CYBERCRIME: IN DISGUISE CRIMES

Pranshu Gupta [1*]
Ramon A. Mata-Toledo [2]

ABSTRACT

Cybercrime is commonly defined as any criminal act in which a perpetrator breaks or hacks into a computer or computer network in order to illegally obtain sensitive information or disseminate destructive computer software. Common examples include Internet fraud, identity theft, credit card account theft, or access to information that can cause harm to an individual or corporation. Web technology has played an important role in giving rise to such crimes. Hacking into a computer these days is like taking snapshots or x-rays of someone's body – there is vast amount of personal information stored in the computer. A person may have actual research or potential ideas for it (the brain), memorable pictures (the heart), work files (making a living) and some additional information stored on the computer. On the surface the hacker is not physically hurting anyone in this scenario, but this is not true in general. The damage caused by these crimes cannot be easily measured. Physical violence is a visible form of crime but cybercrimes are committed in the 'unseen' world of Internet that may be 'accessible' by the world. In this case we could say that this is not physical violence because nobody is physically hurt; however this is no an encompassing definition of violence. According to the World Health Organization (WHO), violence can be defined as "the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, which either results in or has a high likelihood of resulting in injury, death, psychological harm, mal-development, or deprivation." In addition to these, violence can also include exposure to ridicule or defamation of character. In this sense, cybercrimes can cause more psychological harm and deprivation than any other crime committed against a person. The trauma caused by cybercrime can have a long term effects on a person's mental, physical health, and financial affairs. In this paper the authors consider some aspects of how the computer can be used as a tool to commit violent and criminal acts and some key factors to mitigate these risks.

KEYWORDS: *cyber, crime, internet, cyber law, hacking*

1. INTRODUCTION

Before the rise of the Internet, cybercrimes were difficult to commit because the perpetrator had to have a physical access to the computer. Nowadays, hacking has become easier because any computer with an active Internet connection is susceptible to remote access. Hacking or unauthorized access to information stored in a personal or corporate

[1*] corresponding author, DeSales University, Center Valley, PA, 18036, Tel: (610) 282-1100 x 2854, Pranshu.Gupta@desales.edu

[2] James Madison University, Harrisonburg, VA, 22807, Tel: (540) 568-2775, matatora@jmu.edu

computer system can be achieved via website, email, or network with devastating results for the computer's users and/or the equipment itself.

Through a website the hacker tries to find loopholes to access personal or financial information for illegal gain, pleasure or to harm somebody. Websites prone to hacker attacks are those generally used for online shopping, banking, or social media. In 2013, the retail store Target® was a victim of hacking. In this case the website was hacked using the "point of sale" machines to steal credit card information affecting millions of users. This, in turn, caused some banks such as Chase® to limit the amount of ATM withdrawal of all compromised debit cards to a maximum of 100 dollars per day [10]. Users wishing to withdraw larger amounts were forced to visit a bank branch. This is a good example of the users being a victim of cybercrime over which they did not have any control.

Another commonly used method for victimizing computer users is through email. Email hacking can be achieved using social engineering, malware, spyware, worms, viruses, etc. Social engineering is the art of manipulating people so they give up confidential information. It is a non-technical, easy to use, and most successful attack. Social engineering used human interaction to trick people into providing sensitive information because of their trusting behavior. This way the hacker can access personal information including email of highly sensitive nature. Nowadays, a great deal of personal and business communication is carried out using email. Some users may not be well-informed, be technical-savvy or take the necessary precautions to protect their email id/password [9].

A preferred method of hacking is Network hacking because it has the potential of accessing information about a larger number of people. The hacker overcomes the network firewalls and get access through a backdoor or the impersonation of a legitimate user. Hacking techniques on networks also include creating worms, initiating denial of service (DDoS) attacks, or in establishing unauthorized remote access connections to a computer. Other things that could worsen this situation is the existence of many pre-packaged scripts available on the Internet for anyone to use. Sophisticated hackers may study and enhance these scripts to develop new methods of attacks. As reported on the Silicon Angle website, China has one of the most sophisticated filtering systems in the world. However on August 25th 2013, a part of the Chinese Internet went down as a result of the largest denial-of-service (DDoS) attack that it has ever faced. According to the China Internet Network Information Center, the attack began at 2 a.m. and was followed by an even more intense attack at 4 a.m. on the same day. The attack was aimed at the registry that allows users to access sites with the extension ".cn," [2].

In the following sections we will discuss some real-life examples of cybercrimes, cyber law, and the costs incurred due to these crimes and how to mitigate the risks of becoming a victim of these type of crimes.

2. EXAMPLES OF CYBER-CRIMES

2.1. Identity-fraud

In 2012, 12 million people in USA were victims of identity fraud out of which 34% were reported in Florida, 24% in Georgia and 20% in California [7]. Most of the users were hacked using social websites where 15% had unauthorized access to their accounts, 13% had passwords or other sensitive information disclosed through social engineering. A large majority of people, 70%, were asked to visit a scam website via a private message. When using social media websites, people share personal information without even intentionally thinking that such information can be used against them. A 2012 study indicates that 93% people share their full name, 4% their home address, 60% share family names or relatives, and 33% share their current employer. In Facebook™, 30% of its users do not have their profiles set to private and 14% did not know how to change their privacy settings [7].

2.1.1. The Freebie

“In Wichita, Kansas, a man walked into a police station and told the cops that he was an undercover agent who had recently assumed the identity of a local homeowner. He gave them the address of the house he was currently occupying. Therefore, if anyone calls to report him as an impostor or allege that he had broken into the house, the police would have no need to investigate as he had already explained his situation. The cops selected one of the innumerable things about his statement that didn't make sense. They went to the given address and found the same man living there under the original homeowner's identity. He had gotten new credit cards, set up phone service and purchased a few flat screen TVs and computers in the homeowner's name. The man and his wife had also used the homeowner's name to take out a second mortgage. As it turns out, the homeowner had been gone for several months, caring for his mother who had fallen seriously ill in another town. While he was gone, this couple had stolen his house and his name, and then changed the locks and set up a new mailbox before going to the police and exposing their crime [5].”

2.1.2. Life takes a turn

“Simon Bunce was a former RAF (Royal Air Force) pilot and successful business executive living in England. However in March 2004, he was arrested as part of “Operation Ore”, a massive British police crackdown on child pornography. Mr. Bunce was taken into custody and his computer equipment and other personal possessions were confiscated. He was immediately fired from his high-paying job and was essentially disowned by his entire family except for his wife. He discovered that in 1999, his credit card information was stolen from an online shopping site, then used by someone in Indonesia to purchase child porn from an American website. Cross-checking the information he collected with his own records, Bunce was able to prove that at the same time he was supposedly buying child pornography, he was at a restaurant in London [5].”

2.1.3. What? I am already married!

“In terms of the stress involved in wedding preparation, obtaining a marriage license usually ranks in between choosing the font for the invitations and figuring out whether or not you can use Masters of the Universe figures as your cake toppers. You go to court, sign some forms, pay a small fee, and you are legally married. At least that's all Rosa Vargas of Queens, New York, was expecting when she filed her application for a marriage license in 2004. So imagine her surprise when she found out three weeks before her wedding, that the application had been rejected by the City Clerk's Office because they found that she was already married to two other men, one in Mexico and one in Ecuador. About five years later, Vargas was served divorce papers from an Ecuadorian man she had never met. She refused to sign the papers, but the man persisted. He showed up at her assumed mother-in-law's doorstep and would not be persuaded until she showed him a picture of Vargas' wedding day, in which the man could clearly see that he was in no way represented. Vargas had lost her birth certificate about 16 years earlier, and over time her name and information had been used by two different women in two different marriages, most likely as a type of immigration scam. Vargas was eventually able to get the phony marriages nullified by a judge, but has since found herself married to a third stranger somewhere on Long Island [5].”

2.1.4. Mail scam

A ‘4-1-9 Nigerian’ scam is a form of an upfront payment or money transfer scam. These types of scams were pioneered in Nigeria hence its name, however, scams of this type can come from anywhere in the world. The ‘4-1-9’ part of the name comes from the section of Nigeria’s Criminal Code which outlaws the practice. Scammers usually contact the victim by an email or letter and offer a share of a large sum of money that they need to transfer out of their country. Scammers ask the victim to pay money or provide bank account details to help transfer the money. The money promised will never come to the victim but the scammers will keep asking for more money in form of a “fee” or other administrative costs, informing the victim that everything is being done to send the promised money as soon as possible. Obviously, the money never comes and large amounts of money are taken out of the victim’s accounts.

2.1.5. Russian bride scam

Love and Money – the core aspects of this scam. It is important to focus on how the scammers not only are extorting money but also playing emotional games with the victim because they do not want the victim to think rationally. In this scenario, a "female" scammer falls in love with her Internet acquaintance in a short period of time and then shows her interest in meeting with her acquaintance in person. She then informs her acquaintance that money issues are stopping her from meeting him. The victim who falls for the scam will send money for visa and tickets but she may have another excuse to extract more money such as “the money was lost or stolen” or “she is stranded on the airport”. The scammer would also mention that she will pay off the money with a job offer she has in the country. As expected, at the end both, love and money, are lost forever resulting in a “broken” heart and a substantially diminished savings or checking account.

2.2. Industrial/Corporation/political espionage and hacking

With the Internet revolution and growth of new technology, cybercrime is also changing its face daily. A new generation of hackers are interested in intellectual property and trade secrets that can be sold in the market for large amounts of money. If a hacker steals a marketing plan from one company, and sells it on the cyber underground to that company's biggest competitor, there is less risk of law enforcement and controversies. Organizations don't like to publicize that they have been hacked so if there are no data breach notification laws, most likely the theft will be kept confidential and secret even if it is discovered.

2.2.1. Operation aurora

In 2009, there was a series of cyber-attacks using the advanced persistent threats (APTs - is a set of stealthy and continuous computer hacking processes targeting a specific entity) that modified source code repositories at security and defense contractor companies in the USA [13]. As a result, the attackers gained accessed to confidential and sensitive source code repositories at these Corporate Mongols.

2.2.2. Night Dragon

Oil, gas and petrochemical companies were attacked using their public Web sites and social-engineering techniques [14]. Even though social engineering intuitively does not sound as a popular method of hacking but it constitutes as a large part of the hacking industry. Persuasive social engineering was used to trick key executives from different countries to divulge sensitive information that would help in accessing the information through the company website login.

2.2.3. Sony hack

The Sony Pictures Hack was the whole entertainment package in itself - the celebrity, the cybercrime and the geopolitics; a thriller - no pun intended - in the making. This attack involved using a destructive malware to steal huge amounts of corporate data, rendering thousands of Sony's computers inoperable and taking the entire network offline [15].

2.3. Politics

In September 2013, the Port Authority of New York and New Jersey unexpectedly closed two access lanes on the New Jersey side of the George Washington Bridge which serves as a major commuter route between the two states. This resulted in a massive, week-long traffic jam that congested the streets. Press releases and court cases that have emerged indicate that this event was an outcome of political retribution to affect negatively the image of the state’s governors.

2.4. Revenge

In 2014, a man was arrested by blackmailing women, in particular, his ex-lover, by posting nude and sexually explicit photos of her on his website. The man was charged in California for running a "revenge porn" website. The web is full of sites where split up lovers can post images of an ex-partner for all the world to see [3]. California Governor Jerry Brown signed a bill in year 2013 outlawing revenge porn and imposing possible jail time for people who post naked photos of their exes after breakups [1]. This shows the necessity of new laws to control the online behavior of individuals and organizations.

We can see from the above real-life example that it is immature to believe that techniques and schemes behind the acts of cybercrime, hacktivism, espionage and cyber warfare would remain separate and easily identifiable [20]. With the evolving technology it will be a challenge to manage these cybercrimes and their consequences.

3. COST OF CYBER ATTACKS

Cybercrime costs about over $100 billion each year [4]. The Ponemon Institute's 2013 Cost of Cyber Crime study concluded that an average company in the U.S. experiences more than 100 successful cyber-attacks each year. These attacks came at a cost of $11.6M which was an increase of 26% from the previous year [8]. This study surveyed over 230 organizations in countries such as the United States, United Kingdom, Germany, Australia, Japan, and France. The study also showed that companies who implemented preventive measures reduced losses by nearly $4M [8].

The Federal Bureau of Investigation (FBI) – Internet Crime Complaint center reported a total of 269,422 Internet crime complaints in 2014; out of which 123,684 complaints reported a loss due to cybercrime costing more than $800M. The top 5 states registering complaints were California, Florida, Texas, New York and Pennsylvania.

First, it is important to note the distribution of the intended malicious attacks versus unintended attacks such as a software glitch or human errors [17]. Figure 1 shows that all attacks are not malicious and also not intentional. Only 41% of the total attacks are intentionally trying to cause harm to the systems i.e. someone intentionally designing a program to hack into a system. The next step is to understand the motivation behind these malicious attacks. As of April 2015, the distribution of the motivation behind the cyber-attacks is shown in Figure 2. Now if we analyze both figures 1 and 2, we can say that 22% of the total attacks are related to cyber-crime, 13% is hacking, 4% is cyber espionage and 2% is cyber warfare [18]. This analysis shows that not all attacks are meant to cause harm to a computer but some of them have ulterior motives such as hacktivism. **Hacktivism** is the act of breaking into a computer system for a politically or socially motivated purpose [19]. The goals of hacking into a computer machine determine if the attack is a cyber-crime or hacktivism. In this paper we will not get into the details of their differentiation but we will note that they belong to different categories.

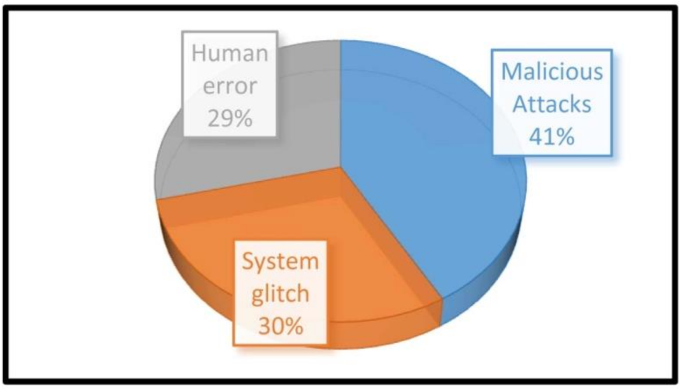
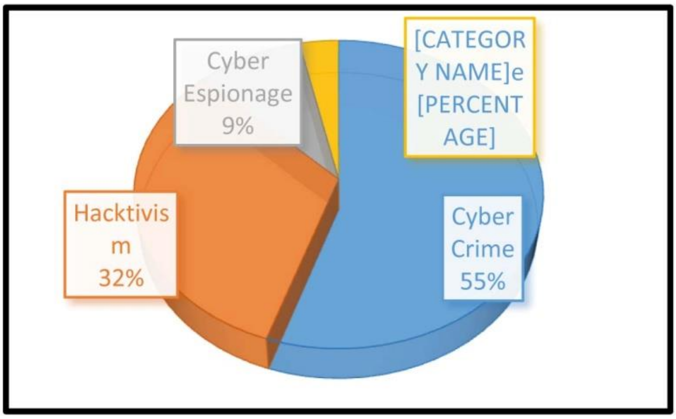


Figure 1. Distribution of the types of attacks [18]

Figure 2. Distribution of the motivation behind the attacks [18]



Now that we have an understanding of the types of malicious attacks and the motivation behind them let us focus on the victim of these attacks. Figure 3 shows the findings of the distribution of targets as of April 2015 [18]. The “Other” category include airports, APTs, Internet services, law enforcement, military and religion. Industry is definitely the major target of cybercrime as it benefits from it the most monetarily. The more sensitive the information, the more money can be gained from that crime. Figure 4 amplifies the distribution of accidental incidents which can be categorized as human error or system glitch from Figure 1. We have observed that 59% of the types of attacks are either human error or caused by a system glitch. Therefore, approximately 9% of the accidental attacks are caused due to Email breach (victim unknowingly opening malicious attachments), 19% are caused due to web breach (victim unknowingly opening malicious web sites), and 8% are caused due to improper equipment disposal.

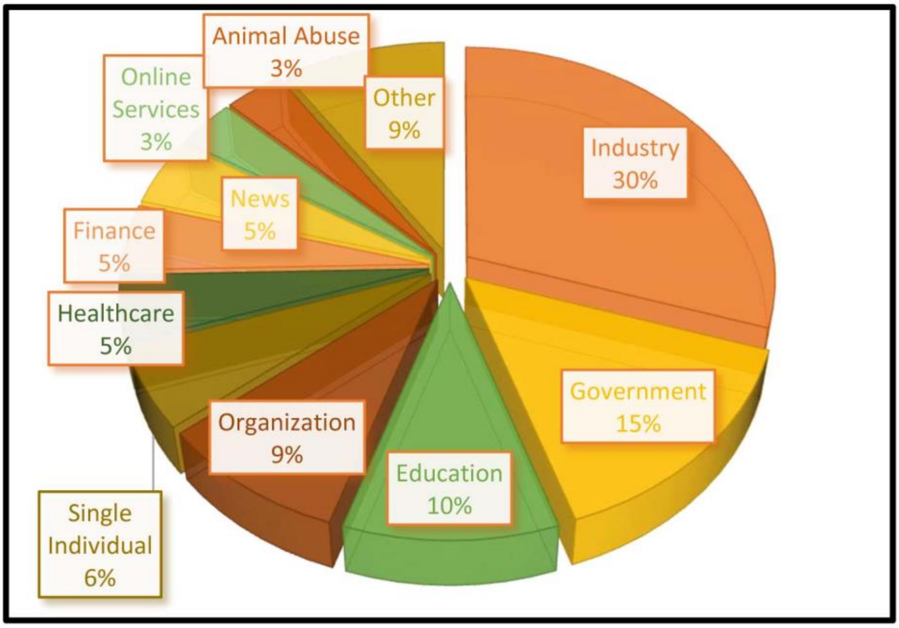


Figure 3. Target of the attacks [18]

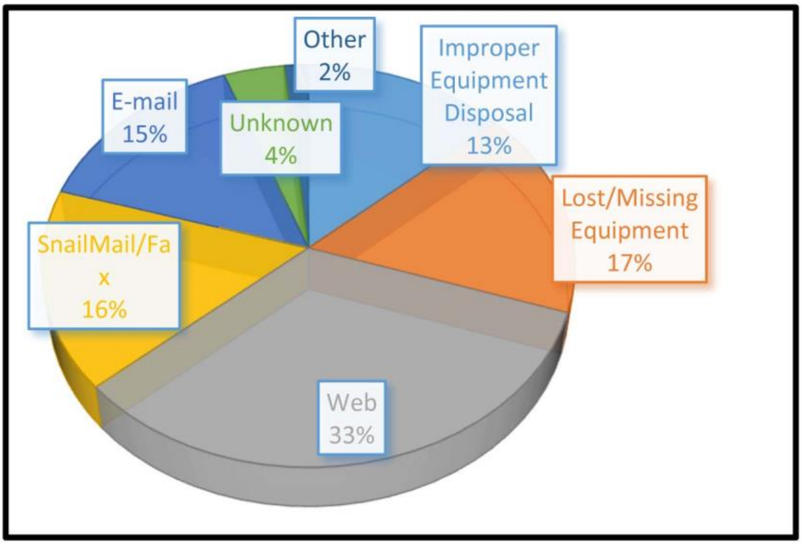


Figure 4. Inside-accidental incidents by breach type [18]

As the previous figures shows that physical damage to hardware and software can be easily measured but the cost of these crimes do not stop there. The more discomforting part of this process is the emotional distress caused to the victims. Photographs, legal documents, and more sensitive information can be made public and accessed by millions of people across the world. This has a long-term effect on cyber-crime victims. Therefore it is necessary to be informed on how people can protect themselves from cyber-criminals.

4. MITIGATING THE RISK

In order to mitigate any risk, we need to understand first the type and nature of the event that creates the risk. The outcome spectrum of that particular risk needs to be evaluated followed by an understanding of the different types of events that can cause it and its various outcomes and consequences. For example, an unsophisticated hacker may cause an accidental event causing a system error results in loss of data that affects the revenue. Another example may be that of a sophisticated hacker who intentionally accesses the system to damage the digital assets or creates system disruption that requires replacement of the physical system components. Other consequences of this type of acts are the loss of revenue due to system downtime, data restoration costs, and verifying the integrity of the data that may have been affected. Therefore, taking into account these events and their consequences a security strategy needs be put in place [12]. With so many techniques being used in cybercrimes, it is recommended that a multi-layer defense mechanism be implemented. Firewalls, along with anti-virus and anti-malware solutions provide a combination of signature-and-intrusion-based detection, heuristic analysis and cloud-assisted technologies can provide a strong defense for the devices and data against new and future threats. However, it is important to include in this strategy to educate the users about all possible threats and how to avoid them.

As of today, the question is not if someone will be breached but when, and, if it does what are you doing to protect yourself? In the late1980s and early1990s, the cyber threats started with unsophisticated attackers who were just experimenting or accidentally created a threat. However, it was not until the Internet became ubiquitous that the next generation of hackers went after systems that had information of some value. The more recent trends, in addition to the now traditionally corporate espionage (where a current or former employee gains financially by selling an intellectual property to the competitor), includes state-sponsored attacks not only of personally identifiable information but military secrets and disability of national defense mechanisms.

5. CONCLUSION

In this paper, the authors, through a series of examples have shown how the computer can be used as a weapon for violence in its most ample definition. The computer, as a medium of communication and sharing information has proven to be both, a blessing and a curse. The computer, if used with mal-intention can inflict tremendous damage upon unsuspected victims and its consequences may last many years. The damages can be both tangible such as physical and mental and intangible such as stolen identity, and exposure of secrets or confidential information. This can be avoided by taking preventive measures that require mostly multi-layered defense mechanism.

BIBLIOGRAPHY

[1] Calif. Governor Brown signs anti-revenge porn bill. (2013, October 1). Retrieved from Fox: http://www.myfoxphoenix.com/ story/23585085/ 2013/10/01/calif-governor-brown-signs-anti-revenge-porn-bill

[2] Cox, R. (2013, August 26). 5 Notorious DDoS Attacks in 2013: Big Problem for the Internet of Things. Retrieved from Silicon Angle: http://siliconangle.com/ blog/2013/08/26/5-notorious-ddos-attacks-in-2013-big-problem-for-the-internet-of-things/

[3] Garcia, M. (2014, February 24). Revenge Porn: Scorned ex-lovers take revenge to a new level. Retrieved from Fox: http://www.myfoxorlando.com/story/ 24811624/2014/02/24/revenge-porn

[4] Gorman, S. (2013, July 22). Annual U.S. Cybercrime Costs Estimated at $100 Billion. Retrieved from The Wall Street Journal: http://online.wsj.com/ news/articles/SB10001424127887324328904578621880966242990

[5] Hahn, A. (2012, September 2). The 8 Creepiest Cases of Identity Theft of All Time. Retrieved from Cracked: http://www.cracked.com/article_19973_the-8-creepiest-cases-identity-theft-all-time_p2.html

[6] Higgins, K. J. (2012, February 7). Law Enforcement Ups Its Game In Cybercrime. Retrieved from Security Dark Reading: http://www.darkreading. com/attacks-breaches/law-enforcement-ups-its-game-in-cybercri/232600423

[7] Hindenach, J. (2013, April 2). Are We Revealing Too Much About Ourselves on Social Media? Retrieved from NextAdvisor: http://www.nextadvisor.com/blog/ 2013/04/02/are-we-revealing-too-much-about-ourselves-on-social-media/

[8] Institute, P. (2013). 2013 Cost of Cyber Crime Study Reports. Retrieved from HP Enterprise Security: http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports

[9] Lyne, J. (2014, January 1). Yahoo Hacked And How To Protect Your Passwords. Retrieved from Forbes: http://www.forbes.com/sites/jameslyne/ 2014/01/31/yahoo-hacked-and-how-to-protect-your-passwords/

[10] Wallace, G. (2013, December 23). Target credit card hack: What you need to know. Retrieved from CNNMoney: http://money.cnn.com/2013/12/22/news/ companies/target-credit-card-hack/

[11] Federal Bureau of Investigation, IC3, NW3C, http://www.ic3.gov/media/ annualreport/2014_IC3Report.pdf

[12] Cyber risks: cause and effect examples (Source: http://www.aon.com/ unitedkingdom/business-risks/attachments/cyber/articles/article-managing-cyber-risk_ten-issues-to-consider.pdf)

[13] Schwartz, M. J. (2013, May 21) Google Aurora Hack was Chinese Counterespionage Operation. Information Week. Retrieved from http://www. darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?

[14] Keizer, G. (2011, Feb 11). 'Sloppy' Chinese hackers scored data-theft coup with 'Night Dragon'. Computer World. Retrieved from http://www.computerworld.com/ article/2513128/security0/-sloppy--chinese-hackers-scored-data-theft-coup-with--night-dragon-.html

[15] Zetter, K. (2014, December 3). Sony got hacked hard: what we know and don’t know so far. WIRED. Retrieved from http://www.wired.com/2014/12/sony-hack-what-we-know/

[16] Federal Bureau of Investigation. Common Fraud Schemes. Retrieved from https://www.fbi.gov/scams-safety/fraud

[17] Hackmageddon, Cyber Attacks Statistics (2015, July 13), Retrieved from http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

[18] Paganini, P (2014, May 9). 2013 Data Breaches: All you need to know. General Security, Retrieved from http://resources.infosecinstitute.com/2013-data-breaches-need-know/

[19] Davis, D (2014, March). Hacktivism: good or evil? Computer Weekly. Retrieved from http://www.computerweekly.com/opinion/Hacktivism-Good-or-Evil

[20] Ranger, S (2014, Dec 19). Sony hack: How cybercrime just got even more complicated. ZDNet. Retrieved from http://www.zdnet.com/article/sony-hack-how-cybercrime-just-got-even-more-complicated/