been breached and that their complete internal network, nation-wide, had signs that the breach was carried out by a group calling themselves GOP, or The Guardians Of Peace. This comes three years after a [large series of attacks against Sony became public](#).

Within hours, Geek.com had reported that [“Sony just got hacked, doxxed, and shut down”](#) as Sony went into panic mode over the

breach. Minutes after the original reddit post appeared, the thread exploded with comments and feedback about the content. Several links to additional files were included within the comments that included [two text files](#) that listed additional file names that were said to be coming in a subsequent leak of information from the Sony network.

In order to better understand the breach and the ramifications, Risk Based Security (RBS) reached out to the Guardians of Peace and asked for more information. During the brief email conversation, they stated that additional data leaks were forthcoming, and that they had obtained over a dozen terabytes of data from various Sony servers. The mail went on to say that additional information would be published soon, and provided a link to a [Facebook page that appeared to be closed](#).

Movie Leaks (November 26th)

A few days after the the initial breach report was announced, four torrent links were published to torrent trackers that contained unreleased movies from Sony, obtained by GOP during the attack. These titles included [Annie](#) (December 19), [Mr Turner](#) (December 19), and [To Write Love On Her Arms](#) (March 2015). According to several torrent tracking sites, these files have been downloaded over 100,000 times.

On December 1st, [NBC News aired a segment reporting](#) that the FBI were investigating the breach and the possibility that North Korea was involved. While this may sound far-fetched at first, North Korea has a clear motive in attacking Sony. On December 25th, Sony is releasing a movie called [The Interview](#), which follows the story of two celebrity TV hosts that get a chance to interview Kim Jong-un. Before heading to North Korea, they are asked by the [C.I.A.](#) to assassinate him. Despite the movie being labeled a comedy, [North Korea has stated](#) that if the movie is released, they would consider it an "act of war".

When the BBC [reached out to North Korean officials](#) asking if they were behind the attack on Sony, they were given a curious response of "Wait and see." North Korea had also [complained to the United Nations](#) about the movie earlier this year in July, while not naming it specifically.

First of the Leaks (December 1)

On December 1st, GOP started publishing the full cache of data files taken from Sony's servers with the first chunk totaling a respectable 24.87GB of compressed files. Surprisingly enough, the GOP appears to have [used compromised servers](#) on Sony's network to upload and [seed the torrent for the leaked data](#), as well as uploading it to [MEGA](#) and [RapidGator](#). Within hours of the upload, MEGA removed all links to the data. [Dec 9 update: subsequent [analysis by Mario Greenly](#) suggests Sony is not seeding/uploading data, only downloading it, likely in an attempt to slow progress for other downloaders.]

First leaked data summary, some analysis [courtesy of IdentityFinder](#):

- 26.4 GB in size, containing 33,880 files and 4,864 folders.
- Includes 47,426 unique Social Security Numbers (SSN)
- 15,232 SSN belonged to current or former Sony employees
- 3,253 SSN appeared more than 100 times
- 18 files contained between 10,860 and 22,533 SSN each.

Example of employee data found:

- One file (\HR\Benefits\Mayo Health\Mayo XEROX assessment feed) contains 402 full Social Security numbers, internal emails, plaintext passwords, and employee names
- An additional 3000 or more Social Security numbers, names, contact details, contact phone numbers, dates of birth, email addresses, employment benefits, workers compensation details, retirement and termination plans, employees previous work history, [executive salaries](#), medical plans, dental plans, genders, employee IDs, sales reports, copies of passport information and receipts for travel, as well as money order details to purchase movie tickets to resell back to the Sony staff. The leaked information also included documents, payment, and account information to order custom jewelry from Tiffany & CO via email.

Second Round of Leaks (December 3)

By this point, we can only imagine how Sony was in full panic mode attempting to respond to, and contain the breach. By this point, Sony executives had [confirmed the leaked data was authentic](#). The mainstream media was coming to grips with the ordeal, exploring ideas on the ramifications, and the resulting fallout. Initial analysis of the data from the first set of files disclosed had begun, as the second disclosure of files occurred. A GOP member identifying themselves as the leader of the group told RBS "Today more interesting data will be presented for you." before pointing RBS to a [new link containing additional files](#), as part of the email dialogue established (interestingly, one mail came from Hushmail who is [known to cooperate with federal agencies](#)). The second leak was considerably smaller, a mere 1.18GB containing two files named "Bonus.rar" and "List.rar". While the files are small, they perhaps contain the most sensitive data to be disclosed by this point. This includes full security certificate information, internal and external account credentials, authentication credentials with plaintext passwords for systems such as the [Sony YouTube page](#), UPS accounts.

Bonus.rar file summary:

- 33.7MB compressed
- Contains plaintext credentials (~ 500 total), server information, internal IP addresses and other data.
- List of security certificates for servers, users, and services, and a list of what each certificate is related to.
- Credentials include YouTube login information for the [SonyPictures](#), Spidermanmovie, EvilDeadMoive, GrownupsTheMovie, and Thisistheend movie channels, complete list of older social media accounts for campaigns on facebook and twitter.
- 121 FTP plaintext credentials, including the main Sony Pictures FTP server.
- Plain text Credentials for major news and media sites like NY times, LA Times, Daily Variety, hollywoodreporter.com, indiewire.com.
- Plain text passwords in formats like "sonyl2345" for critical internal and forward facing services.
- Username passwords combos in a file named My PAsswords contain: novell, mediataxi, inflight, fidelity, spiDR, SPIRIT, sony style family center, FEDEX, Connect, SPTI, Acron TASS, SPE Courier, Concur, SPC Press, AIM, HR Connect, AMEX, outlook all in clear text with username and password combos.
- Accounting and payment information for AMEX for "The Interview" in plain text.
- Accounting and payment and other related credentials for "Death at a Funeral"

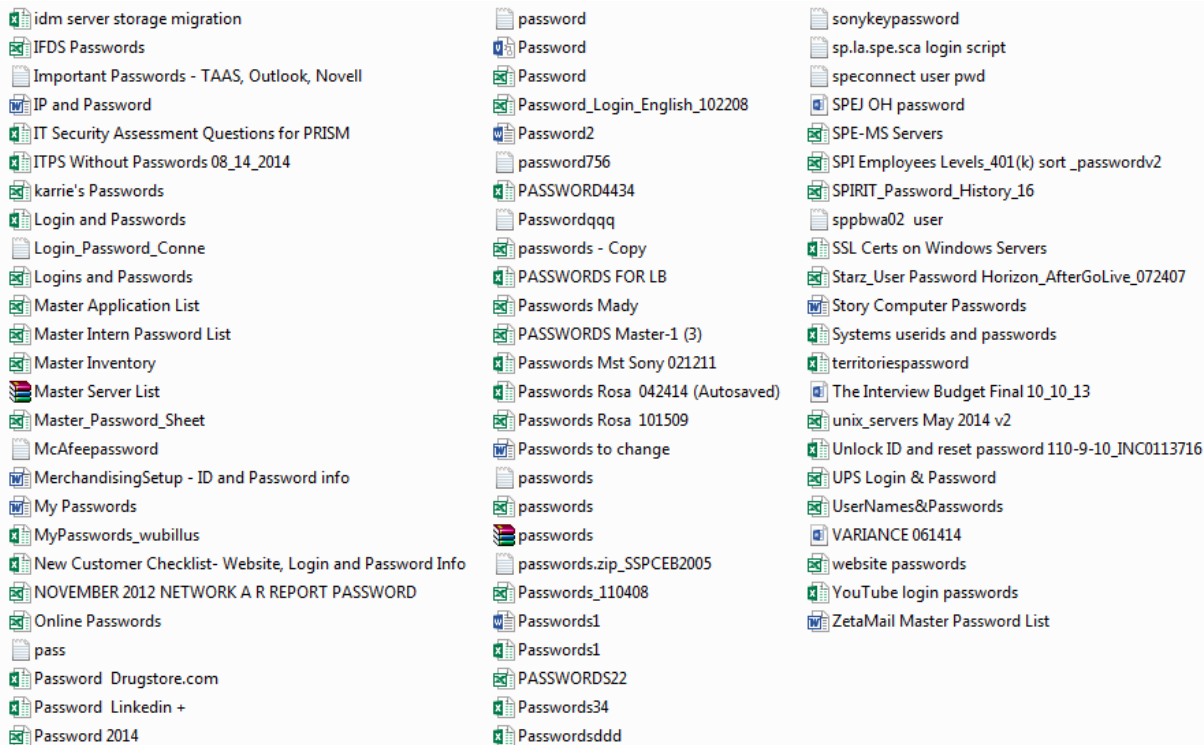
List.rar file summary:

- 1.8MB compressed
- Three files containing internal and external PC data, Linux servers, and Windows servers

The Analysis Game (December 4)

When analyzing high-profile breaches, it is common for the media and security companies to make mistakes. This often occurs due to conflicting or unclear information that seems valid on the surface, but falls apart under heavy scrutiny. For example, a [Gizmodo article](#) says

that Sony stored password information in a folder called 'Password'. A better explanation is that the archive released by GOP was created, and the hackers named that folder, not Sony. Below is a screenshot of some of the contents of the 'Password' folder from the GOP 'Bonus.rar' file:



As more journalists commit time to covering the breach, more details emerge, making this a constantly unfolding story. It also lends to a form of public debate, where one journalist may call into question conclusions of another. For example, [Wired released an article today](#) that went into detail about how the compromise may have happened (malware dubbed "wiper") and also called out other journalists saying the North Korean link is not likely. While they make good points about the GOP group and how nation states generally conduct computer intrusions, there is also the possibility that it was specifically designed not to look like such an attack for plausible deniability. Or it may be as simple as North Korea suggesting they may have had a hand in it, to bolster the notion that they are serious contenders in International computer intrusions for espionage and spying, like their counterparts.

What is curious in this story, is that the FBI released a "[Flash Alert](#)" regarding malware that comes after the reported attacks on Sony. This warning comes very late in the game, and also leads to more questions about the security analysts brought in to figure things out. The same article mentions that Mandiant was brought in to address this breach before it became public. Yet, Mandiant has not made a statement on the matter, while being notoriously media-friendly in [blaming hacker sources, specifically the Chinese](#), even if they may not have been involved.

[According to Re/code](#), Sony is set to announce that they have attributed the attacks to North Korea, making this a he-said, she-said ordeal in the short term. For those interested in more details on the malware found in Sony systems that may have been the point of compromise, [Ars Technica has released a more detailed article](#) focusing on it.

The Next Chapter (December 5)

As mentioned, this story is unfolding every day. New information, new perspective, and new deductions come every day. Risk Based Security has been tracking breaches for a very long time, and has frequently seen such high-profile breaches unfold over years. After the initial weeks or months of a breach, most news outlets and security companies lose interest. Long-term though, part of the story includes the eventual investigation, consultants, lawsuits, stock price fluctuations, and more. The entire picture of a major compromise is the real value, as that is where companies can fully learn of the risks of a breach.

Today the Guardians of Peace have contacted RBS, and likely other companies or journalists, with a third link to leaked data along with a short statement and request calling for others to join them:

Anyone who loves peace can be our member.
Please tell your mind at the email address below if you share our intention.
Peace comes when you and I share one intention!

jack.nelson-63vrbu1[at]yopmail.com

You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses.
These include many pieces of confidential data.

The data to be released next week will excite you more.

The leaked data has been uploaded as BitTorrent links to various file sharing sites via the same methods used in previous disclosures, some of which are served off breached Sony Pictures EC2 servers as well as being uploaded directly to the RapidGator file sharing service. As before, RapidGator quickly removed the data within three hours of it being posted.

The torrent is broken into 22 files spanning 52 parts which appear to be just over 100GB of compressed data. This leak has been titled "Financial data of Sony Pictures" so it likely contains financial details of Sony Pictures, the budgets of movies, or more.

Based on the history of contact from GOP, it appears that each day a new email address is used, and it suggests the accounts may be compromised email accounts. Whether these are fallout from the Sony breach or via another source remains unknown.

The Analysis Continues (December 7)

There have been several news outlets and security firms researching the Sony Pictures breach and analyzing the disclosed files as a result of the compromise. An interesting and unexpected development surfaced on today, when security researcher Dan Tentler announced early in the day that he had had a visit from FBI but was not home at the time.

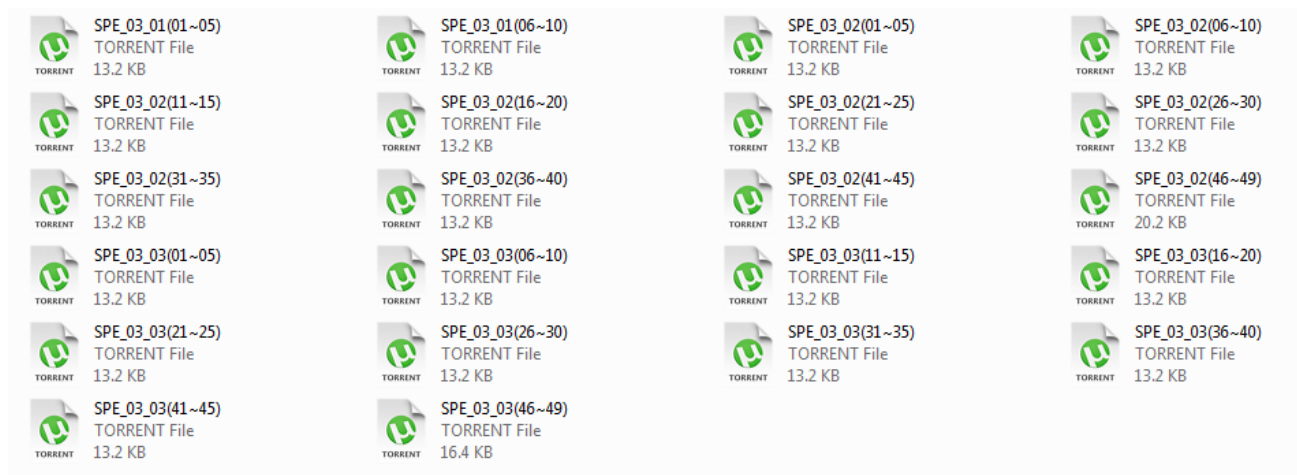
Just to warn other security folk working on the Sony leaks – the FBI just visited my home. I wasn't there, so I'm not sure what they wanted.

He followed up with a comment that was made to his wife:

according to my wife, who answered the door, they started the conversation with the words “illegally downloading” .

Mr. Tentler has been conducting his own analysis and has reported on the Sony incident. He posted a list of nodes where the leaks could be found which may explain the FBI's interest and the subsequent “illegal downloading” comment made to his wife.

Now that the files have been downloaded from the publicly available sources, RBS has had a chance to do a preliminary analysis of the contents. The following is a screenshot showing a sample of the files, to put it into better perspective what is leaked. Note that filenames are logical, not descriptive and human-friendly:



These 22 individual files make up three larger files containing a large set of newly released data, predominantly based on financial information:

File SPE_03_01.RAR (Mostly from Sony [Brasil](#))

- 30,916 individual Files, 2,970 Folders. 16.4 GB / 9.99 GB (Compressed)
- Banking statements, bank account information including wire transfer swift codes etc.
- Financial year reports
- Financial year forecasts
- Budget reports
- Overhead reports
- Receipt and transaction account statements of computer hardware, vehicle (toyota hilux, mitsubishi space wagon), car accessories going back to 1998
- Internal information for Sony Pictures Releasing International portal, screenshots, walkthroughs and other usage information.

File SPE_03_02.RAR (From Sony Pictures Imageworks, Vancouver, and Sony Pictures)

- 89,800 Files, 10,990 Folders. 88.6 GB / 48.9 GB (Compressed)
- Accounting information using [Trintech Inc.](#) software
- Licensing contracts
 - Access Digital (Exyflix)
 - Amazon Europe
 - Amazon Japan
 - Clickpay Multimedia
 - Comcast
 - Eagle Eye
 - Gaia
 - Google (YouTube)
 - Media Vault
 - M-GO
 - Microsoft
 - Playstation
 - Sena
 - Sony Electronics
 - Sony visual products in
 - video futur
 - Yota (aka more)
- Vendors ([Too many to list](#))
- Sony India Financial reports.
- 528 Payrolls for Imageworks Canada with staff full names, contact numbers and residential addresses.
- British Columbia Personal Tax Credit Returns scans of several employees with full personal information including social security number.
- Photocopies and scans of driver licenses, passports and other tax related documents exposing a bunch of personal credentials, home addresses, full names, date of births, social security numbers and more.
- Federal Tax Returns

File SPE_03_03.RAR

- 113,002 Files, 39,612 Folders. 57.1 GB. / 48.1GB (Compressed)
- Incident reports with full names, incident locations, injuries and positions held with Sony.
- SPE Global Security Guidelines v2
- UL training users, full names, addresses, email addresses and common set clear text passwords
- copies of employment contracts and agreements, passports, drivers license, ssn, signatures.

Ongoing (December 7)

The LA Times reported on December 5th, and has said that the FBI have confirmed it, that just hours before the 3rd leak was published online, an unknown amount of Sony employees received threatening emails which are believed to have been sent by the GOP.

The emails which were written is what was described as "broken English", wanted employees to sign a statement disassociating themselves with Sony, and if they did not, were warned that "not only you but your family will be in danger". According to the LA Times, the email included a statement that makes suggests the digital headaches for Sony are going to continue to for some time to come.

"It's false if you think this crisis will be over after some time," the email said, according to a copy obtained by Variety. "All hope will leave you and Sony Pictures will collapse. This situation is only due to Sony Pictures."

Adding to the speculation about how the compromise happened, [Bloomberg is reporting](#) that the compromise and first leak of data happened at the St. Regis Bangkok hotel in Thailand according to an unnamed person "familiar with the investigation".

Fifteen Days Under Siege (December 8)

Late last night, after a long week of previous disclosures, the GOP has released the next batch of leaked data. The new round consists of four archives making two large files, currently being seeded from servers owned by Sony Pictures as before. The torrent that includes all files is only 2.8GB this time and has also been uploaded to a few file sharing websites, although we expect them to be taken down quickly like previous GOP uploads.

Unlike previous disclosures that were straight-forward, this group of files comes shortly after the appearance of a [Pastebin link](#) (now 404) that purports to be from the GOP, and gives a reason for the attacks on Sony Pictures, linking it to the now controversial movie, "[The Interview](#)". There is speculation that the new announcement may not be authentic as it did not get sent out via the previous channels, and suggests an almost afterthought of blaming the movie for their actions. Within hours of this being published on Pastebin it had been removed but was cached by Google on December 8, 2014 15:43:58 GMT. Since then, the cache has also been removed which may be due to Sony complaints. [According to Owen Williams](#), Sony has been sending out [Digital Millennium Copyright Act](#) (DMCA) take-down requests related to the breach and subsequent disclosures. RBS managed to capture the text before it was removed from both Pastebin and Google cache:

by GOP

We are the GOP working all over the world.
We know nothing about the threatening email received by Sony staffers, but you should wisely judge by yourself why such things are happening and who is responsible for it.

Message to SONY

We have already given our clear demand to the management team of SONY, however, they have refused to accept. It seems that you think everything will be well, if you find out the attacker, while no reacting to our demand. We are sending you our warning again.
Do carry out our demand if you want to escape us.
And, Stop immediately showing the movie of terrorism which can break the regional peace and cause the War!
You, SONY & FBI, cannot find us.
We are perfect as much.
The destiny of SONY is totally up to the wise reaction & measure of SONY.

The following is a summary of the fourth leak:

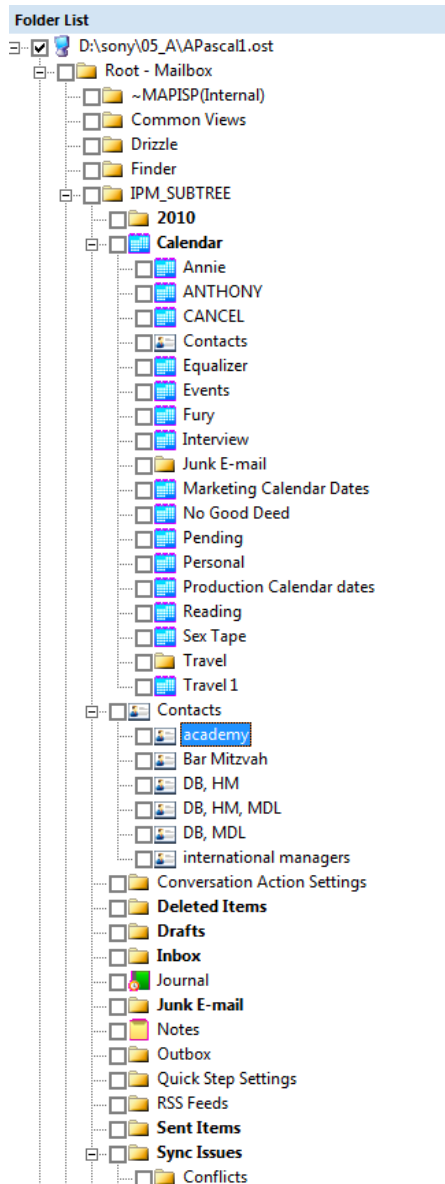
05_01.rar

- mosokos.ost (A Microsoft Outlook mail spool), 3.5GB in size
- "mosokos" is [Steve Mosko](#), President of Sony Pictures Television.
- 3,550 full contact details, full names, email addresses, home addresses
- 14,944 sent emails
- Email contents include account information, password reset mails, personal emails, flight and travel arrangements
- Also includes discussions about internal operations within Sony, the [2013 Breaking Bad Bluray leak](#), discussions about using torrents and the AXN network to distribute Hannibal
- Emails from friends and other Sony staff about TV show torrents and uploads to YouTube, including Breaking Bad, King of Queens, and Hannibal.

05_A.rar

- APascal1.ost (A Microsoft Outlook mail spool), 3.78GB in size
- "APascal" is [Amy Pascal](#), Co-Chairman, Sony Pictures Entertainment and Chairman, Sony Pictures Entertainment Motion Picture Group
- Over 5,000 emails included
- Most recent Inbox email is from November 23, 2014 (likely when the mail spool was taken)
- Emails consist of Sony employee relations, personal invoices, and personal emails
- Includes talk and deals about upcoming movies
- Contains current and closing business deals

View of the APascal1.ost Outlook mail spool showing the folders:



Speculation and analysis of the original compromise method is ongoing. The [Register reports](#) that Kaspersky has published details on the malware that allowed the attackers to gain a foothold into the organization. According to the researchers, the malware has been named BKDR_WIPALL by Trend Micro and Destover by Kaspersky (which [elicited a warning from the FBI](#)), and was previously seen in [attacks against Saudi Aramco](#) by the “Whols Team” in 2012. Kaspersky researchers went on to say that this backs claims that the malware was used in the [2013 Dark Seoul attacks](#), possibly linking the same group or groups to a multi-year campaign of high-profile computer intrusions.

Seemingly unrelated to the GOP breach of Sony Pictures, but coincidental in timing, the Sony PlayStation Network appears to be [suffering their own problems](#) as a group called Lizard Squad is taking credit for a coordinated large-scale denial of service attack, that follows a previous one August of this year. Via Twitter, Sony PlayStation Network has [acknowledged that customers are experiencing problems](#), but do not specifically cite why.

Culver City Sony employees will be briefed by the [Federal Bureau of Investigation](#) (FBI) on Wednesday regarding the recent attacks, [according to the Hollywood Reporter](#). Michael Lynton, Entertainment Chief at Sony, has also called for an all-hands meeting on Friday to further discuss the issue.

Reality and the Blame Game (December 9)

Generally when a high-profile wide-scope breach occurs, news outlets and some security companies are quick to say it was the work of an “advanced” attacker, and that the breach is “unprecedented”. [According to Mashable](#), Michael Lynton (Sony Pictures CEO) sent a letter to all employees featuring a letter from Kevin Mandia, of Mandiant, the company hired by Sony to investigate the breach. An excerpt from the letter:

“This attack is unprecedented in nature. The malware was undetectable by industry-standard antivirus software and was damaging and unique enough to cause the FBI to release a flash alert to warn other organizations of this critical threat,” — Kevin Mandia, [Mandiant Security Consulting](#)

All analysis to date suggests the malware was not unique to Sony, and may have been used several times before. Trying to suggest that malware that evades “industry-standard antivirus software” is “unprecedented” is ridiculous. Antivirus software routinely fails to identify malware due to the archaic signature-based model they use. The software only detects what it knows to look for, and with a few tiny changes, old malware can be made undetectable again; until a new signature is created and pushed to customers. That subscription model is the profit center of the antivirus industry, and they have little reason to improve it. Further, suggesting this breach was “unprecedented” to the size and scope simply isn’t true either. Large-scale compromises like this hit the news every year.

If you recall on December 4th, Re/code [published an article](#) saying that Sony was set to officially blame North Korea for the attacks. Jump

to today, a mere 5 days later, and the FBI is officially saying there is no attribution to North Korea [according to Reuters](#).

“There is no attribution to North Korea at this point...” — Joe Demarest, Assistant Director of the FBI Cyber Division

It has also [come to light via Mashable](#), via the leaked email archives from the fourth leak (December 8), that Michael Lynton (CEO), Amy Pascal (Chairman), and other executives received an email from hackers calling themselves “God” sApstls” . In the email, quoted below, the group threatens ‘great damage’ to Sony Pictures unless financial compensation was provided:

We’ ve got great damage by Sony Pictures.

The compensation for it, monetary compensation we want.

Pay the damage, or Sony Pictures will be bombarded as a whole.

You know us very well. We never wait long.

You’ d better behave wisely.

From God’ sApstls

This goes against subsequent posts from the Guardians of Peace (GOP) who said the intrusion was related to the release of the movie, “The Interview” . At this point it is not clear if a single coordinated group of attackers is changing their public persona or if there are more than one group that have access to the network.

More fallout from the Sony Pictures compromise comes in the form of the attackers using Sony’ s certificates to digitally sign the Destover malware. As [reported by Kaspersky Labs](#), the signed malware appeared on December 5th and will result in additional malware being signed, and likely render subsequent attacks more effective. [Update: It turns out this was a prank carried out by a security researcher, who figured out the password of the certificate (same as the file name), and decided to sign the most amusing/ironic thing he could think of, the malware itself. We are also told that three other certificates used a password of “password” .]

My Life At The Company, Part 1 (December 10)

Now that journalists and security companies have had days to review the incredible amount of leaked data, analysis has shifted to focus more on the contents of the emails of [Amy Pascal](#), Co-Chairman, Sony Pictures Entertainment and [Steve Mosko](#), President of Sony Pictures Television. This has revealed odd details such as Sony [continuing to make considerable money](#) for the show Seinfeld, Sony executives [concerned over the ending of the movie](#) ‘The Interview’ , and that [George Clooney is very savvy](#).

Today also brought the fifth leak of data from the Guardians of Peace (GOP), titled “Gift of Sony for 5th day: My Life At The Company – Part 1” . As before, the leaked data was uploaded to various bittorrent tracking websites with the download consisting of five 1GB parts

The torrent file consists of 5 parts, all 1GB and in RAR format (spe_05_01.part[1-5].rar). The GOP have also included a new statement with this disclosure, again directed at Sony Pictures employees. The message states that they still have large amounts of information to disclose, including personal information and more email spools. The statement reads:

To SPE employees.
SPE employees!
Don’ t believe what the executives of SPE says.
They say as if the FBI could resolve everything.
But the FBI cannot find us because we know everything about what’ s going on inside the FBI.
We still have huge amount of sensitive information to be released including your personal details and mailboxes.
If continued wrongdoings of the executives of SPE drive us to make an unwanted decision, only SPE should be blamed.
Now is the time for you to choose what to do.
We have already given much time for you.

The newly leaked data includes information about Sony’ s anti-piracy efforts, entertainment deals in the works, internal procedures related to tracking torrents and other illegal downloading. It also contains a document that outlines Sony’ s cooperation with 5 major Internet Service Providers (ISPs) to collect full data for monitoring illegal downloads. In addition:

- [Motion Picture Association of America](#) (MPAA) list of outstanding issues and other piracy related information.
- Enhanced Content Protection proposals, drafts, and documents.
- Potential Middle-East partnership deals from 2012.
- Wages of international employees from Sony Australia and Sony China
- Contact information of more than 2,500 employees, additional digital certificates, documents on Internet security, security advisories that may impact Sony systems
- Research documents, internal information about Sony cameras being produced, NATO-Studio August 2014 Tech Meetings Agenda with talks about new technology being produced by Sony
- Project non-disclosure agreements, budgets, financial forecasts for 2013 – 2015, information about projects schedules, deals, costs, profits, advertising revenue, and advisor fees.

Anti-piracy information from Google, YouTube, Netflix, and Farncombe including:

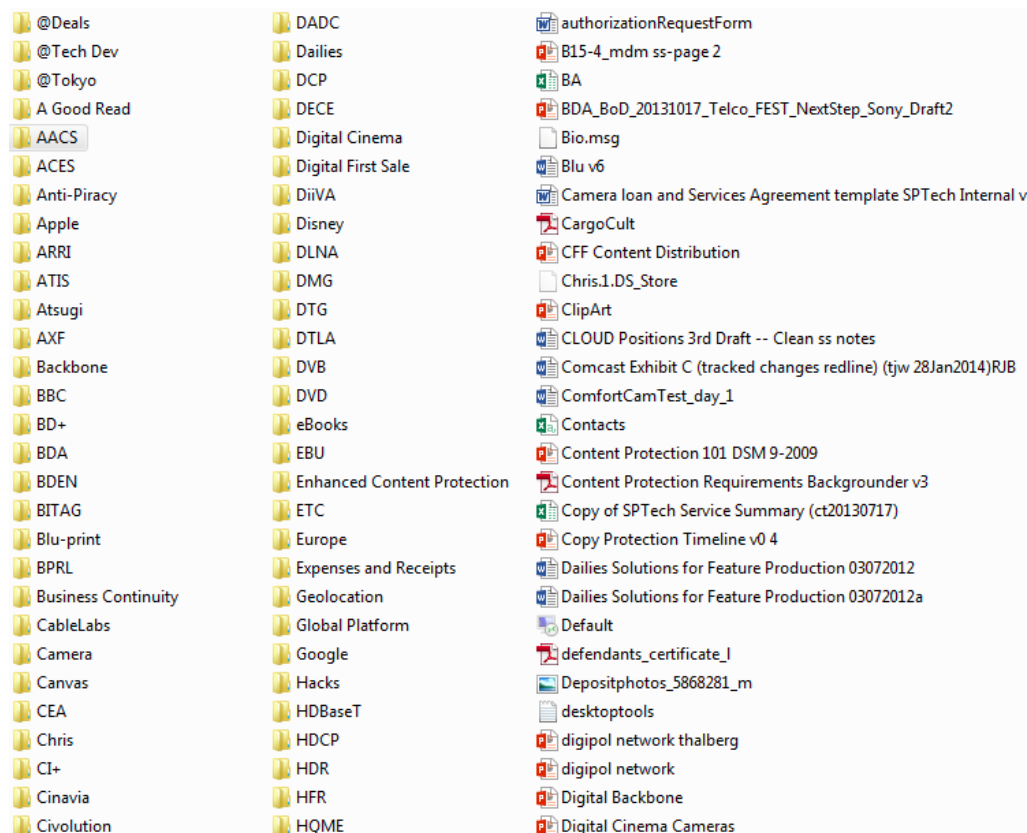
- Total number of notices sent to ISPs with 100% success rate (2,537,932)
- Alerts sent to subscribers (1,475,848)
- Alerts that were not sent but should of been (41,917)
- A breakdown of which content, how many types of alerts sent, and acknowledgements for 2012, 2013, and 2014
- Confidential documents outlining deals, procedures for monitoring, and services provided by [Farncombe](#)
- Large amount of proposals to Google, YouTube, and other services about how to censor search results, remove content from its search
- Content protection documentation

Documents and internal tracking of console hacking information for the PlayStation including:

- 27th Chaos Communications Congress (CCC), Console hacking 2010, PS3 Epic fail.
- Verisign Fraud Alert: Phishing – the latest tactics and potential business impact.
- BHUSA09-Marlinspike-DefeatSSL-PAPER1
- us-14-Rosenberg-Reflections-On-Trustig-TrustZone-WP

A variety of documents on relations with the following companies: AXN, AMC Networks, Hoyts Australia, Animax UK, Channel 5 UK, Chello, Grupo Clarin, 2waytraffic, Dailymotion, Comedy Time, DirecTV, Crackle, Apple, iTunes, Google, YouTube, Hotfile, BBC, BITAG, Telstra,

Rogers, Showtime, Sky, Skype, SNEI, Telus, Tesco, Virgin Media, TVN, Verizon, Telefonica, TTNET, Turner, True Net, Videotron, VUDU, Voole, Redline, and SingNet. The data on deals is extensive to say the least. Below is a small sampling of the folders and documents:



After the [series of incidents with Sony in 2011](#), many analysts were curious about how it would affect Sony's stock price. Between April 4, 2011 and October 12, 2011, Sony's stock price dropped from \$31.45 to \$20.06. That begs the question if this round of incidents is also affecting the price.

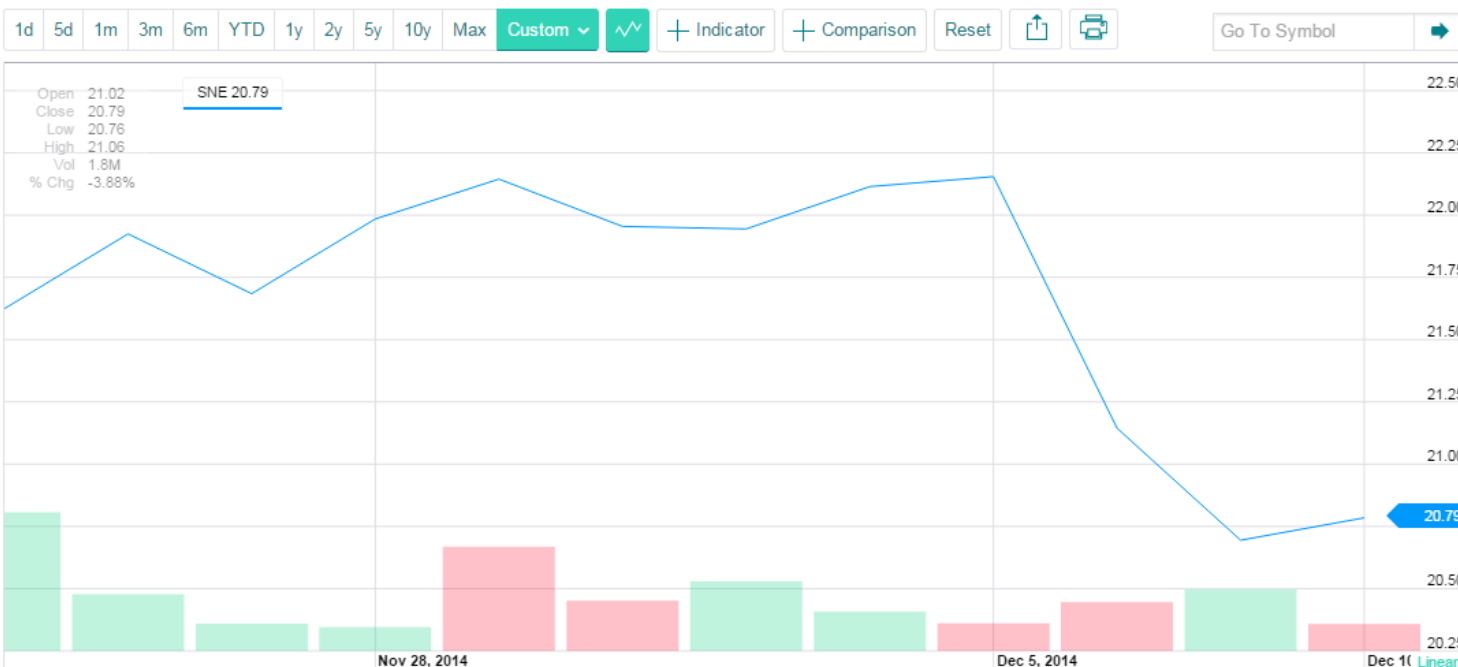
Sony Corporation (SNE) ★ Watchlist

20.79 +0.09(0.43%) NYSE - As of 4:02PM EST

After Hours: **20.92** ↑+0.13 (0.62%) 4:10PM EST

Beat the market

Get the app



Here we [see the stock value between](#) November 25th, when the breach became public, and today. Note that in our experience, we frequently see stock prices drop as an immediate reaction to such events, but often return to the original value within three months.

Yesterday we reported that attackers had used a Sony digital certificate (spe_csc.pfx) to sign the malware believed to have been used in the compromise. It has come to light that this was actually a prank of sorts, carried out by security researchers who figured out the easy-to-

guess passwords protecting the certificates. RBS has seen a portion of the chat log in which they guess the passwords. After placing the [signed malware on VirusTotal](#), Kaspersky apparently made the assumption that it came from the attackers. Steve Ragan [summarized the prank in an article last night](#), and Colin Keigher who was close to the source of the prank, [published a blog this morning](#) giving additional details.

Perhaps the most interesting development though is the possible ‘doxing’ (publishing personal information) of the Sony hackers. Via two Pastebin documents, the real name, address, nickname, birthday, and other personal details of five people are listed. Given the lack of provenance for this information, RBS is not going to further propagate it. The introduction text gives a summary of the alleged hackers:

Sony hackers DX. they hackers from Tunisia Hacker Team but covering as Guardians of Peace for op WeekofHorror to attack USA and support Syria and governments that fight USA (china, korea, iran).

Another Day, Another Email Spool (December 10)

Today also brought the sixth disclosure from GOP, a single file named sony6.rar, that was uploaded to bittorrent tracking and file sharing sites. As usual, the file was quickly removed from the file sharing sites. The file contains another mail spool named “lweil00.ost”, which belongs to [Leah Weil](#), Senior Executive Vice President and General Counsel for Sony Pictures Entertainment. Some details about the 3.84GB mail spool include a list of folders, number of emails, and a brief summary of the content.

Some of the folder names and mail count:

- Admin: 56
- Alertline: 286
- Audit Reports: 28
- Calendar: 6,815
- Compliance dept: 45
- Contacts: 178
- Conversation history: 2
- Deleted items: 4,296
- Designated Employee Notice: 59
- Division Head Meetings: 205
- Executive comp: 60
- Inbox: 41,229
- Sec filings: 30
- SEC FCPA: 102
- Sent emails: 36,586
- SPE Board: 19
- SPE Subsidiaries Report: 3
- Legal: 78

Brief list of highlights:

- Deleted mail contains email retention orders (current financial information email need to be held for 6 years as of 15th jan 2015 that will change to 2 years for all emails unless on legal hold)
- [SKY Perfect TV data leaked June of this year](#), including 10,000 customers name, email addresses, addresses, phone numbers, Pay-TV access control numbers (B-cas#), IC cards, and subscription information which may include payment details. (SKY PerfectTV is responsible for parts of [AXN](#), owned by Sony.)
- Discussions with Paula Askanas and others about uploading fake torrents to frustrate would-be pirates.
- Instructions for how to respond to previous Sony hacking incidents with approved wording for Twitter and Facenook.
- Extensive communications about the 2011/2012 attacks against Sony by Anonymous, including the #opsony threat, sharing pastebin links pertaining to Sony, vulnerabilities on Sony sites (e.g. “Subject: FW: ALERT – ANONYMOUS THREAT – XSS exploited on scajobs.sony.com!!”), details of internal investigations about hacking incidents, and employees attempting to ‘geo locate’ the hackers and match their handles to other aliases.
- Internal concern that Mark Zuckerberg might sue Sony over the movie “[The Social Network](#)”.
- Correspondence between Sony staff about George Clooney wanting to direct a movie based on [Hack Attack](#). Concerns are expressed over potential legal issues if media giant Rupert Murdoch’s name is used within the movie since its based on a real story.
- Emails about previous Sony breaches including SPE, Sony PlayStation, and other divisions of the company.
- Emails about harassing calls from ANTI-SOPA protestors.

Given the severity of this breach, along with the history of previous Sony incidents, it is worth remembering the first part of a 2007 article titled “[Your Guide To Good-Enough Compliance](#)” by Allan Holmes. It is a good reminder that security is not just technology, but a mindset, and that failing to work toward a secure environment may have long-lasting repercussions.

Celebrity Gossip and Hacking Back (December 11)

The culture of watching celebrity lives has captivated the TV-watching audience for years now, with “reality” shows dominating news and airtime. With the Sony Pictures executive mail spools being leaked over the last few days, those analyzing the contents are running into emails from high-profile actors and actresses that communicate with them. As previously mentioned, George Clooney takes a hardline, intelligent approach to emails and knowing the contents could leak out.

Now we learn of drama between [Amy Pascal](#) and [Scott Rudin](#) over the [highly-anticipated upcoming biopic on Steve Jobs](#), in which there is serious disagreement over [Angelina Jolie’s](#) disappointment that director [David Fincher](#) would be involved in ‘Jobs’ instead of her own movie, ‘Cleopatra’. Despite the differences between Pascal and Rudin, the leaked emails show they do have one thing in common: [joking about President Obama’s race](#). In another exchange between Pascal, Michael Lynton, and [Clint Culpepper](#), they are [candid in their feelings for an actor asking for more money](#) to promote a movie via social media:

“I’m not saying [Kevin Hart’s] a whore, but he’s a whore.” — Clint Culpepper (President, Screen Gems)

With the leaked emails, the public is also learning a wide variety of personal information about celebrities. In addition to email addresses, analysts are finding out aliases celebrities use when traveling, phone numbers, and more. These include Brad Pitt, Julia Roberts, Tom Hanks, and more [according to Sophos](#).

Changing tracks, the other interesting development is how people are reacting to, and labeling Sony’s efforts to curb piracy. More specifically, some are considering and/or labeling the actions as a denial of service (DoS) attack. In using that term, they are effectively suggesting that Sony’s tactics are illegal. The tactics in question are based on Sony using hosted servers to pollute a bittorrent swarm, making the downloading of the illicit files (in this case the leaked data) more difficult. By introducing hundreds or thousands of peers that advertise they have parts of the file, and then failing to send them, would-be downloaders experience considerably slower rates. In some cases this causes them to give up on the download completely, and in other cases may mean the download could take more than a day, rather than an hour or three.

The use of the term ‘denial of service’ appears to originate in [an article from re/code](#), where they say that Sony “is using hundreds of computers in Asia to execute what’s known as a denial of service attack on sites where its pilfered data is available”. Technically, this is true as a denial of service attack is just that; it denies some level of service to users. However, in this case Sony is attempting to deny people from obtaining the leaked data from their network. Is this legal? Based on our understanding of U.S. computer crime laws, their actions do not technically violate the [Computer Fraud and Abuse Act](#) (CFAA, specifically [18 U.S. Code § 1030](#)). However, according to the [Department of Justice manual on prosecuting computer crime](#), this may be up for interpretation by a district attorney as far as what constitutes a “legitimate user”:

Intruders can initiate a “denial of service attack” that floods the victim computer with useless information and prevents legitimate users from accessing it. [...] Prosecutors can use section 1030(a)(5) to charge all of these different kinds of acts.

This boils down to whether journalists can publish the contents of material that were illegally obtained by a third party. The Student Press Law Center (SPLC) maintains a [great summary of this issue](#) and cites the Supreme Court’s 2001 decision *Bartnicki v. Vopper*, which struck down wiretapping statutes that prohibited the disclosure of illegally intercepted communications. With this in mind, then anyone attempting to download the leaked Sony data *are* legitimate users and Sony’s efforts to deny that service may violate the CFAA. We’re not lawyers and this is certainly a case full of gray, not black and white.

The one thing we can say with certainty is that using the term “Denial of Service” (DoS) or “Distributed Denial of Service” (DDoS) are loaded terms, as they are typically used to describe either a technical attack against a system (where intent and ethics aren’t part of the discussion), or the actions of a criminal. This terminology gets further confusing and misleading when it is [accompanied with phrases like](#) “When the hackee becomes the hacker... In a somewhat amusing twist to the ongoing Sony Pictures hack...” or [more aggressive wording](#) like “Sony Pictures is employing hacking techniques...”, since this begins to ascribe specific criminal notions to their actions. The one thing Sony is doing right in all this mess, is [denying everything](#).

Debates, Goliath, and Apologies (December 12)

Whenever a large breach occurs and involves the disclosure of personal email, even if “professional”, several debates re-emerge. The first revolves around the ethics of reading private emails. On one hand those emails, while public, were never meant to be published. On the other hand, quite simply, they were made public. This is not a debate that will be ‘won’ as both sides have valid points. One thing to keep in mind is how you would feel if your emails were leaked. RBS has balanced this dilemma by analyzing the meta-data (e.g. mailbox size, number of mails) rather than the content. Instead, we make observations about what others have published regarding the content and link to their articles.

The second debate that crops back up is the ethics of downloading stolen content such as emails. As mentioned on yesterday’s update, the Supreme Court 2001 decision in *Bartnicki v. Vopper* says that downloading and using stolen material such as email is legal for journalists. However, current intellectual property (IP) and copyright law could trivially challenge that ruling if were to re-appear in front of the Supreme Court. Regardless of that decision, [Kashmir Hill reminds us](#) that simply downloading the stolen content may prompt a visit from federal authorities. Not only has Dan Teltler ([@viss](#)) been visited, but Steve Ragan has also had a run-in with the FBI over the Sony material. We have little doubt that they are not the only two to have been visited. We also want to remind the FBI that visiting journalists and researchers who are downloading and analyzing the material are not who you are really after. Assuming you are trying to catch the individuals that actually compromised Sony’s network. If you treat them as sources instead of persons of interest, you may find they can assist you with your job.

The third debate that tends to come up among journalists is if analysis or snippets of such emails should be published after downloading and reading. [Variety weighs in on this topic](#) in an article titled “*Why Publishing Stolen Sony Data is Problematic But Necessary*”. While some of the material coming out of the leaks is very personal and embarrassing (e.g. racial jokes, calling professionals obscene names), such leaks can also lead to information that is specifically of interest to the public and should not be kept behind closed doors.

On the bad side of such disclosures, we see that the leaks are [revealing very sensitive information](#) such as employee’s children health information including special needs, diagnoses, and treatments. The leaks further go on to reveal birth dates, gender, health conditions, and medical costs for as many as 34 Sony employees, according to Bloomberg. On the good side of such disclosures, we find out that the MPAA, in conjunction with six studios, allegedly plans to pay elected officials to attack Google in an effort to curb piracy dubbed “Project Goliath”, [according to TechDirt and The Verge](#). These two things are pretty much the opposite ends of the spectrum on the harm versus value of leaked data.

Finally, after weeks of silence, one [Sony executive has broken their silence](#) and gone on record about the leaked emails, albeit briefly. [Amy Pascal](#), Co-Chairman, Sony Pictures Entertainment, [has apologized](#) and given an explanation for the racially insensitive comments directed at President Obama. Food for thought this weekend; if your email was published, what would you have to apologize for, if anything?

My Life At The Company, Part 2 (December 13)

Today brought the seventh leak of data from the Guardians of Peace (GOP), titled “My Life At The Company – Part 2”. This follows a Pastebin post in which they warn Sony executives that an important message has been sent to them:

by GOP

Important





















Message to SPE executives

I’ve sent you a message.
Confirm your mailboxes.

The Pastebin post with links to the newly leaked information from Sony networks is accompanied by another message saying that upcoming Christmas leaks will contain larger quantities of data and it will be “more interesting”. One thing that is already interesting is that GOP says if anyone sends an email titled “Merry Christmas” to one of five provided email addresses, they will take requests with what should be in the upcoming leak:

We are preparing for you a Christmas gift.
The gift will be larger quantities of data.
And it will be more interesting.
The gift will surely give you much more pleasure and put Sony Pictures into the worst state.
Please send an email titled by “Merry Christmas” at the addresses below to tell us what you want in our Christmas gift.

The actual data leaked today appears consists of 6.45GB of uncompressed data, distributed via bittorrent links that do not appear to be seeding from same 54 IP addresses previously seen. The data consists of 6,560 files throughout 917 folders. A screenshot showing a sampling of the leaked data:

Name	Date modified	Type
 Documents	12/14/2014 9:15 AM	File folder
 junderwood	12/14/2014 9:14 AM	File folder
 Kanal Global	12/14/2014 9:14 AM	File folder
 KNTV	12/14/2014 9:14 AM	File folder
 Korean JV	12/14/2014 9:14 AM	File folder
 Korean Premium	12/14/2014 9:14 AM	File folder
 K-Pop	12/14/2014 9:14 AM	File folder
 LAG - CONFIDENTIAL	12/14/2014 9:14 AM	File folder
 LATAM	12/14/2014 9:14 AM	File folder
 Left Bank	12/14/2014 9:14 AM	File folder
 Legend SPENA	12/14/2014 9:14 AM	File folder
 Legendary	12/14/2014 9:14 AM	File folder
 Library Titles	12/14/2014 9:14 AM	File folder
 London TV	12/14/2014 9:14 AM	File folder
 MAA India	12/14/2014 9:14 AM	File folder
 May Screenings	12/14/2014 9:14 AM	File folder
 Media 4 Equity	12/14/2014 9:14 AM	File folder
 Megaphone	12/14/2014 9:14 AM	File folder
 Model Examples	12/14/2014 9:14 AM	File folder
 Movies 4 Men	12/14/2014 9:14 AM	File folder
 MRP Network Overview	12/14/2014 9:14 AM	File folder
 MSM	12/14/2014 9:14 AM	File folder

A very brief analysis suggests this leak contains:

- Sony internal documents for tracking deals, expenditures, and revenue.
- Complete working folders for [Jim Underwood](#) (likely ex-Sony Executive VP, Worldwide Digital and Commercial Strategy [LinkedIn Profile](#))
- Documents related to the acquisition of Grouper Networks in 2006 and related material the following years.
- Many acquisition proposals, Sony's perspective on the pros and cons to the deals, companies of interest, and potential profit, including [Left Bank Pictures](#).
- Drafts on the best ways to battle piracy, from 2009 on.
- Enhanced Content Protection Overview written by Chris Odgers – complete analysis of possibilities of breaches, exploits, detection, and prevention methods for data streaming services to prevent hijacking.
- Emails about Australian TV not being finalized before screening started. This appears to be related to the recent run of older American TV shows like [Starky and Hutch](#).
- Breach monitoring and revocation rules for Phase 1 Service if the F1 Box is hacked.
- Business documents and dealings with [Abril.com](#) out of Brazil.

As other researchers and journalists perform a more extensive analysis, we will provide links, summaries, and commentary on it.

Between Sony's efforts to hinder acquiring the data via the torrents, and the file-sharing sites rapidly removing leaked data, some people have begun to make their own archives of the leaked data on additional sites. Some of them are being shared via Twitter and others via additional file sharing sites.

Following up on the legal angle (covered on December 11 update), [Betabeat has published an article](#) titled “*No Gray Area: It's Definitely Not OK to Publish Emails From the Sony Hack*” in which they point out the moral and ethical issue with disclosing details of the leaked data. They argue that a variety of news outlets including Perez Hilton called the disclosure of celebrity nude photos “a crime”, while having no issue publishing private conversations from Sony executives. This is an interesting observation as it appears to establish the line between ‘acceptable’ (leaked emails) and ‘taboo’ (nude celebrity photos) for journalists. We are sure that this is a debate that will rage on for some time. [Note that the Perez Hilton [article that mentions the word ‘crime’](#) cites Jennifer Lawrence's statements in which she called the publication of her photos a ‘sex crime’.]

Business Insider has also [published an article](#) citing an “IT worker employed by a firm that has access to Sony's computer network” that says Sony's network security was “outdated and ineffective”. The article goes on to reference the “Password” folder that contained numerous passwords, but as we previously noted, that was likely at the hands of the attackers, not necessarily Sony. In [another article from re/code](#), they also reveal that the leak contains a very recent security audit performed by [PricewaterhouseCoopers LLP](#) between July 14 and August 1. re/code reports that the audit found over 100 systems that were not being monitored by corporate security, who were charged with overseeing Sony's infrastructure.

GOP at Christmas, Part 2 (December 14)

The last few years have shown us that the U.S. legislative body is not always in touch with the current state of computer crime, and [often very out of touch when it comes to the notion of “cyberwar”](#). [Time Magazine reports](#) that Rep. Mike Rogers (R-Mich), chairman of the House Intelligence Committee suggested that a nation-state, specifically North Korea, was behind the attack on Sony. This was on Friday, [three days after the FBI declared that North Korea was not responsible](#). Time goes on to quote Rogers as saying:

“That was the first [time] — if you take at face value public reports — a nation state decided a retribution act could result in destroying data, bringing down a company...” — Rep. Mike Rogers, Chairman of the House Intelligence Committee

Most everyone in computer security knows, taking initial public reports at face value is not a wise action. As we have pointed out in previous updates, the attribution for this attack has ranged from North Korea, to an independent group known as the Guardians of Peace, and has also seen some indication that multiple groups may be involved.

Even worse than Rogers' reliance on initial early public reports, he or Time Magazine are using the term ‘cyberwar’ to describe this attack. That is simply dangerous and misleading. If this is a group of computer criminals acting on their own, it sets a dangerous precedent that a few random people [could conduct war](#). Such terms, when used in Congress, can invoke the wrong image of what is really

happening, and lead to an over-reaction in U.S. response. That could lead to knee-jerk legislation or worse.

Following up on the legal aspect of the breach, David Boies, a lawyer for Sony, [has sent a firmly worded three-page missive](#) to several media organizations including the New York Times stating that the leaked documents are “stolen information”. He goes on to demand that if a media organization has acquired them, that they be destroyed. His letter states:

“[Sony] does not consent to your possession, review, copying, dissemination, publication, uploading, downloading or making any use [of the information].” — David Boies

All of this comes days before the eighth leak of data from the Guardians of Peace, titled “GOP at Christmas, Part 2”, published earlier today (Note: yesterday’s disclosure was titled “Gift of Sony for the 7th Day – GOP at Christmas” making today’s release ‘Part 2’). Like previous leaks, the data has been made available via several bittorrent trackers, and uploaded to [RapidGator](#) and [TurboBit](#), where it was subsequently removed. Given the pattern of the data being removed so rapidly from various file sharing sites, it is pretty clear that they are either monitoring for Sony-related data being uploaded, likely to avoid legal issues, or receiving take-down requests from Sony.

Today’s leak centers around the email spool of [O’ Dell Steven](#), Senior Vice President, International Distribution for Sony Pictures Releasing International. The leak comes with two short messages for Sony Pictures Entertainment and Sony’s staff further warning them about what is to come, if their demands are not met:

Message to SPE

The sooner SPE accept our demands, the better, of course.

The farther time goes by, the worse state SPE will be put into and we will have Sony go bankrupt in the end.

Message to SPE Staffers

We have a plan to release emails and privacy of the Sony Pictures employees.

If you don’t want your privacy to be released, tell us your name and business title to take off your data.

The attackers claim that Sony staffers can opt-out of the upcoming leaks, which may be a ploy to engage employees. It will be interesting to see if they follow through, or even if they actually monitor the email addresses provided.

A quick analysis of the leaked mail spool (spodell.ost) shows that it is 5.53GB uncompressed, and contains over 72,900 emails spread across 7 primary folders. A bulk of the emails (54,793) are in the ‘Sent’ folder going back to May 20, 2008, with 12,414 in the inbox, and 4,276 deleted. As with previous disclosures, the topic of piracy seems to be front-and-center, specifically related to cinemas responsible for allowing camcorders to record movies in India, Taiwan, Japan, Brazil, Australia, and others.

Cyber Insurance, Copyright, Parody (December 15)

Today brings us a wide variety of updates and perspective for the ongoing Sony breach and resulting fallout. In no particular order...

More journalists have acknowledged receiving the three-page missive instructing them not to publish details from the leaked data, as mentioned in yesterday’s update. Brian Krebs writes about his [“cease and desist” letter](#) in an article titled [“In Damage Control Sony Targets Reporters”](#). Krebs cites an analysis by UCLA law professor Eugene Volokh who [goes into detail on if Sony has a legal leg to stand on](#) in pursuing journalists. TechDirt, [who offers commentary](#), says that this is a bad move for Sony and points out the curious use of “stolen information” versus “Stolen Information” throughout the document. As for Krebs, like other journalists he plans to continue on and will not be deterred by the letter, saying:

While I have not been the most prolific writer about this incident to date, rest assured such threats will not deter this reporter from covering important news and facts related to the breach. — Brian Krebs

As more news of the fallout comes to light, the topic of data breach insurance (aka ‘cyber liability’ aka ‘cyber insurance’ aka other terms) has finally come up. Steve Ragan at CSO [published a well-researched article to this effect](#), saying that leaked documents show Sony Pictures has “upwards of \$60 million in cyber insurance coverage” and then questions if it is enough. Per the article, it goes on to say that after Sony Pictures was breached in 2011, the company “made a claim of \$1.6 million in damages with Hiscox, their cyber insurance carrier at the time.” That damage figure was calculated after the disclosure of 37,000 people’s personal information, making the new breach potentially staggering when it comes to a monetary damage assessment.

[CNN reports reports today](#) that the leak also included an early version of the screenplay for the upcoming [24th James Bond movie titled “Spectre”](#). The producers of the film, [Eon Productions](#) have [posted a statement on the official movie site](#), warning the masses that publishing the script violates copyright law. While this may seem to bleed into the last few days of legal threats, note that copyright law is more straight-forward and has considerable history behind it with regards to demanding takedowns. For example, in the late 90s, many web sites that were compiling lyrics to popular songs received takedown requests from music artists, producers, and media companies citing it violated copyright. Eon Production’s statement hinges on this very point:

The screenplay for SPECTRE is the confidential information of Metro-Goldwyn-Mayer Studios and Danjaq, LLC, and is protected by the laws of copyright in the United Kingdom and around the world. It may not (in whole or in part) be published, reproduced, disseminated or otherwise utilised by anyone who obtains a copy of it. — Eon Productions

With any breach of this magnitude, there are countless media outlets that cover the event in some fashion. Fortunately for the public, most of this coverage is relatively well done and offers a more classic news style, looking for a balanced narrative. Unfortunately, there are always some outliers that go way too far, offering commentary or analysis that is absurd and that we desperately wish were hyperbole. Today’s outlier comes from notorious DJ Howard Stern who likened the attack on Sony to 9/11. [According to the NY Daily News](#), Stern recently quipped:

This attack is no different than a 9/11-type attack. They stole this material. It probably was North Korea. They want to f-k with Sony. They’re really pissed off. It’s outrageous. The president should have announced immediately we’re under attack... — Howard Stern

To this we can only state that such comparisons are an absolute insult to the victims of the 9/11 attacks, and ultimately only serve to hurt Sony as it further polarizes them in the public’s eye. Some are already speculating if this is a [“PR car crash from which company may never recover”](#). Consider that we have seen less than 10 leaks including a small number of executive mail spools. If the Guardians of Peace truly have over 100 terabytes of stolen information and plan to leak more every day until Christmas, there may be a wide variety of further damaging details to come. Finally, some have moved on to the unofficial sixth [stage of grief](#) (humor or parody) and are turning to comedy after shock and acceptance. [One such remark](#) was via a reddit ‘Showerthoughts’ post suggesting that “Sony should make a movie about the Sony hacks.” Well, someone else has [delivered a parody trailer already](#). Perhaps the healing can really begin.

Lawsuits, Terror, War, and we hope Hyperbole (December 16)

It seems like each day the issues surrounding the Sony breach grow considerably, and it isn’t just from the leaked data. As more people begin to contemplate the breach, as Sony reacts to different aspects of it, and the logical fallout happen, a world of perspective emerges.

Given the large number of issues surfacing, we will try to keep this as brief as possible. That said, this may be a substantial update. In no particular order...

First up, [Steve Ragan reports at CSO](#) that some of the leaked data may fall under Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations, which covers the security and/or disclosure of Protected Health Information (PHI). [Per Wikipedia](#), citing Title 45 of the Code of Federal Regulations, PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. Ragan's article goes on to quote from the letter Sony sent to affected employees and give more details about the data leaked ([Full copy of the letter in PDF](#)). [Seth Rosenblatt at CNet writes about](#) two former employees who are suing Sony over the breach of healthcare information. Based on a quick [PACER](#) search, the case was filed yesterday in the District Court for the Central District of California (Western Division – Los Angeles) and has been assigned case number 2:14-cv-09600-RGK-SH.

After more than a week of veiled threats from the attackers, Guardians of Peace, Sony has made its first move that appears to cater to their demands. [According to NPR](#), Seth Rogan and James Franco have canceled several media appearances that were to promote their upcoming movie, "The Interview". Despite this shift in media promotion, the movie still appears to be scheduled for release on December 25th. A second potential move, [according to NY Daily News](#), is that Sony Pictures executive Amy Pascal may be fired to send a message. After her email was leaked by the GOP, a wide variety of embarrassing emails were published including racially charged content, insulting high-profile actors, and more.

Speculation has been flying over how long the GOP had access to Sony's networks. While the general consensus is "about a year", [Network World reports](#) that it may have been in February. According to their article, Sony used SpiritWORLD as a central system for distributing their media, but admit the system may have been compromised and malware uploaded. The compromise resulted in personal information of 759 people being exposed, including name, address, and email address. The article goes on to say that Sony's VP of legal compliance admitted to the hack, but recommended the individuals not be notified. It's unclear at this time if the decision to forego notification is in keeping with Sony's statutory obligation to do so.

Attribution in computer compromises is a surprisingly complex task that may ultimately never be definitive. While an attacker may appear to come from an IP address belonging to a certain country, you can't simply assume the attacker originated there. Or that the country sponsored the attacks, even if it actually did. Savvy computer criminals will compromise multiple low-end machines and use them as bounce-points, diverting their traffic through them. An administrator or security professional looking at logs on the compromised system will only potentially see connections from that one IP address, not where the attacker actually came from originally. The early talk about North Korea was speculative at best, and appears to have been debunked since (see previous updates). Now, the blame shifts again, this time to China.

In what ultimately amounts to more speculation based on a few tenuous facts and an unnamed source, Deadline Hollywood is reporting that the attacker could be China. Their unnamed source tells them "Mandiant has investigated so many Chinese attacks. It's kind of their forte." True, but as several security professionals have commented in the past 24 hours, "because Mandiant is involved, it must be the Chinese? That's a pretty big stretch." While Mandiant is known for their investigations into alleged state-sponsored Chinese hacking teams, many wonder if they have become the proverbial hammer that only sees a nail. It should also be noted that while they have that reputation among some, Mandiant has investigated many hacking teams from other countries.

Despite that speculation, perhaps that is why we are now hearing more rhetoric regarding the breach, specifically suggesting that the attack on Sony is an "act of war". Michael Kelly and Armin Rosen at [Business Insider make their case](#) that it should be, despite quoting the widely accepted [Tallinn Manual on the International Law Applicable to Cyber Warfare](#) which clearly states that the attack on Sony does not meet the criteria for an act of war. They go on to quote noted security expert Dave Aitel, an ex-[NSA employee](#) and current CEO of [Immunity, Inc.](#), who says:

"We need to change the way we think about cyberattacks. In many cases, these aren't 'crimes' — they're acts of war. A non-kinetic attack (i.e., destructive malware, destructive computer network attack) that causes just as much damage as a kinetic attack (i.e., a missile or bomb) should be viewed at the same level of urgency and need for US government/military response." — Dave Aitel, Immunity Inc.

The first question this brings to mind is if malware "causes just as much damage as a [missile or bomb]". For the average citizen, especially the majority not affected by this breach, they would likely argue against such claims. The second issue that comes to mind is that Aitel suggests there should be "firm diplomatic repercussions for these types of attacks." Perhaps, but Aitel also believes North Korea is behind this according to the article, while the FBI says they are not involved. Given the list of possible suspects named so far, which includes North Korea, China, and an independent group of non-state hackers, such "diplomatic repercussions" could be a disaster unless we have definitive attribution of the attackers, which we may never get.

As an example to the attribution problem, [Mario Greenly points out](#) that the first computer to seed data in the latest leak is hosted in or around Taipei, Taiwan. Does this suggest the attacker is located there? Or does it mean the attacker picked a compromised computer there to host the data, in an effort to mislead investigators? Given that a single botnet, which is a group of compromised systems controlled by a person or group, [can be as large as 450,000 systems](#), it isn't a stretch that skilled attackers could pick and choose which systems to use to hide their tracks, or throw off those looking for them. The most important part of the process at this point is to try to obtain positive attribution. Then, Sony can determine what legal remedies are available to them, or if this becomes a bigger issue that requires Government response.

Almost as if prompted, the notion that this is an act of war was further bolstered after the ninth leak released today, which included a message that hints at terror attacks. The GOP posted the following to Pastebin today which suggested there may be real-world terror attacks at theaters showing "The Interview" on Christmas day, likening the attacks to those on September 11, 2001:

[...]
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.)
[...]

Damon Beres at the [Huffington Post writes about this statement](#) and cites an unnamed Department of Homeland Security official who confirmed they are aware of the threat, but emphasized "there is no credible intelligence to indicate an active plot against movie theaters within the United States."

And finally, that brings us to the ninth leak posted today, titled "1st Christmas Gift, Michael Lynton". As the name suggests, this disclosure includes two files, both email spools (mLynton.ost is 864MB and mLynton1.ost is 1GB) for Michael Lynton, [Chairman and CEO of Sony Pictures Entertainment](#). The mails range between November 8, 2013 and November 22, 2014. Some of the folder names and mail count between both files:

- Inbox: 12,482
- Contacts: 7,085
- Calendar: 5,433
- Deleted: 6,966
- Lost & Found: 12,629
- Drafts: 77

It should be noted that these spoofs are almost half the size of previous leaked email spoofs, and neither file contains a 'Sent' folder. Oh, one last thing... are the [GOP on Twitter](#)? We remain skeptical for now.

Leaks, Blame Game Redux, and Caving In (December 17)

Today's round-up of post-breach fallout is diverse. Points of interest:

As expected, many more details have emerged from the leaked mail spoofs. One little bit that stood out as interesting takes us back to 2013 when a story broke about Facebook offering as much as [\\$3 billion to acquire start-up SnapChat](#). [According to BusinessInsider](#), it turns out that several mails were exchanged between SnapChat CEO Evan Spiegel, SnapChat board members, and Sony. Now that those mails are public, it offers more insight into what is still considered to be one of the craziest IT acquisition deal rejections in history.

The second interesting thing to come from the leak are the [Motion Picture Associate of America's](#) (MPAA) apparent plans to try to negatively impact the Internet by attacking DNS servers. [According to The Verge](#), the tactic was first proposed as part of the now defunct [Stop Online Piracy Act](#) (SOPA), but the MPAA is still looking for legal justification to take this route in efforts to curb online piracy.

So far, we've heard theories that North Korea, China, and a group of non-state actors were involved in the breach. The latest theory [comes from the Hollywood Reporter](#), in which they outline an interesting coincidence. One of the emails allegedly sent from the Guardians of Peace came from an account configured with a 'real name' of "Nicole Basile". That name is the same as an accountant who worked for Sony in 2011, [according to LinkedIn](#), and a [payroll accountant on at least one Sony production](#). Of the various mails received by RBS claiming to be from GOP, that name does not appear in any of them. Of all the names we received, none appear to match current or past Sony Pictures employees. As it is, this is a pretty tenuous link given the email spoofs leaked contain email received in November, 2014, two or more years after Basile worked there.

In addition to the series of compromises in 2011, more information has emerged regarding a compromise of the Sony corporate network in 2013 [according to Bloomberg](#). While details are sparse, the attackers were never identified but allegedly stole "gigabytes of data" several times every week for a period of time.

The biggest news today centers around the decision of several theatre chains canceling the movie premier of 'The Interview'. [According to CNN](#), AMC Entertainment, Regal (RGC), Cinemark (CNK), Carmike Cinemas (CKEC), Bow Tie Cinemas and Southern all dropped the movie that was to open on December 25th. This prompted Sony to officially cancel both the [New York premiere](#) and the general release as well, according to a [Sony statement posted by Mark Day](#). In the statement, Sony refers to the attack against their network as "unprecedented" even though there is [clearly precedent](#) for such large scale intrusions. Roger Grimes at InfoWorld also [makes this point in an article](#), speaking from his own experience performing computer security reviews after attacks.

The cancellation of a major studio picture is unexpected, and potentially sets the wrong precedent. As [Steve Ragan writes](#), this basically shows that any group of attackers can make a veiled threat against a studio and theaters, and potentially cancel or disrupt the release of a movie. While many people think it is overly cautious, they also have to admit that theater patron safety would have to come first if they were making the decision. On the other hand, [many people took to Twitter](#) calling out theater chains and Sony as "nutless weasels", asking if all releases would be run past North Korea, and saying that their decision "appeases terrorists". Producer [Judd Apatow was also vocal](#), saying the choice was "disgraceful" among other things.

Attribution is Hard, the Guessing Game, and Perspective (December 18)

We have brought up the issue of "who is to blame" in the Sony hack several times. Original reports indicated North Korea was likely behind it. Then [we heard no, they were not](#). Some [speculated China was involved](#), simply because Mandiant was called in by Sony. Others suggest this is a group of individuals, with no state-sponsorship, using the political climate to throw off would-be investigators. Now? We're back to the beginning, with North Korea being named as 'definitely' involved. There's only one problem at this point...

Yesterday afternoon, news outlets all over started reporting that the U.S. is blaming North Korea for the attacks on Sony. These accusations are all based on what appears to be a wide variety of unnamed "officials" with no indication that they are in a position to know anything about the breach. The [New York Times article](#), which appears to be a central source of the accusations, says "administration officials" among other terms, but again do not qualify why said officials would have any specific knowledge of the investigation. That article [has been dissected to a degree](#) showing how the firm title accusing North Korea buckles under subsequent observations and quotes. Ultimately, we have a named FBI official in a position to have knowledge of the investigation on record saying it was not North Korea, and we have an unknown amount of unknown officials that may or may not have knowledge of the investigation. Yet, the prevailing thought based on watching social media is that most people believe North Korea was behind it.

[According to the Washington Post](#), who spoke with an "intelligence official" who was "briefed on the investigation", they are almost certain hackers working for North Korea were behind the attack. To counter this, we have pieces from [Kim Zetter at Wired](#) and [security professional Marc Rogers](#) who make a case that North Korea is likely not involved. One point that can't be said enough is that "attribution is hard" given the nature of computer intrusions and how hard it is to ultimately trace an attack back to a given individual or group. Past attacks on Sony have not been solved, even years later. The idea that a mere two weeks into the investigation and there is positive attribution, enough to [call this an act of war](#), seems dangerous and questionable.

Intelligence officials believe with "99 percent certainty" that hackers working for the North Korean government carried out the attack, said one individual who was briefed on the investigation and spoke on the condition of anonymity. — Washington Post

At this point, it certainly could be North Korea. Or China. Or a group of people with no political affiliation, laughing at their tricks that have thrown the rest of society for a loop. As we have said before, it would be best if we reserve judgement until there is a documented forensic trail that truly establishes some level of attribution with certainty. At that point, Sony Pictures and the U.S. government can determine the best way forward. As [Jason Koebler at Vice writes](#), "Reaction to the Sony Hack Is 'Beyond the Realm of Stupid'" and has a wide variety of points that put the events in perspective.

Following up on the "fallout" angle, it appears that this attack has resulted in the cancellation of two movies. The first movie canceled, 'The Interview' has been extensively covered in the media and is accompanied by diverse commentary saying it was the right thing to do or it was caving in to terrorist demands. [According to The Wrap](#), the second movie cancelled, not even in full production, is titled "Pyongyang" and was to star Steve Carell. Produced by company New Regency and directed by Gore Verbinski, the story is based on a graphic novel and follows a Westerner that is accused of espionage in North Korea. According to the [Internet Movie Database](#) (IMDB), it was also to be a comedy.

While the technical investigation into the breach is carried out, [Tech Crunch reports](#) that Sony is being forced to embrace legacy

technology such as faxes and face-to-face meetings. Given that the compromise appears to be extensive, companies cannot assume that the attackers have stopped accessing the network. To err on the side of caution, they must assume that just about every device on their network is compromised.

Finally, in the wake of the North Korea guessing game, we'd like to offer a few points of perspective. When the Guardians of Peace (GOP) called for the cancellation of 'The Interview', no one thought it would work. Yet it did. Since the demands of the GOP centered around that and the demands have now been met, [Jake Kouns asks](#) if that means the leaks are over? [Cyber War News reminds us](#) that one hack led to one movie being cancelled and the world cares deeply. Yet every day, hundreds of companies are hacked leading to tens of thousands of credentials being leaked. Despite that, no one cares. It is interesting how a large media company can have such influence outside the scope of their usual means of influence (i.e. movies). Despite the veiled threats from the GOP suggesting December 25 may see "9/11 type attacks", President Obama is saying there is no credible threat and encouraging Americans to go to the movies [according to CNN](#). Finally, [Mitt Romney chimes in](#) with this great idea:

.@SonyPictures don't cave, fight: release @TheInterview free online globally. Ask viewers for voluntary \$5 contribution to fight #Ebola.

Unfortunately for Romney and those supporting his idea, a CNN email flash arrived shortly after the Tweet saying "Sony Pictures has no further release plans for 'The Interview,'" a company spokesperson tells CNN's Brian Stelter, discouraging speculation that it might release the movie digitally."

Proportional Response, Fallout, and Politics (December 19)

Every day that passes, the amount of news and commentary on the Sony breach grows. What started as a relatively simple breach has ballooned quickly. There are aspects of the breach fallout that we simply have not seen before. The victim caving to the demands of the alleged attackers, a "new" nation-state not thought to have this capability years ago being blamed, and knee-jerk yet serious talk from politicians calling this "an act of war" while the U.S. government seriously discusses how we react to the threat, even though we haven't necessarily identified said threat. This is a chaotic and fluid situation developing every day.

When a breach like this becomes mainstream, there is a growing concern over public outreach from the alleged attackers. Previous disclosures came in a fairly routine format, from a new email address, and had certain characteristics as far as the communication contents. This leads everyone to wonder if a new disclosure via one of the usual channels is actually legitimate. For example, a Pastebin appeared yesterday purporting to be the Guardians of Peace (GOP) claiming the "ban" is over:

This is GOP.
You have suffered through enough threats.
We lift the ban.
The Interview may release now.
But be careful.
September 11 may happen again if you don't comply with the rules.
Rule #1: no death scene of Kim Jong Un being too happy
Rule #2: do not test us again
Rule #3: if you make anything else, we will be here ready to fight
This is Guardians Of Peace.

While this may appear to have the same characteristics as the previous disclosures, several journalists that have periodically received previous communications [feel this one is not genuine](#). Moving forward we must be cautious about not only attribution of the attackers, but attribution of those [claiming to be or represent them](#).

The biggest development today is that the Federal Bureau of Investigation (FBI) has [firmly come out and declared North Korea was behind the attack](#). This follows a string of articles citing unnamed "officials" saying it to news outlets, but not on record. The announcement says that their investigation has turned up three major points of evidence linking the attackers to North Korea. It should be clearly noted that the FBI refers to the attackers as from North Korea, and that the North Korean government is responsible for these actions.

As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. — FBI Statement

Unfortunately, they have not released any evidence to back these claims. While the FBI certainly has many skilled investigators, they are not infallible. Remember, this agency represents the same government that firmly stated that Iraq had weapons of mass destruction, leading the U.S. into a more than ten year conflict, which was [later disproven](#). Journalists that have been following the story closely are already skeptical of the announcement. As [Kim Zetter from Wired asks](#):

Question is, how do we know the South Korea attack was North Korea? If a one-time communication between NK and malware is all they have... — Kim Zetter

Analysis of both the attack on Sony, and the subsequent evidence recovered and eventually disclosed by authorities will be ongoing. Sony is a multi-national company with computer resources spread throughout the globe. Analysis of a compromise of this magnitude will be a long process, especially given all of the unknowns. Even worse, some external analysis of the breach is being digested by Sony staff, as it is [the first time they have heard of it](#). RBS has also been asked for comment by a third party about information in the email spools that show compromises of Sony servers in Japan and Germany earlier this year, if it could be the precursor to this breach. At every point of the analysis, we have to remember that ultimate attribution is problematic, and [has been for a long time](#).

Of course the FBI can't divulge all of their evidence this early into an investigation. However, publicly attributing this attack to a foreign government when some politicians are bantering about this being an act of war is dangerous for everyone involved. TechDirt reminds us of the ["ridiculousness of turning the Sony hack into the 9/11 of computer security"](#). Further, [Martyn Williams at PC World makes several excellent points](#) that remind us to be skeptical, as some evidence doesn't add up and it is convenient to blame North Korea. Finally, there is [speculation](#) that blaming North Korea and calling this war may be the result of [pressure put on cyber command to justify their increased budget](#). Fortunately, at least one senior official is [keeping a more reserved opinion](#) and not calling the attack on Sony an act of terrorism.

The next step in all of this is the U.S. response to the intrusion. As rhetoric continues to fly around about us ["losing the cyberwar"](#), one phrase we continue to see is ["proportional response"](#). In short, how can the U.S. respond to this attack on Sony in a proportional manner, without escalating the issue. Some will no doubt call for an increased response to flex our own digital muscle, while others will call for a more reserved approach. One problem is that we can't simply [issue economic sanctions](#) against North Korea as they are already well isolated. Diplomatic punishment is a token gesture at best. Whatever we decide, we must also consider the precedent it sets, as the U.S. was [complicit in state-sponsored attacks on Iran's nuclear program](#) via computer intrusion, that has been deemed an [illegal "act of force" by some](#).

A spokesman from the White House is calling this a ["national security matter"](#) but every official seems to be forgetting that Sony is a multi-national company based in Japan. Where is Japan's statements or response to this attack on one of their companies? Either way, this has been a serious wake-up call to the U.S. administration and we are late to the game in calling for a ["doctrine of deterrence to cyber"](#)

[attacks](#) .

For those who are surprised to hear that North Korea has this type of capability, regardless of their alleged involvement in the Sony hack, it is important to note that most first-world countries have maintained government run hacking teams. While “[Bureau 121](#)” is just getting on the public’s radar as a result of recent incidents, remember that [China’s PLA Unit 61398](#) has been in the news on and off as possible perpetrators of various hacks. The U.S. is no exception, as different agencies and the military maintain their own groups of hackers for the same type of activity. The [National Security Agency’s TAO group](#) came to light last year via the [Edward Snowden leaks](#) and showcased their wide range of technology for snooping. This is also why it is important to have a measured response to the Sony breach as it is quite clear that most governments don’t maintain these teams just to sit on the sidelines.

Moving on, the volume of news and commentary over this incident has become staggering, as one might expect. We are certainly in some level of uncharted water at this point. To better cover the latest news, we will have to resort to bullets.

- [The AntiWar Blog reports](#) that emails from the Sony leak show the U.S. State Department heavily influenced the ending of the movie “The Interview”, “so as to encourage assassination and regime change in North Korea”.
- More lawsuits have been filed against Sony. We previously covered the first lawsuit filed by ex-employees over health information being disclosed. [The second](#) comes from two more former Sony employees and the [third class action suit](#) from two more former employees. Perhaps the six should join forces?
- The [Hollywood Reporter writes](#) that South Korean activists plan to drop copies of “The Interview” onto North Korean soil via balloon, a tactic they have previously used to deliver other items.
- After movie theater chains dropped The Interview from their upcoming lineup, [one Texas theater refused](#) to “let terrorist hackers win” so they planned to give out free toy guns and show [Team America: World Police](#). Unfortunately for them, [Paramount quickly banned showing the movie](#). Is the decision political or financial, as they would likely not profit from the showings?
- The past few days have seen coverage of this incident expand rapidly as the ramifications develop. BBC has started [considerable coverage](#) of the events, as well as outlets all around the world. RBS executives travelling yesterday observed that every airport they visited was showing CNN, who was giving it non-stop coverage. One RBS employee across seas noticed that even the local news channels were giving it heavy coverage.
- Perhaps not all Sony employees got the message about “The Interview” being cancelled? A day after that decision was made and covered widely in outlets, [E! Entertainment reports](#) that a new trailer for the movie was posted to the official Sony YouTube page. Shortly after their article landed, the new trailer was made private.
- As with any big event, the Twitterverse expects a variety of parody accounts to add levity to the situation. The [‘Official GOP’ Twitter feed delivers](#).
- [Deadline Hollywood reports](#) of an interesting sub-story about George Clooney starting a petition to encourage Sony not to give into the hacker’s demands. Despite his clout, not a single industry leader or executive would sign it. The article shares extensive commentary from Clooney as well as a copy of the petition.
- Security researcher “Krypt3ia” [offers amusing commentary](#) of the “winners and losers” in this Sony debacle.
- As the commentary about these events continues to pour forth, we all wondered when [Godwin’s law](#) would rear its ugly head. Apparently, 24 days later as seen in [this blog by Barbara Lippert](#).
- As previously reported, the leaked emails show that MPAA was working with major studios on “Project Goliath”, an attempt to revive industry-favorable legislation. The project also specifically targeted Google in their plans for increased anti-piracy actions. Google has announced it is not happy with the MPAA and their plans in this [blog by Kent Walker](#), SVP and General Counsel at Google. The [Hollywood Reporter offers commentary](#) on all of this.
- A Sony-owned web site, [sonymoviechannel.com](#), was [defaced](#) by a group called [“Middle East Cyber Army”](#), showing that Sony still has a long way to go in the realm of network security.
- [Perspective from Chris Rock parody account](#), who reminds us that people saying Sony’s choice to pull “The Interview” means the terrorists won have forgotten that we have been taking off our shoes at airports for 14 years.
- [President Obama has stated](#) that he feels Sony pulling the movie was a mistake, and has since encouraged the public to go to movies. His comments mimic many others in that their actions set a dangerous precedent, where we can be too easily influenced by bad actors.

Attribution Dilemma Continues and Weekend Roundup (December 21)

The attribution dilemma continues and more confusion seems to be added every day. Since the FBI statement about the Sony hack being linked to North Korea, more people are [doubting the forensic evidence really points to them](#). With an official U.S. government statement blaming North Korea, their officials have [finally responded to the attack allegations](#) suggesting they were not involved and that a “[joint investigation](#)” would demonstrate that. [Dave Lee reminds us](#) that in 1998, the U.S. blamed a computer compromise on Iraq, but later came to light it was [actually a couple of teenager](#). This should serve as a not-so-gentle reminder that we must be prudent in assigning blame. President Obama has firmly stated that the attack on Sony is [not an act of war](#) at least. To make matters more confusing, the Guardians of Peace (GOP) have allegedly posted a new letter openly [mocking the FBI and calling them idiots](#). The GOP statement:

By GOP

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 success.

FBI is the BEST in the world.

You will find the gift for FBI at the following address.



Enjoy!

As before, the information and commentary about the Sony breach is staggering. For a quick Sunday summary, here are some of the points we found interesting:

- Is the [hacktivist group Anonymous entering the fray?](#) (Note that withholding 'The Interview' has nothing to do with the FOIA act, making this message suspect.) After 25 days, it seems they are by announcing a [new operation for vengeance against North Korea](#).
- [Ars Technica writes about](#) continuing analysis of the malware used to compromise Sony.
- [BBC reports](#) that Snapchat founder Evan Spiegel is "devastated" and "angry" that mails about his app were leaked.
- Information security professional [Stephen Cobb responds](#) to George Clooney's petition mentioned in yesterday's update.
- [The Daily Journal reports](#) that Sony faces lawsuit #4, this time from a former director of technology.
- [Dell Cameron reminds us](#) of this perspective: The U.S. Department of Justice argued in October that hacking a foreign country is not illegal. Consider that along with our response to allegations that North Korea hacked a foreign country (the U.S.).
- [VR-Zone reports](#) that NBC claims Sony's Xperia Z4 designs were in the leaked emails.
- [Left Wing Nation has posted an article](#) that includes 30 seconds of 'The Interview', specifically the scene in which Kim Jong-un dies. Note that the "Property of Columbia Pictures" at the bottom indicates this was a screener copy, generally released to media outlets for advanced reviews of a film.
- [Alex Marsh](#) reminds us that Sony has had [several rounds of layoffs over the last year](#) and we wonder how many of them cut into the IT or security staff. Not surprisingly, there is also a new opening for a ["Director of Vulnerability Management"](#) at Sony now. Someone who wishes to remain anonymous also points out that the Sony jobs site appears to have a 1999 era vulnerability, an old ASP.NET diagnostic page that reveals sensitive information about the system. (Note that the Sony job site appears to be hosed via [Technomedia](#), an [ISO 27001 certified company oddly enough](#).)
- Another bit of perspective: While everyone is still focusing heavily on the Sony breach, dozens of other companies and organizations have been compromised in the last few weeks. These include [an interesting compromise](#) at the [Internet Corporation for Assigned Names and Numbers](#) (ICANN) and a [huge breach at Staples](#) that resulted in details of 1.6 million credit cards being stolen. [Update: Staples was announced in October, but the news of how many compromised came this week.]
- After details of the MPAA's plans to attack Google were disclosed in the leaked emails, [Google has filed a lawsuit against the MPAA](#).
- And finally, after the back-and-forth from Sony about if 'The Interview' will be released, they appear to have settled on [releasing it via their own Video On Demand \(VOD\) service](#).

Holidays. A Time To Reflect (December 26)

When the Sony hack first came to light, many were asking if the data leaks were ever going to stop as they seemed to happen every few days and contained damaging information. While the original Pastebin has since been removed, there was even a threat of additional data leaks that would come during the Christmas time frame.

We are preparing for you a Christmas gift.
The gift will be larger quantities of data.
And it will be more interesting.

The gift will surely give you much more pleasure and put Sony Pictures into the worst state.

At this point, there have been no new data leaks related to the Sony breach since December 16th. This still suggests that the Guardians of Peace (GOP) were sincere in their claim that they would stop the leaks if 'The Interview' was not released on December 25. However, Sony ended up releasing it via Video on Demand (VOD) despite originally stating they would not release the movie at all. Does this mean that the GOP will resume leaks?

While no additional data has been released for analysis, there has continued to be a ton of developments in this case and more questions have been raised, rather than answers.

Even with the [FBI statements](#), there are [still serious debates raging](#) over who is behind this attack on Sony:

- [Brian Krebs provided a post that examines some compelling evidence from past attacks that has helped form the conclusion that North Korea is to blame](#).
- [Kurt Stammerger, a senior vice president with cybersecurity firm Norse said "Sony was not just hacked, this is a company that was essentially nuked from the inside"](#). While Norse is not involved in the Sony case, it has done its own investigation, and stated "We are very confident that this was not an attack master-minded by North Korea and that insiders were key to the implementation of one of the most devastating attacks in history". Stammerger says Norse data is pointing towards a woman who calls herself "Lena" and claims to be connected with the so-called "Guardians of Peace" hacking group. Norse believes it's identified this woman as someone who worked at Sony in Los Angeles for ten years until leaving the company this past May.
- [Marc Rogers](#) has had several posts about the issue of attribution and a good amount of [thoughts and now more evidence that points out that he believes NK was not behind the Sony hack](#).
- You can [listen to a debate between Dmitri Alperovitch of CrowdStrike and Marc Rogers of CloudFlare about North Korea's involvement](#).

[President Barack Obama has said the US is considering putting North Korea back on its list of terrorism sponsors after the hacking of Sony Pictures](#). A decision would be taken after a review, he said, calling the attack an act of cyber-vandalism, not of war.

- [Russia has offered sympathy to North Korea](#) amid the Sony hacking scandal, saying the movie that sparked the dispute was so scandalous that Pyongyang's anger was "quite understandable."
- North Korea has threatened unspecified attacks on the US in an escalation of a war of words following the Sony Pictures cyber-attacks. In a fiery statement, the North warned of strikes against the White House, Pentagon and "the whole US mainland".
- North Korea's shaky Internet infrastructure has been suffering from widespread outages this week, North Korea watchers said, who added that the network failures were highly unusual, even for the reclusive nation. The connectivity problems are coming just days after President Obama warned of a ["proportional response"](#) to North Korea. [According to Dyn Research, North Korea's Internet is currently showing intense instability](#).
 - [North Korea comes back online](#) and now many are debating who is responsible for the outage.
 - ["I'm quite sure that this is not the work of the U.S. government. Much like a real world strike from the U.S., you probably wouldn't know about it until it was too late. This is not the modus operandi of any government work," said Arbor's Dan Holden of the attack.](#)
 - Apparently the Lizard Squad, who has become rather well known for causing a lot of outages for online gamers, may be causing North Korea some issues as they imply that they have attacked NK. [A post by Dan Holden from Arbor, share some more information on the outages.](#)

Just as we have seen a ton of back and forth on who is believed to be responsible for the Sony Hack, we saw Sony also go back and forth on if they were going to release 'The Interview'. [Sony canceled the Christmas Day release of the film, citing threats of violence by the hackers and decisions by the largest multiplex chains in North America to pull screenings and then later said it has "no further release plans for the film."](#) And many people from all different backgrounds were [very unhappy with Sony's decision](#).

- Despite North Korea warning of 'grave consequences', Sony said on December 26th that they will screen the controversial film. [Lynton said: "We have not caved. We have not given in. We have persevered and we have not backed down. I would make the movie again. We would still like the public to see this movie, absolutely."](#) As of yesterday, the movie could be streamed via Youtube

- and several other services.
- While the major chains still did not show the movie, [there ended up being about 331 small cinemas that decided to show 'The Interview'](#). [The move was heralded as a free speech pitch](#) and appeared to be well received by the public. [One Texas theater's website was down, not due to a hack but overwhelming traffic.](#) "Our website is currently having some issues due to overwhelming traffic," says the theater. "Please be patient and feel free to swing by to pick up tickets." While it can be very hard to believe that so much damaging information would be leaked for a PR stunt, there are quite a few people that still believe exactly that, that [this whole thing was a major PR stunt](#). An interesting [story was posted that provided details on how the movie actually made it to theaters.](#)
- [Film industry website Den of Geek reports](#) that any kind of film release could be difficult until the hack is cleared up, saying: "even video on demand services are reluctant to carry The Interview, presumably for fear of finding themselves at the mercy of cyberterrorists themselves."
- Even with potential concerns, [the movie is now available online, streaming on Xbox consoles, Windows Phones, and Windows 8 computers, or on any other computer or smart device that has access to YouTube or Google Play.](#)
 - Microsoft said in a statement that it's basically defending anyone's right to see the movie in the U.S., but not endorsing its contents. "A cyber-attack on anyone's rights is a cyber-attack on everyone's rights, and together we need to defend against it," Microsoft [said](#).
 - Google posted a similar message on its official [blog](#), "Last Wednesday Sony began contacting a number of companies, including Google, to ask if we'd be able to make their movie, The Interview, available online," Google said. "We'd had a similar thought and were eager to help—though given everything that's happened, the security implications were very much at the front of our minds."
- While Apple has [yet to release the movie](#) on iTunes, even Sony has [setup an online method to view The Interview](#), all you have to do is give Sony your credit card information. [What could possibly go wrong?](#)
- Now that the Interview is being screened in some theaters, as well as available for [rental for \\$5.99 from Google on YouTube](#), many begin to wonder if we will begin to see the leaks start again in the near future. Whether the motivation for the Sony Hack was truly the film, or in an effort to just to keep up the rouse that The Interview had anything to do with it. The fact that no further messages have been posted with the movie already showing is already quite telling. Or perhaps the GOP are just enjoying their holidays.

A few others items of note:

- While everyone is focusing fully on Sony, many have overlooked a pretty substantial issue, as South Korea preps for cyber attack after recent [nuclear reactor data leaks](#). South Korea is investigating the [online leak](#) of partial blueprints and operating manuals for some of its nuclear reactors, as the perpetrator threatens to continue publishing data unless three facilities were shut by Christmas. While the leaker's identity remains unknown, it comes at a time that South Korea's anti-nuclear lobby is growing and becoming more active following the 2011 Fukushima disaster in Japan and a domestic scandal sparked by faked safety documents. It is important to note that the leaks also coincide with the Sony Hack.
- Lizard Squad has now turned their sights on the Sony PlayStation Network (PSN) and Microsoft's Xbox networks, [causing tons of new gamers getting their Christmas presents to be even unable to play them at all. In an interview with Lizard Squad](#) they explains that the task simply began for the laughs, but evolved into what they say is a real cause. Taking down Microsoft and Sony networks shows the companies' inability to protect their consumers' service reliability and instead shows their true vulnerability to such saturation-based attacks. Lizard Squad claims that their actions are simple, take down gaming networks for a short while, and forcing companies to upgrade their security as a result. When asked why Microsoft and Sony were both targeted on Christmas day, the group explained they felt it would anger and reach the largest amount of people – more people angry calls for a greater response from the companies; others were considered, including Nintendo, but no action was taken. The group is attempting to stress the point of computer security, while also getting a few "laughs".
 - [KimDotcom](#) appears to have wanted to play some [games on Christmas](#) and was unable to do so. He took to Twitter to offer Lizard Squad a deal involving his growing file sharing service MEGA which ultimately [Lizard Squad agreed](#). It appears this choice has enraged some users who see it as [caving in to the hackers](#), just like Sony did when they cancelled the movie. [KimDotcom](#) views the deal as a ["Christmas Miracle"](#).



- It appears that Sony's legal team [views using Twitter to post screenshots of their data](#), as the same exact thing ([and have the same issues with it](#)) as posting to a major news site or a blog post and they have also [threatened Twitter to remove the tweets](#) or face lawsuits.
- [An employee of Sony Pictures Entertainment outlines what they went through following North Korea's alleged cyber attack on the company.](#)
- According to uncovered emails, [a high-ranking CIA agent visited the Los Angeles headquarters of Sony Pictures Entertainment weeks ago](#), before the company realized its entire computer system had been [compromised by hackers](#) the FBI links to North Korea. Furthermore, comments were made that "Arrests Imminent" and that insiders were suspected of helping North Koreans.
- The Japanese government has announced it is planning to work on improving its cyber security, [specifically to boost internal](#)

[cybersecurity defense as the threat of foreign-based attacks reaches frightening levels](#). This also raises some additional questions as there were emails located in Leah Weil's email spool that shows that a vendor in Japan, [Sky Perfect TV](#) was breached at the start of this year resulting in access to personal information.

Where are we now?

- It is still very unclear who is responsible for the Sony hack. [Nicky Selby has a post](#) worth reading that really reminds us that no one has any evidence still.
- People are watching the movie, and [pirates are swarming over 'The Interview'](#) downloads. This also includes links posted on Pastebin as where to get the movie.
- There have been no reported issues at this point with any of the theatres that screened the movie.
- There have been no reported issues at this point with any of the VOD providers that are now selling or renting the movie.
- Sony executive [Amy Pascal made some initial comments on Dec 17th, and still has no plans from what we understand to step down](#) over the hack or her controversial statements pulled from her emails. No one from Sony has resigned or lost their job due to the breach at this point. As we saw with the Target breach, it was approximately six months later that we saw [Target CEO Gregg Steinhafel resigns as part of the data breach fallout](#).

Ex-Sony Employees, Russia, NK, Anonymous, and Sanctions (January 5th)

Rather than focusing on learning from the Sony hack and how companies can avoid these sorts of data breaches in the future, for most news agencies the main topic continues to be attribution. Over the past couple days, more and more articles have been published that are now pointing out issues with blaming North Korea as others keep blaming North Korea.

[The strongest argument that counters the official FBI report has continued to come from researchers at Norse](#) that allege that their investigation of the hack of Sony has uncovered evidence that leads, decisively, away from North Korea as the source of the attack. They have come out with more information that alleges that a group of six individuals are behind the hack, including at least one former Sony Pictures Entertainment employee who worked in a technical role and had extensive knowledge of the company's network and operations. It is important to note that Norse does not appear to have been consulted by Sony in the clean-up efforts, so their level of access and insight is not clear.

[The FBI granted a three-hour briefing with Norse to provide their information on the Sony Pictures hack](#). When asked about the meeting, the FBI declined to comment beyond a prepared statement which said, again, that they are confident that North Korea is behind the attack and there is "no credible information" to suggest otherwise. Further, a "U.S. official familiar with the matter" said after the meeting with Norse that the company's analysis "did not improve the knowledge of the investigation." Given the number of unnamed officials that are being quoted by every news outlet, as well as security companies that are pushing their own investigation without privileged access, all of this must be taken with a grain of salt.

[A post from Gotnews claims they have conducted an independent investigation](#) and identified two female persons of interest. The post is quite detailed and focuses on identifying a few individuals including ex-Sony employees that lines up pretty well with the claims from Norse. Ultimately, they say that they are continuing to investigate the theory of disgruntled former Sony employees may have joined forces with pro-piracy hackers, who have long resented the Sony's anti-piracy stance, to infiltrate the company's networks. If true, it goes against all of the claims of the FBI.

[According to computational linguists at Taia Global](#) who performed a linguistic analysis of online messages from the Guardians of Peace, they concluded based on translation errors and phrasing, that the group is more likely Russian than Korean. [Shlomo Argamon, Taia's Global's chief scientist](#), said he and a team of linguists had been mining hackers' messages for phrases that are not normally used in English and found 20 in total.

- Korean, Mandarin, Russian, and German linguists then conducted literal word-for-word translations of those phrases in each language. Of the 20, 15 appeared to be literal Russian translations; only nine were Korean, and none matched Mandarin or German phrases, reports [The Boston Globe](#).
- [The team also performed a second test on language used by hackers](#). They reportedly asked the same linguists if five of those phrases were valid in their own language. One was said to be a valid Korean construction, while three of them were consistent with Russian.

While CrowdStrike named North Korea being the culprit early on, they [continue to believe and be vocal that the hackers are indeed located in North Korea](#). This still does not speak to the issue if the hackers are just located there, or state-sponsored.

While many still debate who is behind the attack, North Korea issued a statement on its official state news agency denouncing Sony Pictures Entertainment's release of The Interview. [They called President Barack Obama the "chief culprit" who forced the production](#) [United States of being responsible for](#) KCNA news agency, a spokesman is w, saying: "Obama always goes one can post "crackpot theories"

Select at least one time that works for you

⌚ Duration: 30 minutes ⌵ Your time zone: GMT 0 (Change)

← February 2016 →

Finding first available date...

Retr

Your time zone

All times will be displayed according to your time zone:

Taiwan Taipei (GMT+8)

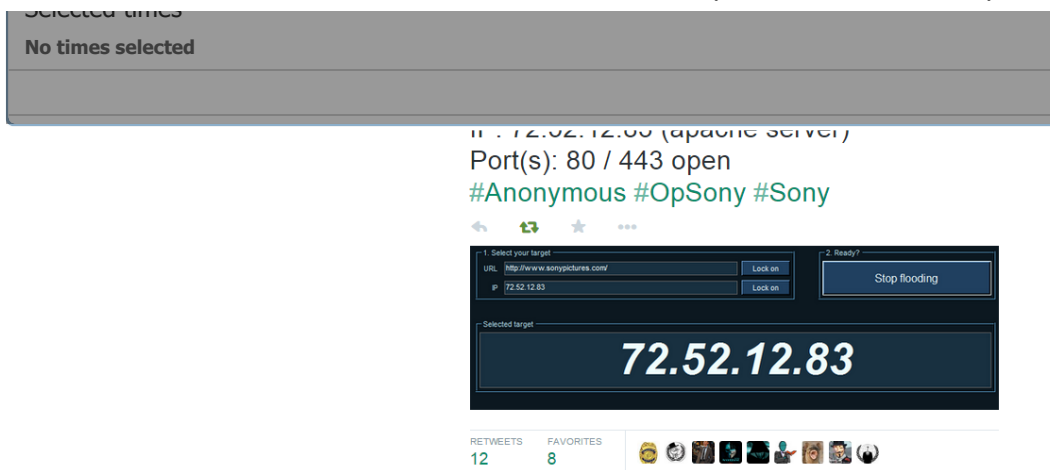
Next

Next

Selected times

ever; This was a publicity stunt truth. Anonymous never fights k, Anonymous will continue to

re posting a porn image from s Anonymous or those who wanted to pact the main sonypictures.com ed a picture of what appeared to be



Regardless of the continued attribution debates, [the US announced on January 2nd that they are holding North Korea responsible](#) for the cyber-attack on Sony Pictures Entertainment and President Barack Obama imposed [sanctions](#) on 10 individuals and three entities associated with the North Korean government.

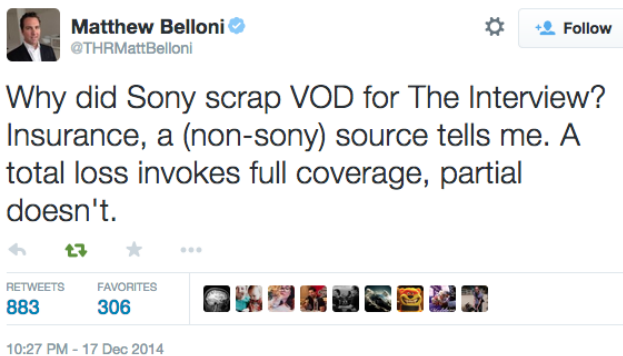
- On Jan. 2, the president ordered the seizing of property held by these individuals and organizations in the United States, a mostly symbolic action because few, if any, assets of those named in the order are likely located in the U.S.

In other news, another round-up of recent events:

- The recent developments on the [war against The Pirate Bay](#) created an interesting perspective, as [Sony's advertising campaign may have had their ads appear](#) on the very sites they so detest.
- Despite repeated threats of lawsuits against journalists publishing email content from the leaked email spools, we still have [a Twitter feed that continues to post content from them](#). Even worse, despite repeated tries from Sony to put a muzzle on Twitter, [the social media site apparently isn't budging](#).
- If you ever wonder how convoluted the entertainment business is, read about celebrity Amy Adams and [her scheduled interview on The Today Show](#) and consider the politics involved in that industry.
- As expected, the email leaks are causing more fallout as the disclosures expose salaries and other sensitive information. Both Sony employees and celebrities are "raging over" the disclosures, [which are likely to affect future salary negotiation rates](#).

Insurance Claims, Money and Pranks (January 6th)

There was some early speculation (as with so many other aspects of this incident) about the reasons for the movie being originally pulled from theaters. Money, as is usually the case, was also at the center of the decision allegedly and [Matthew Belloni tweeted that the reason was actually due to insurance](#).



Matthew's tweet would really have [nothing to do with typical Cyber Liability](#) or terrorism insurance for that matter. Most productions are insured against a variety of mishaps ranging from accidents taking place during filming to complete cancellation of the production. In fact, there is a sizable specialty market dedicated to the entertainment industry and the unique risks that go along with making any sort of show. It has come to light that Sony had coverage for The Interview through Allianz Canada, for an estimated \$38 Million dollars, for the production accounting and other risk management aspects of the project. Now that the movie has been released online and through some theaters, it will remain to be seen how the insurance claim, if submitted, will play out. Recovery under the policy may be more difficult since The Interview [quickly became Sony's most-downloaded title of all time, just four days after its release on 24 December, and has already made an estimated \\$15 million dollars](#). The movie was downloaded more than two million times as of 27 December, making back a third of its \$44 million dollar budget.

As we continue to report on the attribution debate (a recurring theme in this analysis), we saw over the holidays that anyone can easily post threats to sites such as Pastebin, and in some cases they are considered serious and not just pranks if that is the intention. [On December 20th, a threatening message aimed at CNN was posted to Pastebin](#), which had very similar wording used by a previous message believed to have been from the Guardians Of Peace.

By GOP

The result of investigation by CNN is so excellent that you might have seen what we were doing with your own eyes.
We congratulate you success.
CNN is the BEST in the world.
You will find the gift for CNN at the following address.



Enjoy!
P.S. You have 24 hours to give us the Wolf.

Four days after the initial post, [it was reported](#) in [multiple places](#) that the [FBI issued an internal bulletin warning in which they said the Guardians of Peace's threats "have extended to a news media organization."](#) It was believed that [this FBI bulletin was posted in connection with the Pastebin post](#), and further demonstrated that the vague threat was in fact taken seriously.

As soon as freelance writer and web designer David Garrett Jr. saw the link, he apparently notified the FBI that the Pastebin post was his and he also contacted some of the news sites reporting the threat to CNN to make clear he was the source of the post.



[After taking credit for the fake post to the media, the FBI and on Twitter](#), he received a phone call from a Knoxville FBI agent [asking him to come to agency headquarters on New Year's Day for an interview](#). [It appears that the fake post was only meant to be a prank as he stated](#), 'It was a joke. And to show that no one investigates anything. Everything is rumors. I had no idea it would be taken seriously.'

[Garrett was also quoted saying](#), "I think I just proved my point maybe news organizations should do a little bit more fact checking before they jump to conclusions". It has been pointed out that the [organizations investigating and news agencies reporting on the Sony hack still leave a lot to be desired](#).

More Attribution, Someone Is Wrong, and Lulz! (January 12th)

The attribution ~~conversation~~ debate just continues to go on! So much so that a few folks and even us here at Risk Based Security, have decided some Lulz (also known as laughs) are desperately needed to inject some levity into the situation.

Without further delay, we bring to you [Cyber War Attribution Bingo cards!](#) If you have every played [Buzzword bingo](#) then you are going to love this! You can play Cyber War Attribution Bingo with our standard card, or you can [generate your own cards for you and your friends!](#)

Attribution Bingo				
Vietnam	France	Saudi Arabia	Corp HackBack	Germany
Canada	Iraq	Poland	Script Kiddies	Russia
United Kingdom	Turkey		Insider Threat	Dreaded APT
Japan	Ukraine	North Korea	USA	Kazakhstan
Third Party	Romania	Brazil	China	Hacktivists

If a bingo game is not your thing and you are still trying to figure out who did it and why, then check out the [Sony Hack Attribution Generator](#). As the project team suggests, “Hit refresh on your browser and you’ ll get a new and exciting version of what happened complete with ‘evidence’ linking the crime to some random country.” Now you too can get a bit of enjoyment out of this mess.

While the [Sony Hack Attribution Generator](#) is amusing, [Kim Zetter makes an important point](#):



Kim Zetter
@KimZetter



Following

Note to members of media: the Sony hack attribution page is a joke; please don't write serious stories about it - sony.attributed.to



RETWEETS
28

FAVORITES
19



12:59 PM - 6 Jan 2015

With the Lulz behind us in this update, on to more serious thoughts with regards to attribution. Why do companies feel the need to do their own external research to determine who was behind the Sony hack? What do security companies gain from making claims that they have evidence and can prove who did it? Do these same companies benefit from sharing their research with the public of the US government? In many cases we know the answer is “media exposure” , but at some point that may backfire for many making claims.

When thinking about these points, it leads you quickly to try to understand the benefit versus the risk. We have seen over the past several weeks lots of individuals sharing their thoughts on the attribution issues, and many companies have made statements. Two companies, [CrowdStrike](#) and [Norse](#) have been at the front of the pack, making bold statements that are in direct conflict with each other; meaning one of them is right, and one is wrong.

CrowdStrike was one of the first companies to come out and declare that it was North Korea and support the FBI’ s claim. [In an interview on PBS Newshour, Dmitri Alperovitch describes how his company specifically tracks North Korea](#) and agrees that they were behind the attack.

JUDY WOODRUFF: So, Dmitri Alperovitch, to you first.

What do you make of the FBI finding — and the president referred to it — that North Korea and North Korea alone was behind this attack?

DMITRI ALPEROVITCH: At CrowdStrike, we absolutely agree with that. We have actually been tracking this actor. We actually call them Silent Chollima. That’ s our name for this group based that is out of North Korea. [sic]

Dmitri was confident in his statement and it didn’ t appear to be made as his personal opinion. It was a statement made about what his company does, and they believe it to be the case based on their intelligence gathering. [Dimitry came back on PBS Newshour the following week](#) after his initial statements, and when the host questioned him about previous statements he made saying it was “definitely, definitely North Korea” , he replied that he could speak for CrowdStrike who has done independent analysis. Here is the transcript:

Dmitri Alperovitch, you came on the program last week and you made the case that the president was correct and that the FBI was correct and this was definitely, definitely North Korea. Why so certain? Remind people, why are we so certain of that?

DMITRI ALPEROVITCH, CrowdStrike: Well, I can’ t speak for the FBI or U.S. government, who are very certain on this, but I can speak for CrowdStrike, who has done independent analysis of this attack.

And we have tracked it back to a group that has been active since 2006, primarily South Korea, military networks in South Korea, U.S. Forces Korea, the U.S. military installations, they are looking for specific information related to military planning, exercises on the peninsula, things that would be of natural concern and importance to North Korea.

We have also seen them engage in destructive attacks just like the Sony attacks, including the use of some of the same infrastructure. Some of the I.P. addresses that were used in the attack on Sony were also used in some of the past attacks. And parts of the malware, the malicious code that was used at Sony, has been shared across some of the previous attacks.

So we have seen them attack South Korea destructively in 2009, 2011, 2013, so we have a tremendous amount of visibility into this group.

Marc Rodgers, who works for a company called CloudFlare, [has been very vocal about the fact that he does not believe it was North Korea and no real evidence has been presented tying the country to the Sony Hack](#). Marc was on the same PBS Newshour segment and provided some counter thoughts, but he was more cautious with his statements. Additionally, he has not involved the company he works for by stating it was research conducted by them or their intelligence technology being used, which lead to his differing beliefs.

When asked what his issue was with the statements from Dmitri, who believes North Korea is behind the hack, he replied and ultimately stated *"until I see some tangible stuff myself, things more than just correlations between certain pieces of malware, I'm going to remain skeptical."* [You can listen to the debate for yourself or read the transcript.](#)

GWEN IFILL: Marc Rogers, that sounds pretty persuasive. What's your problem with that?

MARC ROGERS. CloudFlare: The biggest problem with this is, a lot of this information is based on evidence that isn't accessible to a lot of folks.

So if you look at the evidence that the FBI passed out in its notice, on its own, it's largely speculative and it's not backed up by any really solid evidence. There are hints, however, that there may be things like signals intelligence and other information that they can't disclose for national security purposes.

Unfortunately, without being able to access that information, there's no way for other security experts to really validate that. My colleague Dmitri from CrowdStrike has access to channels a lot of other folks don't have, so, to me, it's certainly interesting to hear the stuff that he's talking about.

But until I see some tangible stuff myself, things more than just correlations between certain pieces of malware, I'm going to remain skeptical.

As we have reported in several previous updates, Norse Corporation has stated that they do not believe it was North Korea. [Kurt Stammerger, a Senior Vice President with Norse, did an interview with CBS News](#) and was clear that his company has data that doubts some of the FBI's findings. Here are a few of the key statements that are of interest:

"We are very confident that this was not an attack master-minded by North Korea and that insiders were key to the implementation of one of the most devastating attacks in history," said Stammerger.

He says Norse data is pointing towards a woman who calls herself "Lena" and claims to be connected with the so-called "Guardians of Peace" hacking group. Norse believes it's identified this woman as someone who worked at Sony in Los Angeles for ten years until leaving the company this past May.

"There are certainly North Korean fingerprints on this but when we run all those leads to ground they turn out to be decoys or red herrings," said Stammerger.

So there we have it. [Norse](#) and [Crowdstrike](#), both of which are [highly funded](#), paint themselves as the next generation intelligence firms based on reading their website and press material. While we may never know who was really behind the Sony Hack, based on each of their statements which have left little wiggle room, one of the companies is clearly right and one is wrong. [Accuvant reminds us](#) that trying to determine attribution based on malware samples is often problematic.

If evidence ends up being released, and there is clear attribution, how will this impact companies like Norse and CrowdStrike that have made such bold statements? If a company making this statement is blatantly wrong, does that suggest threat intelligence they sell can't be trusted or relied on by corporations? Or when it comes down to it, will anyone care or notice long after these statements are made? Ultimately, will this fall under the statement that "there is no such thing as bad publicity"? As whether they were right or not, it does give companies who are willing to make bold statements a chance to [get their name out and make subtle or not so subtle pitches about their services and products](#).

DMITRI ALPEROVITCH: Well, Gwen, you can be absolutely certain that the companies that are involved in the distribution of this movie are taking this threat very seriously and working with companies like CrowdStrike to make sure that they're doing threat assessments in advance, because a second wave of attack may very well come and they need to be prepared.

While human nature craves to understand who the attacker was and their motive, we may never know who was behind the Sony Hack. If this is the case, it will rob us of the ability to see how it would play out for each of these companies. This might just have to be called a stalemate if there is secret evidence that will never be released.

[Even though the FBI did not believe the information that Norse](#) provided was enough to change their minds, that has not stopped Norse from continuing to be vocal and make their case. [They continue to believe that at least one former Sony employee was involved:](#)

Kurt Stammerger, senior vice president at Norse, which provides cyber intelligence to customers in financial services, technology and government, told The Huffington Post that the company remains "pretty confident" that "at least one ex-employee was involved, probably more" in the Sony hack.

As evidence, Stammerger said that Norse has samples of malware used in the Sony hack that existed as early as July, "completely in English with no Korean whatsoever." Sony credentials, server addresses and digital certificates were already built into the malware, he added.

While Norse and some others continue to put out a different story on the Sony Hack, the FBI is standing firm. [Lisa Monaco, a top White House homeland security and counterterrorism official even stated that groups that dispute their conclusion](#) that North Korea was behind the attack "don't have the information that the intelligence community and the FBI" has and that their assertions are "counterproductive." [We have also recently learned from current and former American officials, that the FBI and U.S. intelligence agencies](#) for years have been tracking the hackers who they believe are behind the attack on Sony. Furthermore, U.S. agencies have accumulated still-classified information that helps tie the hackers to the breach.

While the FBI apparently have conclusive evidence, the Obama administration has been tightlipped. [FBI director James Comey is standing by the bureau's conclusion, and has now offered up a few tiny breadcrumbs of the evidence that led to it, as reported by Wired:](#)

- Sony hackers sometimes failed to use the proxy servers that masked the origin of their attack, revealing IP addresses that the FBI says were used exclusively by North Korea.

- He named several of the sources of his evidence, including a “behavioral analysis unit” of FBI experts trained to psychologically analyze foes based on their writings and actions.
- He also said that the FBI compared the Sony attack with their own “red team” simulations to determine how the attack could have occurred.
- And perhaps most importantly, Comey now says that the hackers in the attack failed on multiple occasions to use the proxy servers that bounce their Internet connection through an obfuscating computer somewhere else in the world, revealing IP addresses that tied them to North Koreans.
 - “In nearly every case, [the Sony hackers known as the Guardians of Peace] used proxy servers to disguise where they were coming from in sending these emails and posting these statements. But several times they got sloppy,” Comey said. “Several times, either because they forgot or because of a technical problem, they connected directly and we could see that the IPs they were using...were exclusively used by the North Koreans.”
 - “They shut it off very quickly once they saw the mistake,” he added. “But not before we saw where it was coming from.”

Even with those statements from the FBI, [there are still some who are not yet convinced](#). Director of National Intelligence, James Clapper, has gone on the record going so far as to name the North Korean official who ordered the attacks. He recently stated that General Kim Youn Chol, essentially Clapper’s counterpart in North Korea, “must have ordered” the attack [according to The Daily Beast](#). That information was apparently based on a dinner between Clapper and Chol several months ago, [reports the Japan Times](#).

Perhaps those doubting will reconsider given the recent disclosure that the National Security Agency provided data and technical analysis for the U.S. government’s investigation, leading to the conclusion that North Korea was involved. [According to First Look Media](#), Admiral Michael Rogers said:

“We partner with the Department of Homeland Security and FBI in various areas and this is one such area. We specifically did—we were asked to provide our technical expertise. We were asked to take a look at the malware, we were asked to take a look at not just the data that was being generated from Sony but also what data could we bring to the table—here’s other activity and patterns leading up to it, what is this act really about? [...] We were part of a broad interagency effort, not in the lead role—the Federal Bureau of Investigation was the overall lead. Yes, we were part of a broad government attempt to understand exactly what happened.”

Regardless, an interesting article was also published that shared the [North Korea/Sony Story Shows How Eagerly U.S. Media Still Regurgitate Government Claims](#). This has no doubt been a contributing factor to the [back-and-forth attribution articles we continue to see](#).

If all else fails, consider the colorful [John McAfee who told Fox News](#) that social engineering is “how Sony got hacked” in a colorful on-air demonstration.

Catching Up and Closing Out! (February 22nd)

The amount of news around the Sony hack continues to be pretty intense, despite other [significant breaches](#) and [disclosures coming to light](#). But as far as Sony goes, it seems to mostly be the same topics rehashed over and over. Here is a round-up of some notable articles and topics that have come up over the past couple weeks that have yet to make an update:

- A single line of text on Google’s homepage read, “Our mission is to make the world’s information accessible — yes, even [Seth Rogen movies](#).” [The link, of course, led directly](#) to the Google Play store, where curious viewers can buy or rent *The Interview*, the Seth Rogen-James Franco romp that’s caused international brouhaha and become an unexpected symbol for freedom of speech.
- Any debate about Sony making moves in an attempt to call ‘The Interview’ a total loss should be put to rest, as they have [made over \\$36 million dollars](#) between the Video On Demand (VOD) and box office release.
- South Korea, the U.S. and Japan [will sign their first-ever trilateral intelligence-sharing pact](#) to better cope with North Korea’s increasing nuclear and missile threats, Seoul officials said Friday. If they are sharing on those threats, why not share a bit on digital threats too?
- Yoon Mi Rae is [set to take legal action against Sony Pictures](#) for using one of her songs in “The Interview” without Permission. This of course is an [amusing dose of irony](#) as Sony has heavily invested in anti-piracy efforts over the years.
- The LizardSquad, known for claiming to attacking both Microsoft and Sony game networks shortly after the Sony breach has run into trouble. Vincent Omari, who is allegedly linked to the group, has been arrested over unrelated computer crime. Now in the public light, he is [maintaining that his group had nothing to do with the attacks](#) on the game networks.
- As the Sony breach continues to unfold, [Richard Forno reminds us](#) that such incidents may see immediately action shortly after, but may also result in long-lasting national policy changes that impact us all.
- While many continue to debate who hacked Sony and why, others are using Sony as a lesson for all corporations regardless of size. This includes [“breach lessons we must learn”](#) as well as learning from the [“7 breach response mistakes”](#) Sony made.
- As expected, North Korea has responded negatively to the U.S. sanctions imposed against the country in the wake of the breach. Few, if any, thought that the sanctions would actually impact the Democratic People’s Republic of Korea (DPRK), but [officials from the country are certainly playing it up](#).
- Well over a month after the breach, Sony Chief Executive Officer Kazuo Hirai has [finally made a public statement](#), praising his company and employees as well as thanking those supporting Sony through this ordeal. Sony Pictures Chief Executive, Michael Lynton, [recently told Reuters](#) that the attack on his company won’t set the studio back.
- A security researcher examining the website of North Korea’s official news service, the Korean Central News Agency, [has discovered that the site delivers more than just the latest photo spread](#) of Democratic Peoples’ Republic of Korea leader Kim Jong Un inspecting mushroom farms. There’s a little extra surprise hidden in the site’s code—[malware](#). The news site appears to double as a way for North Korea to deliver a “watering hole” attack against individuals who want to keep tabs on the “activities” of the DPRK’s dear leader.
- A North Korean ambassador [insisted that his country had nothing to do with the massive computer hack](#) at Sony and has called for the United States, which has blamed North Korea, to provide evidence. In a rare press briefing last month, An Myong Hun, North Korea’s deputy U.N. ambassador, emphatically denied his country’s involvement. “My country has nothing to do with the Sony hacking. It is out of sense to do that, and we very want United States to provide evidence,” An said. He said that North Korea had offered last week to the United States to “undertake joint investigation” into the hacking scandal.
- Almost two months later, Sony Picture’s network is still down — and is expected to remain so for a few weeks, as techs work to rebuild and get it fully back online. [In a wide-ranging interview Lynton talked about the isolation and uncertainty](#) created by the attack and the unique position the company found itself in, in a case that’s undoubtedly being closely watched in boardrooms around the world. “We are the canary in the coal mine, that’s for sure,” Lynton said. “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. You’re on completely new ground.” “We were so taken by surprise by the events...that we didn’t have a plan at that moment to go forward,” Lynton said. For those following data breach news, we know that Sony is one of hundreds of such canaries.
- Apparently though, enough of the network is operational to allegedly allow [Russian hackers to infiltrate it](#) months after the initial breach. And because attack attribution is a forever changing game, we also now have [reports suggesting Russians were behind the breach](#), not North Korea.
- Hollywood drama followed the [Golden Globes](#) last month when top agency CAA demanded its famous clients not attend [Tina Fey and Amy Poehler](#)’s bash after the pair poked fun at the [Sony hacking scandal](#). Sources say CAA’s Bryan Lourd — who the Hollywood Reporter says has been serving as “privy counselor” to [Sony Pictures](#) Entertainment co-chairman [Amy Pascal](#) — had asked Globes hosts Fey and Poehler to lay off the hack. “CAA warned that they didn’t want jokes about the scandal,” [a source](#)

[told Page Six](#). "But Iina and Amy [who are not CAA clients] ignored their warning and made the jokes anyway, so CAA asked its own clients not to go to their afterparty."

- A UK man was [recently arrested over a denial of service attack against Sony](#). The 18-year-old was arrested at an address in Southport, near Liverpool. He is accused of unauthorised access to computer material and knowingly providing false information to law enforcement agencies in the US. The investigation was a joint operation between UK cybercrime units and the Federal Bureau of Investigation (FBI). Microsoft and Sony were attacked on Christmas Day, making it difficult for users to log on. The distributed-denial-of-service attack – which floods servers causing them to stop working – caused major disruptions.
- FBI investigating possible revenge hacking by U.S. banks. In 2012, the U.S. government announced that [Iran was behind the hacking of some of the country's largest banking institutions](#). The banks soon met with U.S. officials, where according to Bloomberg News, an individual from J.P. Morgan proposed that the banks hit back by taking down the Iranian servers." There were a lot of legal questions that came up, but somebody shut down the servers, and the FBI is trying to find out who did it." Bloomberg News reporter Michael Riley said. [This is interesting as it better frames the notion of a nation-state \(North Korea\) attacking a foreign company \(Sony\) as not an isolated event](#).
- Speaking of "hacking back", according to the AP, [sources tell them that the U.S. did not hack back against North Korea](#) after the Sony incident came to light. This may be true, but [other sources say that the NSA had already been in North Korean networks](#) as far back as 2010. This is also being [attributed to how the U.S. government was so quick to blame North Korea](#), citing evidence they couldn't share.
- In another dose of irony, National Security Agency Director Admiral Michael Rogers told the House (Select) Intelligence Committee that the [Sony hack was a "game changer"](#) for cybersecurity, and that North Korea was responsible. Months later, [Kaspersky unveils a damning technical report exposing a group they dubbed "Equation"](#) as being the most advanced hacking group known and responsible for more than 10 years of computer intrusions around the globe. It didn't take long for people to match up the report with the Edward Snowden leaked documents about the ["NSA Playbook"](#) to figure out that "Equation" is actually the NSA. It certainly changes how many view Admiral Rogers comments about the U.S. response to North Korea now that he is essentially saying that any other country can hold the US to the same standards and response.
- After the numerous lawsuits against Sony have been filed, some lawyers are now [asking to consolidate the similar suits](#) of (ex/current) employees looking for compensation. These cases will no doubt drag out over the coming years and be a constant reminder to Sony of what happened.
- While historically very close, Sony Pictures and the MPAA may be facing a breakup of sorts. Michael Lynton, Sony Pictures chairman, is not happy with the MPAA's response after the breach. [According to the NY Times](#), Lynton "cited the organization's slow response and lack of public support in the aftermath of the attack on Sony ..., as well as longstanding concerns about the cost and efficacy of the group."

The other lingering issues that tend to come up with such large-scale breaches include the fallout. Did the stock price get affected, and stay impacted by the event? What did it cost Sony overall? Was anyone at the breached entity held responsible?

As we have seen many times before and [discussed previously](#), the stock of the affected company did not continue to go down. Instead, it actually increased considerably after the breach. This typically happens due to a company being transparent to varying degrees, promising customers that they will improve, and appearing to take responsibility for the breach. The level to which a company does those things may vary greatly.



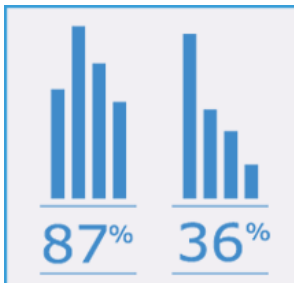
The question of overall damages has been a hot topic in the past few years, especially with the sharp rise in companies purchasing "cyber liability" insurance. While the insurance industry has been around for a long time, covering companies for these large breaches is still relatively new for most people. [Sony has postponed their 2013 earnings announcement](#), blaming the Sony Pictures compromise. In a filing with the Financial Services Agency of Japan, the company asked for an extension of a month and a half to file the report saying that a call would be held on February 4 to update analysts and investors on its outlook. After that call, Sony said that [the attack cost the company \\$15 million dollars](#). While that sounds like a considerable sum, remember that is less than half of what was earned from the movie "The Interview". Shortly after these damage figures were published, [Reuters reported](#) that Amy Pascal will "step down as co-chairman of Sony Pictures Entertainment ... to launch her own production venture on the studio lot with its financial backing." That certainly doesn't sound like she is being held responsible for her leaked emails that caused considerable drama, or the hack itself.

And with that we come to the end of our updates, [just as others have](#). We've said it before, and we'll say it again. We may never know the full story of what happened with Sony Pictures. While a lot of evidence points to North Korea, other evidence points elsewhere. More importantly, we have to remember that this was not necessarily a single group that was inside their network. Whether it was nation-state anger over a movie (doubtful), or part of a financially motivated intrusion (to hurt Sony, benefit the hackers, or both), we must also remember that [sometimes hackers just want to embarrass the victim](#).

As with most breaches, after the initial hype the interest dies off and the public moves on to other things. In this case, the public can latch on to one of the many options such as the recent [Anonymous versus ISIS battle](#), or the Anthem breach (which is getting far less press as compared to Sony). We're sure that Sony is perfectly happy with attention being focused elsewhere.

With a record-breaking 1.1 billion personal records compromised in 2014 across 3,014 incidents it is clear there has been no slow down of companies experiencing data breaches. Thanks for reading our Sony analysis and until the next time!

Filed Under: [Data Breaches](#), [News](#) Tagged With: [GOP](#), [Guardians of Peace](#), [Sony Pictures](#)



VuInDB

The most comprehensive vulnerability intelligence and third party library monitoring service available.



Cyber Risk Analytics

assessments.

Extensive database of data breaches with interactive dashboards, leaked email accounts and vendor



YourCISO

Affordable SaaS security solution providing a complete Information Security Program with access to a CISO.



Risk Management

improvement strategies.

Risk Based Security' s risk management solutions are a combination of data analytics, risk assessment and



Not just security, the right security

Richmond, VA
(855) RBS-RISK
[EMAIL US](#)

Resources:

- [VuInDB – Vulnerability Intelligence](#)
- [Cyber Risk Analytics](#)
- [ISO/IEC 27001:2005 Pre-certification Consulting](#)
- [YourCISO Services](#)
- [Security Intelligence Reports](#)
- [Risk Assessments](#)
- [Security Program Gap Analysis](#)

About Us

Risk Based Security, incorporated in 2011, offers a full set of analytics and user-friendly dashboards designed specifically to identify security risks by industry.

Risk Based Security is the only company that offers its clients a fully integrated solution – real time information, analytical tools and purpose-based consulting.

[\[Read More...\]](#)

Latest News

- [Fraternal Order of Police \(FOP\) Security Proves To Be A FLOP](#)
- [Wendy's: Where's The Breach?!](#)
- [RBS Named Top 10 Vulnerability Management Solution Provider](#)
- [TRENDnet Devices Bundle Infamous scfamar Service](#)
- [Risk Based Security Finds Vulnerabilities In Moxa SoftCMS](#)
- [Our New Year Vulnerability "Trends" Prediction!](#)
- [Nine Hotel Point of Sale Systems Hit With Startlingly Similar Breaches](#)

[Top of Page](#)

Copyright © 2016 Risk Based Security. [Privacy Policy](#). [Terms of Use](#)

Schedule A Demo!

