**Sources of Security Threats: Human, Nature, and Technology Factors**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**SLP 01**

INTRODUCTION

Information security threats and attacks impact more than a single machine or individual or entity. While the scale of the damage varies from the smallest level of impact, the individual user, to entire countries, not all attacks are intended or even of a human’s doing. This discussion explores threats and attacks to information security that have taken place, locally and abroad; such as extortion, data destruction, release of confidential information, disrupting state infrastructure, and holding information for ransom.

DESTRIBUTED DENIAL OF SERVICE

Distributed denial of service (DDoS) is a term or phrase given to identify when a service like, the ability to visit a Web site or use a network is denied directly because of deliberate data congestion. During the week of March 24, 2013, a stream of data about 300 billion bits per second made some Web sites unavailable and slowed networks down around the world. Some areas reported reduced operations for up to 9 days (Markoff, 2013).

This ability to harness thousands of computers to send streams of data to a single host or address, simultaneously, is seen by many as a threat to businesses and the general public. When users are interrupted in their work flows, businesses have the potential to lose a significant portion of production and the users, themselves, may become accountable for the works they were not able to render during such ‘downtimes’.

In contrast, governments could use this ability to identify, known and unknown cyberterrorists, sources of the attacks, and locations of areas that attacks stem from. With this knowledge, governments can better prepare themselves and their citizens against such attacks making these threats futile, at best.

NORTH KOREA LOSES INTERNET

On Monday, December 22, 2014, North Korea is described to have its internet have gone, “as dark as one of those satellite photographs showing the impoverished country by night” (Perlroth et al., 2014). There are some who suggest this could have been an indirect or proportional response from the United States with regard to North Korea’s cyber-vandalism against Sony Pictures. Sony pictures’ information security was compromised by a group of hackers, known as, Guardians of Peace (GOP), the Monday before Thanksgiving 2014 (Peterson, 2014).

According to a CNN article published Wednesday, December 24, 2014, President Obama stated that, he doesn’t consider “North Korea’s hack of Sony Pictures an act of war. It was an act of cybervandelism” (Bradner, 2014). The close proximity of timing of the two very large events, North Korea’s internet going down and the hack on Sony Pictures, has observers questioning authenticity of this statement.

In an article on [www.slate.com](http://www.slate.com), author David Auerbach stated that on Wednesday, January 21, 2015, FBI Director James Comey revealed that, “some of the emails from hacker group GOP came from IP addresses ‘exclusively’ used by North Korea” (Auerbach, 2015). Then, Mr. Auerbach points readers to more skeptical writers like Rem Rieder.

Author Rem Reider shared in an article in USA Today dated January 5, 2015, “a growing chorus of cybersecurity experts have their doubts” (Rieder, 2015). He writes deeper ideas and shared professional supporting arguments, on these doubts; like that of Scott Borg, director of the non-profit United States Cyber Consequences Unit, where Mr. Borg stated, “North Korea has never before demonstrated any advanced hacking capabilities” and “it has hardly any way of acquiring those capabilities” (Rieder, 2015).

With these conflicting stories, it is hard to understand which authority to trust. Was the Obama administration wrong? If so, what threats to the information security of America and her allies truly exist and how might the American people be under attack from such threats?

RANSOMWARE

“Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker). Other ransomware use the onion router (TOR) to hide C&C communications (called CTB Locker)” (Ransomware, 2015).

According to an article entitled, “How my mom got hacked”, in the January 25, 2015, New York Times, a woman fell victim to a ransomware attack for about $500 to have her 5,726 files returned to her. The article elaborates on the circumstances and the precarious inconveniences of the mother and daughter while they frantically proceeded to pay the ransom. Their message ended with the caveat that the criminals wanted to ensure people understand that they are going to give the ransomed data back because, they want to keep a good reputation (Simone, 2015).

NATURAL DISASTER

In October, 2012, the east coast was struck by hurricane Sandy. On the 29th, New York was riddled by her and along with the loss of life there were significant power outages. Due to heavy winds, rain and flooding, most of New York City and Long Island experienced power outages (Sanchez et al., 2012).

Amazon Web Services (AWS) U.S. East -1 services complex has seven locations in New York and others located in, Virginia, Washington, D.C., Philadelphia, Buffalo and northern New Jersey. The Amazon Health Services dashboard reported elevated outages with its CloudFront, content distribution network. Compuware tracked "more than a dozen outage events on the East Coast during (Monday) afternoon and evening" (Babcock, 2012). Many customers went without power, but only a few customers experienced Amazon’s EC2 downtimes. Many of the AWS sites have back up power or were able to re-route user traffic to accommodate for the loss of machines.

CONCLUSION

There are several observed effects of damages incurred by breaches of information security. As discussed, some incidents leave countries without internet access. Other incidents leave people and companies in a state of chaos. From power outages to cybercrimes, information security has a large array of potential threats.

REFERENCES

Auerbach, D. (2015, January 7). Don’t Trust the FBI. Don’t Trust the Countertheories. The Sony Hack Is As Murky As Ever. Retrieved October 28, 2015, from <http://www.slate.com/articles/technology/bitwise/2015/01/sony_hacks_and_north_korea_> why\_the\_cyber\_attack\_is\_as\_mysterious\_as\_ever.html

Babcock, C. (2012, October 31). Amazon, Equinix Data Centers Vs. Hurricane Sandy - InformationWeek. Retrieved November 2, 2015, from <http://www.informationweek.com/amazon-equinix-data-centers-vs-hurricane-sandy/d/d-> id/1107135?

Bradner, E. (2014, December 24). Obama: North Korea's hack not war, but 'cybervandalism' - CNNPolitics.com. Retrieved October 28, 2015, from <http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-> vandalism/

Markoff, J. (2013, April 1). Distributed Denial of Service. Retrieved October 28, 2015, from <http://www.nytimes.com/2013/04/02/science/distributed-denial-of-service.html?_r=0>

Perlroth, N., & Sanger, D. (2014, December 22). North Korea Loses Its Link to the Internet. Retrieved October 28, 2015, from <http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-> internet-collapses.html

Peterson, A. (2014, December 18). The Sony Pictures hack, explained. Retrieved November 1, 2015, from <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-> pictures-hack-explained/

Ransomware. (2015). Retrieved October 28, 2015, from <http://www.trendmicro.com/vinfo/us/security/definition/Ransomware>

Rieder, R. (2015, January 5). Rieder: Maybe North Korea wasn't behind Sony hack. Retrieved October 28, 2015, from <http://www.usatoday.com/story/money/columnist/rieder/2015/01/05/maybe-north-korea-> wasnt-behind-sony-hack/21290467/

Sanchez, R., Winch, J., Hughes, M., & Willis, A. (2012, October 29). Hurricane Sandy: October 29 as it happened. Retrieved November 2, 2015, from <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9642980/Hurricane-> Sandy-October-29-as-it-happened.html

Simone, A. (2015, January 3). How My Mom Got Hacked. Retrieved October 28, 2015, from <http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html>