CYBER RISKS & LIABILITIES_
NEWSLETTER

January/February 2015

IN THIS ISSUE

All About the Sony Hack

Sony Pictures Entertainment was hacked in late November by a group called the Guardians of Peace. The hackers stole a significant amount of data off of Sony's servers, including employee conversations through email and other documents, executive salaries, and copies of unreleased Sony movies. Sony's network was down for a few days as administrators worked to assess the damage.

According to the FBI, the hackers are believed have ties with the North Korean government, which has denied any involvement with the hack and has even offered to help the United States discover the identities of the hackers. Various analysts and security experts have stated that it is unlikely that the North Korean government is involved, claiming that the government likely doesn't have the infrastructure to succeed in a hack of this magnitude.

The hackers quickly turned their focus to an upcoming Sony film, "The Interview," a comedy about two Americans who assassinate North Korean leader Kim Jong-un. The hackers contacted reporters on Dec. 16, threatening to commit acts of terrorism towards people going to see the movie, which was scheduled to be released on Dec. 25. Despite the lack of credible evidence that attacks would take place, Sony decided to postpone the movie's release. On Dec. 19, President Obama went on record calling the movie's cancelation a mistake. The movie was released online and in a limited number of theatres.

Although much of the attention over the hack centered on the cancelation of "The Interview," information has been released that claims Sony knew its network was prone to a large cyber event. In late 2013, the company was warned that hackers were stealing data on a weekly basis, and then encrypting it to hide their tracks. This discovery was made as part of a review of Sony's cyber security practices after the company struggled with security on its PlayStation network. The personal data of 77 million PlayStation Network users was compromised in 2011, but, according to two people familiar with the incident, Sony did not conduct an audit afterwards to determine just how much data was stolen.

In addition, an audit of Sony by PricewaterhouseCoopers from July 14 to Aug. 1 found that one firewall and more than 100 other devices were not being monitored by the company's corporate security team, but instead by the studio's in-house group. Auditors alerted Sony that this inefficiency could lead to slow response times, should an attack occur. Results of the confidential audit were released as a part of the hack in late November.

Security experts believe the hack could cost Sony a minimum of $100 million, possibly even reaching double that amount.

The attacks on Sony just reiterate what security experts have been saying for years—prepare for the worst by implementing strict cyber security protocols and having a sound cyber security insurance policy for the worst case scenario. Contact Seubert & Associates today to discuss your cyber security insurance options.

Seubert
Insurance | Surety Bonding | Benefits

Securing Your Files in Cloud Storage

Cloud storage—a service that allows you to upload documents, photos, videos and other files to a website in order to share those files with others or for backup storage—is proliferating across the Internet. Users can access their files stored in the cloud from any location on any type of device. While it's easy to use, a quick glance at recent newspaper headlines shows that storing files in the cloud—especially sensitive files—is not without risks.

For example, in late August, an anonymous hacker extracted private, nude photos of several major celebrities from Apple's online iCloud storage service. Because the celebrities had synced their iPhones with their iCloud storage, any photos they took on their phones were automatically saved in the cloud. Apple believes that the hacker either correctly answered the users' security questions or used a phishing scam to breach the celebrities' accounts.

The message is clear: Anything saved in the cloud is vulnerable. Therefore, if you choose to store your business' files in the cloud, check that the security and availability is right for the types of files you want to upload. When considering whether to use a cloud storage service, ask yourself the following:

- **Who can access my files?** Choose the privacy control that matches the sensitivity of your files: private (only you can view the files, although the cloud storage provider may be able to view them, too); public (everyone can view the files without any restriction); and shared (only people you invite can view them).
- **What is my password?** Choose a strong, unique password, and never use the same password across more than one site.
- **What are the storage provider's terms and conditions?** Reputable cloud storage providers should have clear, transparent information describing how they secure your information. If you cannot find it or feel the terms are unclear, shop around for other providers.
- **What types of encryption does the provider offer?** Encryption adds a further layer of security by rendering your files illegible unless the user has the decryption key. Some cloud storage providers encrypt files on your behalf.

2015 Cyber Threat Predictions

What kinds of threats will affect the cyber security landscape as we look ahead to 2015? McAfee recently made some predictions:

- Cyber espionage will continue to gain popularity among hackers.
  - As we have seen in the Sony hack, nation states and other terror/hacker groups can wage war against their enemies by using cyber espionage to launch distributed denial of service (DDoS) attacks or to plant malware in networks.
- Attacks on the Internet of Things will increase.
  - The number of things connected to the Internet continues to grow, but many lack the proper security to prevent an attack. Attacks on health care devices are expected to continue to rise.
- An individual's personally identifiable information (PII) is more vulnerable than ever.
  - As companies increasingly collect PII, the odds of it being compromised are increased, as well. Fortunately, advancements in biometrics and other, safer methods of securing PII will also be made.
- Mobile malware remains a big, yet mostly untapped, threat.
  - App stores often do a poor job of preventing fraudulent and/or malicious apps from appearing. Near field communications (NFC) as a point of sale transaction will grow in popularity, and, therefore, be attractive attack points for hackers.

What Can You Do to Reduce the Cost of a Data Breach?

According to the Ponemon Institute's 2014 Cost of Data Breach Study, the global average cost per record of a data breach was $145, but the following factors generally reduced the per-record cost:

- Strong security posture (cost $14.14 less per record)
- Incident response plan ($12.77)
- Business continuity management ($8.98)
- Chief Information Security Officer ($6.59)

CYBERRISKS&LIABILITIES_
NEWSLETTER

Seubert & Associates

Pittsburgh, PA
412-734-4900
http://www.seubert.com

© 2015 Zywave, Inc. This publication is for informational purposes only. It is not intended to be exhaustive nor should any discussion or opinions be construed as compliance or legal advice.