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

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**Case 01**

INTRODUCTION

According to Eric Schmidt, CEO of Google, every two days we, as a people of Earth, “create as much information as we did from the dawn of civilization up until 2003” (Siegler, 2010). Each minute, Facebook users share about 2.5 million times, Twitter users tweet about 300,000 messages, and Instagram users add or post about 220,000 new photos. Each minute YouTube users upload an average of 72 hours of video, Apple users download about 50,000 mobile and other device applications, and Email users send and received over 200 million email messages. Each minute Amazon averages about $80,000 gross in online sales (Gunelius, 2014).

The amount of information that is being generated is about an Exabyte of data and it’s communicated, electronically (Siegler, 2010); as such, there are inevitable threats to the security of personal or private or sensitive information. This discussion answers the questions, why is information security an important issue and what are the sources of information threats?

THREATS, VICTIMS, AND PURPOTRATORS

The internet, in its simplest form, is nothing more than two or more computers with the ability to connect to each other. Each computer or machine must, therefore, have its unique IP (Internet Protocol) address. IP addresses are constructed in the form of nnn.nnn.nnn.nnn where nnn is a number between 0 – 255 (Shuler, 2002).

In a class A IP address, the first section of the IP address (0nn) represents the network and the trailing section (nnn.nnn.nnn) represents the host address. In a class B IP address, the first half of the IP address (10n.nnn) represents the network address and the second half (nnn.nnn) represents the host address. In a class C IP address, the first section of the IP address (110.nnn.nnn) represents the network address and the second section (nnn) represents the host address (Doughty, 2013).

The risk of potential security breaches by hacks such as, phishing or social engineering may use these IP addresses and puts the integrity of all the data on each machine at risk; for example, product information, financial information, and customer information. It may not be obvious as to what concerns there are for a breaches of security in this way. To help with this, the exploration of the value of each different type of data is necessary.

Product information could include any number or combination of the following types of data: designs, plans, patent applications, source code, or drawings. Financial information could include market assessments or financial records or both. Customer information could include confidential information that is held on to, on behalf of the customer.

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission. The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence (Cybercrime Definition, 2015). This includes the previously mentioned hacks, but does not limit the definition as such.

Stealing data is one common form of cybercrime, but there are also other forms to be concerned with; such as, extortion, data destruction, the release of confidential information, distributed denial of service (DDoS), disrupting state infrastructure, and holding information for ransom (Franklin, 2015).

There are several cybercrimes being committed around the world at any given time. “It appears more cybercriminals are entering into the game at a quicker pace than quite honestly we can keep up with, in the US, to defend our networks from malicious hackers,” says JD Sherry, the vice president of technology and solutions at Trend Micro, a Tokyo-based cyber-security firm (Raymon, 2014). These crimes involve, private institutions, public works, and personal assets.

JP MORGAN

In July, 2014, hackers had attacked JP Morgan and breached their security effecting more than 83 million households and businesses. In doing so, they were able to access information about the names, addresses, phone numbers, and email addresses of account holders. This big data attack was not completely halted until the middle of August within the same year by the bank’s security team (Goldstein et al, 2014). The source of the penetration was found out to be two unidentified men, described as co-conspirators and not charged, from New Jersey and Florida. The men charged are Gery Shalon and Ziv Orenstein, both Israeli citizens, and Joshua Samuel Aaron, a U.S. citizen, who resided in both the United States and Israel (Riley et al, 2015).

JP Morgan spends approximately $250M, per year, on security to protect its computers. Even so, hackers were still able to retrieve 40 gigabytes of data on at least 100 servers. It was discovered, later in the investigation, that this crime was a setup for a larger stock exchange crime (Goldstein et al, 2015).

The hackers were able to gain access with relative ease; as, the company’s security team had overlooked one server for a simple security fix that had been installed on all the other servers. This penetration was nothing short of an embarrassment for the banking giant (Goldstein et al, 2015).

“Pump and dump” is a phrase used to describe illegal activities concerning the convincing of shareholders to buy or invest in a specific type of stock and then, at some point, the criminals would sell their stocks to optimize their financial gains. The emails obtained from JP Morgan were used to do just that by sending promotional emails telling the victims that certain stocks were ‘hot’ and to buy them quickly (Riley et al, 2015).

CURRAN-GARNER WATER DISTRICT

On November 8th, 2011, the Curran-Garner Water District, located at, 3382 Hazlett Road, Springfield, Illinois 62707, fell victim to a cyber-attack. Sometime during the day, a water district employee noticed problems with a supervisor control and data acquisition (SCADA) system. After an unnamed information technology service and repair company had checked the computer logs of the SCADA system, they were able to determine that the system had been remotely hacked. The IP address, of the hacker(s), was last traced to Russia (Krebs, 2015).

While in the system, hackers were able to toggle switches on, off and modify pump activity. These unauthorized activities caused the eventual failure of a water pump at the facility. Joe Weiss, managing partner of Applied Control Solutions, a SCADA systems security firm stated, “It is believed the hackers had acquired unauthorized access to the software company’s database and retrieved the usernames and passwords of various SCADA systems, including the water district systems” (Krebs, 2015).

Officials who reported on this attack also shared that the method of these attacks were very similar to the way that the servers were compromised during the attacks at the Massachusetts Institute of Technology (MIT). phpMyAdmin is a popular Web-based database administration tool and security logs indicated that, in both incidents, there were references to phpMyAdmin (Krebs, 2015).

In larger and well-funded facilities, remote access is carefully monitored with security solutions like, virtual private networks (VPNs). The more protected companies are less likely to experience and suffer from an attack like this. However, with many low budget water districts they cannot afford substantial infrastructure and have come to rely on remote Web access for day to day business practices (Krebs, 2015).

RANSOMWARE

Ransomware, a growing information security threat, is a malware that prevents or limits users from gaining access to their systems. This type of security threat can be encountered by a variety of means. Some users simply navigate to a website and inadvertently download the software onto their system(s). It can also arrive in tandem with other programs that are being downloaded without the user being made aware of its presence. Others are delivered through spam or phishing schemes via email (Ransomware, 2015).

Ransomware first emerged in Russia and Eastern Europe in 2009 and quickly spread across Western Europe, the United States, and other countries. “Professional cybergangs use intelligent malware, which once on your computer, identifies which country you live in (via your IP address) and presents the message in the local language with a logo of a local public authority” (“Ransomware on the rise”, 2015). The ransomware, like the name sounds, takes your computer hostage for a fee. Once that fee is paid, you may or may not get your computer back. According to an expert analysis by Symantec experts, a crime committed over the course of a month violated users of approximately $33,600 each day (“Ransomware on the rise” , 2015).

SOURCES OF INFORMATION THREATS

There is no shortage of sources of information threats. In exploring the development of software, information threats stem from, specification errors, organizational errors, and faulty code in integrated architectures that enable cyber terrorists to attack critical systems (Perrow, 2008).

Additionally, there are five main sources of security threats. The Internet or worldwide web hosts a series of malware such as, drive-by attacks, which put Trojan viruses on a machine while browsing a particular website, downloading malicious software like, keygens, cracks, or patches, and downloading shared files from direct share sites like torrents. Email attacks have been seen in the form of spam, which are just a waste of your time, and phishing, which seeks out for personal data such as, credit card information. Software vulnerabilities are most common targets of hackers where, through software bugs and glitches, hackers can take control of your computer. Removable data storage media is the fourth main source of security threats and can infect a users’ system when they attach a USB or other peripheral device and attempt to install data or files or other. Lastly, users’ actions of installing software that is socially engineered, meaning that the software is malicious and tricks the user into installing this malware, catches the user off guard and compromises their data or machine (Kaspersky, 2015).

NATURAL DISASTERS

Of the many threats to information security, natural disasters can be catastrophic. Earthquakes, floods, hurricanes, tornados, lightning strikes, and fires are examples of such phenomenon. To protect against these types of events users typically employ any of the following strategies: backup their data, install their machines in non-hazardous environments, and install an Uninterruptible Power Supply (UPS) to provide backup power in the event of a power outage (“Natural threats”, 2013).

CONCLUSION

Because there are inevitable threats to the security of personal or private or sensitive information it is important to keep up awareness and to update software, regularly. This discussion answered the questions, why is information security an important issue and what are the sources of information threats? Data management dictated by governmental and other agencies is the key indicator that data is the most important information to secure (Hein et al, 2015).

REFERENCES

Franklin, B. (2015). 5 Cybercrimes on the Rise in 2015. Retrieved October 30, 2015, from <http://www.forensicscolleges.com/blog/resources/cybercrime-on-rise-2015>

Cybercrime. (2015). Retrieved October 26, 2015, from <http://www.interpol.int/Crime-> areas/Cybercrime/Cybercrime

Cybercrime Definition. (2015). Retrieved October 26, 2015, from <http://searchsecurity.techtarget.com/definition/cybercrime>

Doughty, A. (2013, January 10). IP Addressing and How it Works. Retrieved October 30, 2015, from https://www.youtube.com/watch?v=KFooN7Mu0IM

Edwards, C., Kharif, O., & Riley, M. (2011, June 27). Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy. Retrieved October 27, 2015, from <http://www.bloomberg.com/news/articles/2011-06-27/human-errors-fuel-hacking-as-test-> shows-nothing-prevents-idiocy

Goldstein, M., Perlroth, N., & Corkery, M. (2014, December 22). Neglected Server Provided Entry for JPMorgan Hackers. Retrieved October 27, 2015, from <http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-> identified/

Goldstein, M., Perlroth, N., & Sanger, D. (2014, October 3). Hackers' Attack Cracked 10 Financial Firms in Major Assault. Retrieved October 26, 2015, from <http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-> assault/?r=0

Gunelius, S. (2014, July 12). The Data Explosion in 2014 Minute by Minute – Infographic. Retrieved October 23, 2015, from [http://aci.info/2014/07/12/the-data-explosion-in-2014- minute-by-](http://aci.info/2014/07/12/the-data-explosion-in-2014-%09minute-by-)minute-infographic/

Hein, T., McClain, N. (2015). Every company needs to have a security program. (2015). Retrieved October 26, 2015, from [https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a- security-](https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-%09security-)program

Kaspersky, E. (2015). Safety 101: Main sources of threats penetration. (2015). Retrieved October 27, 2015, from http://support.kaspersky.com/us/viruses/general/789#block1

Krebs, B. (2015). Krebs on Security. Retrieved October 27, 2015, from <http://krebsonsecurity.com/2011/11/cyber-strike-on-city-water-system/>

Natural Threats. (2013). Retrieved October 31, 2015, from <http://online-> passport.info/comsecpriv/?page\_id=37

Perrow, C. (2008, March 31). Software Failures, Security, and Cyberattacks. Retrieved October 27, 2015, from http://www.cl.cam.ac.uk/~rja14/shb08/perrow.pdf

Ransomware. (2015). Retrieved October 27, 2015, from <http://www.trendmicro.com/vinfo/us/security/definition/Ransomware>

Ransomware on the rise: Norton tips on how to prevent getting infected. (2015). Retrieved October 27, 2015, from <http://us.norton.com/ransomware/article>

Rayman, N. (2014, August 7). The World's Top 5 Cybercrime Hotspots. Retrieved October 31, 2015, from <http://time.com/3087768/the-worlds-5-cybercrime-hotspots/>

Riley, M., & Robertson, J. (2015, July 21). Digital Misfits Link JPMorgan Hack to Pump-and- Dump Fraud. Retrieved October 27, 2015, from <http://www.bloomberg.com/news/articles/2015-07-21/fbi-israel-make-securities-fraud-> arrests-tied-to-jpmorgan-hack

Shuler, R. (2002). How Does the Internet Work? Retrieved October 26, 2015, from <http://web.stanford.edu/class/msande91si/www-> spr04/readings/week1/InternetWhitepaper.htm

Siegler, M. (2010, August 4). Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003. Retrieved October 23, 2015, from <http://techcrunch.com/2010/08/04/schmidt-data/>