The Sony Hack: Information Technology Strategy Lessons Learned

Christopher Furton

Syracuse University

Abstract

On November, 24, 2014, someone claiming to be a former Sony Pictures Entertainment (SPE) employee announced via the website reddit.com that current employees were being sent home due to a network hack. Over the following couple weeks, details of the hack emerged highlighting the severity of the intrusion. This paper analyzes open source information gathered within the first three months after the attack and highlights several Information Technology Strategic lessons learned.

The Sony Hack: Information Technology Strategy Lessons Learned

Overview of the Sony Hack

On November, 24, 2014, someone claiming to be a former Sony Pictures Entertainment (SPE) employee announced via the website reddit.com that current employees were being sent home due to a network hack. Over the following couple weeks, details of the hack emerged highlighting the severity of the intrusion. A massive amount of data was stolen from SPE including salary details, social security numbers, birth dates, human resources performance reviews, criminal background checks, termination records, internal emails, intellectual property, user access credentials, and documents detailing the technical design and configuration of the information systems (Zetter, 2014). The amount of data stolen likely indicates that the perpetrators had access to SPE networks for a significant amount of time.

In addition to the theft of information, statements from a Federal Bureau of Investigation (FBI) alert alludes to, but does not specifically verify, information destruction as being one of the objectives of the cyber criminals (Zetter, 2014). As of January 23rd, 2015, Sony has also asked for an extension in filing its quarterly financial reports due to financial and accounting systems being offline because of the November 2014 incident. In that filing, Sony acknowledges that hardware was also damaged during the sophisticated cyberattack (Cozza, 2015).

The perpetrators of this cybercrime are currently unknown. The United States Government actively blames the Democratic Peoples Republic of Korea (DPRK) (Gallagher, 2015) while the hacktivist group Guardians of Peace (GOP) have accepted responsibility (BBC News, 2014). Furthermore, another hacktivist group named "Lizard Squad" has claimed responsibility for providing usernames and passwords to the Guardians of Peace (Fung, 2014).

Identifying who is behind the Sony hack is clearly a difficult process with evidence pointing in several directions.

Industry Relevance

Cybersecurity is quickly becoming one of the most important issues facing the United States. It has been discussed by political figures ranging from the President down to local city mayors. The days of bolting on security after-the-fact or outsourcing the function are gone. Organizations of all sizes – both public and private – must include cybersecurity in their Information Technology Strategy and be reflected in their Business Strategy. Although this paper focuses on Sony Pictures Entertainment, they are just one of many companies affected by large scale data breaches including Target, Home Depot, Community Health Systems, and JPMorgan Chase (Barrett, 2014).

Cybersecurity isn't just something discussed within the Information Technology departmental meetings; it affects all facets of the company, Board of Directors, and the customers. Senior level leaders can be forced to resign as was seen with Target's CEO Gregg Steinhafel (Barrett, 2014). Equally important, however, are the customers whose information is often the target for identity theft or other financial gain. Regardless of the motive, cybersecurity risks are enormous and need the focus of stakeholders throughout the organization.

IT Strategy Lessons Learned

This section will make several assumptions about SPE's Information Technology strategy and identify areas of improvement based on industry best practices. These recommendations are just a small portion of changes that ought to be included in Information Governance and SPE's overall strategy.

Information Management Policies

The attack has identified several information management policies that Sony Pictures Entertainment should consider. First, companies – including SPE - should develop methods to classify information with particular interest on identifying "assets" that require significant protection (Greenwald, 2015). Based off the wide variety of information stolen as identified by Zetter (2014), it is likely that SPE did not fully classify its information assets and set protection measures equal to the impact level of compromise. For example, an unreleased motion picture that is stolen and released to the pirated movie scene can result in millions of dollars in lost revenues. The exact amount of loss is influenced by many factors and should include possible gains from increased "hype" and publicity (Strauss, 2013). Information policies should be developed that classify corporate information and assign security controls or minimum levels of protection.

Closely related is the second information management policy that SPE should consider: data retention and destruction. As stated by Bruce Schneier (2015), "companies should have an aggressive deletion policy." This ideology conflicts with current perspectives on big data where companies retain as much information as possible; however, having this quantity of information stored poses a risk. In the SPE hack, the perpetrators published old-emails and documents that really had no business value for SPE but were still retained. "Saving data, especially e-mail and informal chats, is a liability" (Schneier, 2015). Implementing an organization wide deletion policy, where information that is not necessary to retain is deleted, will reduce possible exposure of sensitive personal communications.

Some types of information require special attention and protective measures are needed: namely, Personally Identifiable Information (PII). Currently, government organizations are held

to a high level of scrutiny for protection of PII (Wilbanks, 2007) and that same sentiment should be mimicked by companies like SPE. The Whitehouse is also urging Congress to pass cybersecurity legislation aimed at information sharing between government organizations and corporations (Hennessey, 2015). Ultimately, SPE and other corporations ought to implement - and strictly enforce - information protection measures now as legislative efforts will surely force them to so in the near future.

Managing the Cyber Risk

The Director of the Federal Bureau of Investigation, James Comey, has said that there are two types of US corporations, “Those that know they’ve been hacked and those that don’t” (Mellon, 2015). This notion seems to be finally sinking in after the Sony Hack as companies are ramping up their risk management strategies. According to a Chicago-based cyber risk insurance provider, “The Home Depot and Target breaches already had woken up the risk manager, but for some reason the huge prior breaches had not woken up the management to the extent (Greenwald, 2015)." This has caused an increase in enterprise-level response for managing cyber risks. One method gaining popularity is a financial risk management solution of buying cyber insurance. These cyber policies cover privacy and security risks; however, caution is required as not all policies cover terrorism or an act of war (Satter, 2015) (Greenwald, 2015).

Sony Pictures Entertainment could implement a holistic Enterprise Risk Management (ERM) framework designed to identify risks across the company including those associated with cyber threats. Protection can be gained through an insurance policy designed to reduce the financial impact of an incident; however, SPE still must focus on improving its technical capabilities for incident prevention, detection, and response.

Technical Perspective Ideology Shift

Historically, many corporations – and likely SPE – held a "Castle and Moat" design for cyber security. Under this paradigm, corporations design technical infrastructure similar to a medieval castle. A semi-secured area or demilitarized zone (DMZ) surrounds the architecture similar to how a moat surrounds a castle. The final defensive layer is the digital firewall to keep undesirable packets out similar to how a castle wall keeps undesired people out (Kip, 2010). Unfortunately, this architectural design no longer works in today's cyber environment.

SPE ought to implement a security architecture that relies on multiple layers throughout the infrastructure creating a defense in depth. Security protocols need to be implemented on all types of networking equipment including the backbone switching and routers, the endpoints, and data repositories (Vacca, 2014, p. Ch 10). SPE's most valuable information ought to be physically separated from their Internet accessible infrastructure providing increased security almost eliminating the risk of massive data exfiltration (Barrett, 2014). Through smart technical infrastructure design, SPE could have reduced their exposure caused by the exfiltration of publicly embarrassing information.

Encryption is Key

Another technical mechanism that would have reduced SPE's exposure and protected sensitive information would have been through the use of industry standard encryption. "Assuming that outsiders will get across the moat and penetrate the castle walls, companies have to do a better job of concealing the crown jewels" (Barrett, 2014). As stated by Barrett (2014), both Google and Yahoo implemented encryption technologies in the wake of the Snowden revelations to prevent snooping by the National Security Agency on their search engine data flows (para. 11). SPE could follow the lead of Canada's National Research Council and redesign

their entire security infrastructure taking advantage of the emerging field of quantum communication by implementing physics-based encryption systems (Spears & Press, 2014). More realistically, public key encryption solutions would offer that additional layer of defense at an affordable price.

Conclusion and the Author's Personal Reflections

Sony Pictures Entertainment is just one of many companies that have become victims of cybercrime. Most recently, on February 5th, 2015, healthcare organization Anthem Incorporated reported a network intrusion which exposed Social Security numbers and other details of 80 million customers (Riley & Robertson, 2015). The threat is real and no one is immune. Personally, my information was stolen including username, email address, and encrypted password from Adobe in October 2013. As a consumer, I lose confidence in companies who fail to protect the information I entrust to them. As an Information Technology Professional, I feel it is my responsibility to safeguard my employer's sensitive data and that includes our customer's information. As demonstrated by SPE, Anthem, and many others, often times the information could have been protected by employing techniques discussed in this paper. According to Riley & Robertson (2015) video interview, Anthem did not encrypt the contents of a database because the process of encryption/decryption makes the data "very hard to use" (1:58). Failures of this magnitude are unacceptable.

This paper's recommendations are based solely off publicly available news reports on SPE's November 2014 intrusion. Open information sharing between Government and Corporate America is critical so that organizations can learn from each other's mistakes. A deeper look into SPE would surely reveal more lessons to be learned but, unfortunately, that level of details will most likely remain undisclosed.

.

References

Barrett, P. (2014, 12 16). Forget the Gossip, these are the lessons of the sony hack. *BloombergBusiness*.

BBC News. (2014, 11 25). Sony Pictures computer system hacked in online attack. *BBC New - Technology*. Retrieved 02 04, 2015, from http://www.bbc.com/news/technology-30189029

Cozza, J. (2015, 01 23). Sony hack still causing headaches and now earnings delay. *CIO Today*. Retrieved 02 04, 2015, from http://www.cio-today.com/article/index.php?story_id=120003V3ZPS0

Fung, B. (2014, 12 29). A Q&A with the hackers who say they helped break into Sony's network. *The Washington Post*. Retrieved 02 04, 2015, from http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/29/a-qa-with-the-hackers-who-say-they-helped-break-in-to-sonys-network/

Gallagher, S. (2015, 01 07). FBI Director says Sony Hackers "got sloppy," exposed North Korea connection. *Ars Technica*. Retrieved 02 04, 2015, from http://arstechnica.com/security/2015/01/fbi-director-says-sony-hackers-got-sloppy-exposed-north-korea-connection/

Greenwald, J. (2015, 01 19). SONY ATTACK RECASTS CYBER SECURITY DEBATE: Information sharing seen as key component. *Business Insurance, 49*(2). Retrieved from http://search.proquest.com.libezproxy2.syr.edu/docview/1647431191?accountid=14214

Hennessey, K. (2015, 01 13). White house renews effort on cybersecurity bill with new proposal. *McClatchy Tribute News Service*. Retrieved 02 02, 2015, from http://search.proquest.com/docview/1644837537?accountid=14214

Kip, G. (2010, 05). A meter perspective on cyber security. *Electric Perspectives*, pp. 102-105. Retrieved from http://search.proquest.com/docview/506788770?accountid=14214

Mellon, C. (2015, 01 09). The Sony Hack in Contect. *CTOVision*. Retrieved 02 04, 2015, from https://ctovision.com/2015/01/sony-hack-context/

Riley, M., & Robertson, J. (2015, 02 05). Chinese state-sponsored hackers suspected in Anthem attack. *BloombergBusiness*. Retrieved 02 06, 2015, from http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack

Satter, M. (2015, 02 02). What advisors can learn from the Sony hack. *Investment Advisor*. Retrieved 02 04, 2015, from http://www.thinkadvisor.com/2015/02/02/what-advisors-can-learn-from-the-sony-hack?t=life-planning-ltc

Schneier, B. (2015, 01 12). The importance of deleting old stuff -- another lesson from the sony attack. *Ars Technica*. Retrieved 02 04, 2015, from http://arstechnica.com/security/2015/01/the-importance-of-deleting-old-stuff-another-lesson-from-the-sony-attack/

Spears, T., & Press, J. (2014, 07 30). Suspected cyber attack forces NRC to revamp security; Agency works on advanced encryption. *Star - Phoenix*. Retrieved from http://search.proquest.com.libezproxy2.syr.edu/docview/1550037478?pq-origsite=summon

Strauss, K. (2013, 03 06). TV and Film Piracy: Threatening an Industry? *Forbes*. Retrieved 02 04, 2015, from http://www.forbes.com/sites/karstenstrauss/2013/03/06/tv-and-film-piracy-threatening-an-industry/

Vacca, J. (2014). *Chapter 10 - Securing the Infrastructure.* Syngress Publishing.

Wilbanks, L. (2007, 07). The impact of personally identifiable information. *IT Pro, CIO Corner*. Retrieved 02 05, 2015, from http://www.computer.org/publications/dlib

Zetter, K. (2014, 04 12). Sony Got Hacked: What we know and don't know so far. *Wired*. Retrieved 02 04, 2015, from http://www.wired.com/2014/12/sony-hack-what-we-know/