Acknowledgments

I completed my undergraduate degree at UW-Whitewater in 2008 with a Bachelor of Arts in Sociology with a Criminal Justice Emphasis. I found the study of Criminal Justice to be very interesting, especially the field of cybercrime, and knew this was the area of study I wanted to pursue for my Master’s. Unfortunately in late 2009, I received the diagnosis of Stage 4 Diffused Large B-Cell Lymphoma. After the daunting battle, I am now in remission and back on my educational path. Today, I am earning my Master’s of Science in Criminal Justice Theory from UW-Platteville. This journey has given me a sense of accomplishment and satisfaction that I never thought possible.

My appreciation to those who have assisted me in achieving this goal has to begin with the ongoing support from my family and friends. My entire family has supported me with their guidance and patience throughout this journey and for that I am thankful. To my friends who have encouraged my education and stuck with me even though most of my time was dedicated to my education and to Claire Reinke, my English mentor, for her time and dedication to assure my success in this program. I could not have done this with out you. Lastly, a special thanks goes out to my Grandmother Betty Heller-Hobbs who has given me the financial support to pursue a higher education. She started this path with me even before I knew I wanted it. I will be forever grateful for her foresight.

I want to express an appreciation to all the instructors at University of Wisconsin-Platteville for their knowledge they have shared with me to complete my Master’s program. Personal acknowledgement goes out to Dr. Cheryl Banachowski-Fuller, who has provided me with the direction from the start to finish my Master’s degree and made the process clear and achievable. As a final point, I want to express my utmost appreciation to Dr. Susan Hilal for her
challenging me to go a step further and her guidance she gave me in achieving this challenge through the classes I have taken with her and through the completion of my capstone paper.

Thank you all for helping me complete this journey. I am very lucky and grateful to have had each and every one of you on this path with me.
Abstract

HACKED: RECOMMENDATIONS FOR MINIMIZING CORPORATE ONLINE FRAUD AND IDENTITY THEFT

Kyle S. Heller

Under the Supervision of Dr. Susan Hilal

Purpose

One major problem facing criminal justice is the ability to profile and recognize hacker behavior to be able to administer preventative measures to organizations. Hacking occurs when a cybercriminal commonly known as a hacker, infiltrates encrypted corporate online files (i.e. financial files). In most cases, hackers want to steal credit card information and/or social security numbers for financial gain.

Methods

This paper used secondary sources to discuss hacker demographics and the impact hackers have on corporations. Furthermore, applications of criminological theories to further understand what drives hacker behavior are discussed. The theories that were used in this paper were Routine Activity Theory and Social Learning/Self Control Theory to further understand what drives hacker behavior. Lastly, corporate prevention strategies and recommendations for future research have been provided.

Key Findings

This research has shown that the Internet is a virtual playground for hackers and being educated on the current prevention software and strategies, such as creating strong passwords, is crucial for a company’s data security. Furthermore, if organizations educate themselves on the basic demographics of a hacker, this may give them an advantage when protecting their company
from cyber fraud because, company staff will know what basic cues hacker’s have used in the past. While there are laws against cybercrime, corporations should know the proper protocol if and when their company has been victimized by cyber fraud. Ultimately, a corporation’s goal is to protect their employees’ and customers’ personal data, which can be possible with the proper prevention strategies and being proactive on educating/training their stakeholders against these hackers.
# TABLE OF CONTENTS

Approval Page

Title Page i

Acknowledgements ii

Abstract iv

Table of Contents vi

Sections:

I. Introduction 1
   A. Synopsis of hacking 1
   B. Statement of the Problem 1
   C. The purpose of the research 2
   D. Limitations 3

II. Literature 5
   A. Definitions and Typologies 5
   B. Evolution of Cybercrime 9
      a. Demographics of hackers 11
   C. Penetration Testing 12
      a. Most common hacking styles 12
      b. Scanning and moving through the network 14
   D. Organizational Cybercrime Costs 15
   E. Cybercrime vs. Real World Crimes 16
   F. Global Fraud Comparison 18
   G. Cybercrime Regulations 18
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Global Internet Freedom Task Force (GIFT)</td>
<td>18</td>
</tr>
<tr>
<td>b. The Computer Fraud and Abuse Act</td>
<td>19</td>
</tr>
<tr>
<td>d. Protect the Rights of the Victim: 18 U.S.C. §3771(a)</td>
<td>21</td>
</tr>
<tr>
<td>e. Sarbanes-Oxley Act 2002</td>
<td>22</td>
</tr>
<tr>
<td>f. The Cyber Action Team</td>
<td>23</td>
</tr>
<tr>
<td>III. Theoretical Framework</td>
<td>25</td>
</tr>
<tr>
<td>A. Routine Activity Theory (RAT)</td>
<td>25</td>
</tr>
<tr>
<td>a. Application of RAT to Hackers</td>
<td>27</td>
</tr>
<tr>
<td>B. Social Learning Theory</td>
<td>29</td>
</tr>
<tr>
<td>a. Application of Social Learning to Hackers</td>
<td>31</td>
</tr>
<tr>
<td>C. Self Control Theory</td>
<td>32</td>
</tr>
<tr>
<td>a. Application of Self Control to Hackers</td>
<td>33</td>
</tr>
<tr>
<td>IV. Recommendations for Prevention Strategies</td>
<td>35</td>
</tr>
<tr>
<td>A. Prevention Trends &amp; New Technologies</td>
<td>35</td>
</tr>
<tr>
<td>a. User passwords</td>
<td>36</td>
</tr>
<tr>
<td>b. Biometrics</td>
<td>37</td>
</tr>
<tr>
<td>c. Cloud Data Security</td>
<td>38</td>
</tr>
<tr>
<td>B. Corporate Prevention of Customers Personal Data</td>
<td>39</td>
</tr>
<tr>
<td>C. The future of cybercrimes</td>
<td>40</td>
</tr>
<tr>
<td>V. Recommendations and Conclusions</td>
<td>43</td>
</tr>
<tr>
<td>A. Recommendations for further research</td>
<td>43</td>
</tr>
<tr>
<td>B. Conclusions</td>
<td>44</td>
</tr>
</tbody>
</table>
VI. References
Section I. Introduction

Cybercrime is considered one of the top four economic crimes globally, alongside misappropriation, bribery/corruption, and accounting fraud (Yar, 2013). One major challenge facing this problem is the ability to profile and detect cybercriminals’ activities/behaviors. This is because it is difficult to identify who they are and locate them (Yar, 2013).

Through secondary sources, this paper will provide a literature review of corporate online fraud, identity theft and a theoretical review of cybercriminals, identifying theories as Routine Activity Theory and Social Learning/Self Control. This paper will further discuss methods and profile characteristics of a computer hacker. This information will provide corporations with the knowledge and type of prevention needed to counteract any data breaches that could lead to identity theft.

Statement of Problem

Worldwide, businesses are faced with the real problem of being a victim to cybercrime. Cybercrime includes a lot of different types of crime, but this paper will focus on online fraud and identity theft in United States’ corporations. In 2014, there were several reports about hackers making their way into the computer systems of big companies. In January, 2014, 110 million customer accounts were stolen from Target; in August, 83 million accounts were stolen from J.P. Morgan; in September, an estimated 56 million accounts were breached from Home Depot; and, in December, an estimated 47,000 social security numbers where stolen from Sony (Tobias, 2014). Furthermore, in 2011, Sony was breached and hackers were able to collect information from 77 million accounts and 12 million of those accounts had unencrypted credit card numbers (Fogarty, 2014). These examples express that there is a current problem with cybercrime that comes with a huge cost and demonstrates large corporations’ vulnerabilities.
Cybercrime is a relatively a new phenomenon. The top five worst data breaches in US History included (Armerding, 2012):

1. Heartland Payment Systems (March 2008): 134 million credit cards exposed through SQL injection to install spyware on Heartland’s data system.
2. TJX Companies Inc. (December 2006): 94 million credit cards exposed.
3. Epsilon (March 2011)- Exposed names and e-mails of millions of customers stored in more than 108 retail stores plus several huge financial firms like CitiGroup Inc. and the non-profit educational organization, College Board.
5. Stuxnet (2007-2010): Intended to attack Iran’s nuclear power program, and also served as a template for real-world intrusion and service disruption of power grids, water supplies or public transportation systems.

Purpose of the Research

The purpose of this research is to outline and define the effects of online fraud and identity theft. It will then examine such variables as the financial impact it has on businesses and corporations, the financial impact it has on consumers, methods used by hackers, profile characteristics of a hacker, and corporate prevention methods. Furthermore, the methods of online fraud and identify theft will be reviewed. This paper will also identify and define penetration testing and how hackers apply it to hacking into computer systems. Additionally, the paper will define the typical set up of a penetration testing box and will discuss different types of techniques such as external scanning and web application scanning (Kim, 2014).
**Methods**

With these types of cybercrimes being difficult to stop, successful hacking prevention methods will be discussed. It is of utmost importance that companies educate themselves on the risks of cyberspace fraud. This study will provide further information about these types of cybercrimes in hopes that corporations will take adequate measures to protect themselves and their customers.

Everyday companies are using the Internet to create new accounts, make payments for invoices, send e-mails, transfer money, etc. The wide use of the Internet for sensitive information provides openings for hackers to get inside and penetrate companies’ classified data.

The use of laptops, iPads, tablets and cell phones allows people to have access to the Internet at all times. This wide use of Internet compatible devices allows anyone with hacker knowledge to get to know a corporation’s routines, which provides a hacker with the perfect opportunity to strike. However, even though companies have preventative software and often have the technology staff to prevent hackers from penetrating their software, hackers are still able to outsmart corporate prevention efforts by knowing the common computer programming languages.

**Limitations**

The ability to categorize and understand what cybercriminal behaviors entail is far from being permanently defined. A couple significant limitations facing state and federal law enforcement officials is being up to data with cyberspace and the crimes embedded within it and what law officials are looking for (i.e. behavioral cues) when investigating hacking. Is hard to ensure that tools like, computer monitoring software, are being properly used by law officials to analyze hacker behaviors.
In this study another limitation is the use of secondary sources because the information reported from these sources are past studies and potentially outdated. These secondary sources provide suggestions that are relevant today and may be outdated in the years to come; whereas, a primary study may provide more accurate suggestions.
Section II. Literature Review

The following is divided into seven sections that assist in providing a full description of a computer hacker. Initially this section includes definitions and typologies of hackers and then discussion of the evolution of cybercriminals and hackers. Next, a further description of the demographics of a hacker and how they use penetration testing to scan through the network to retrieve personal data. A discussion of how organizational crimes costs corporations and then compares cybercrimes versus real world crimes along with a global comparison of most the prevalent crimes in select countries is then provided. Finally, a description of cybercrime regulations, which include task forces, acts and action teams.

Definitions and Typologies

Hacking is defined as “illicit and usually illegal activities associated with unauthorized access to, or interference with, computer systems” (Yar, 2013, p.173). A very simple typology is that which classifies hackers into two types—hackers who work in groups and hackers who work alone. The hackers who work alone are known as lone hackers and work independently to increase their feeling for security, whereas, hacker groups provide a psychological support for their members by sharing responsibilities. Being involved in a hacker group provides support in finding a hacker’s personal identity. Both kinds of hackers initially seek out an experienced hacker to help mentor them through their growth. At the time when a hacker feels confident enough to no longer need a mentor, he usually places himself in either a hacker group or decides to be a lone hacker (Kirwan & Power, 2013).

Roger (2003) categorizes of hackers starting with beginners to experts; categories include: newbie/tool kit, cyber-punks, internals, coders, old guard hackers, professional criminals, and cyberterrorists (as cited in Kirwan & Power, 2013). Each of these categories
identifies the level of programming skills and knowledge a hacker possesses and what kind of computer equipment and software the hacker might be using to attack. For example, a newbie/toolkit would be a person with limited programming skills and will rely on already developed software to follow through with a hacking attack. Subsequently, a professional criminal could specialize in corporate espionage and could be well trained with the programming skills and the knowledge of the proper computer equipment needed to execute a hacking attack (Kirwan & Power, 2013).

Another typology is presented by Grabosky (2014) who identifies how cybercriminals may classify themselves, to include: 1. Coders—or programmers who write the malware, exploits, and other tools necessary to commit the crime; 2. Distributors—or vendors who trade and sell stolen data, and vouch for the goods provided by the other specialties; 3. Technicians—maintain the criminal infrastructure and supporting technologies, such as servers, ISPs, and encryption; 4. Hackers—search for and exploit vulnerabilities in applications, systems, and networks in order to gain administrator or payroll access; 5. Fraud specialists—develop and employ social engineering schemes, including phishing, spamming, and domain squatting; 6. Hosts—provide ‘safe’ facilities of illicit content servers and sites, often though elaborate botnet and proxy networks. 7. Cashers—control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or money mules; 8. Money mules—transfer the proceeds of frauds, which they committed to a third party for further transfer to a secure location; 9. Tellers—assist in transferring and laundering illicit proceeds through digital currency services and between different currencies; and 10. Executives—select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceedings (p. 6-7).
Yet another typology is presented by Secpoint (2015) to include: **White Hat:** A white hat hacker is someone who has non-malicious intent whenever he breaks into security systems. In fact, a large number of white hat hackers are security experts or penetration testers who are specifically hired to test out the vulnerability of a system; **Ethical Hacker:** An ethical hacker is a white hat hacker who performs vulnerability assessments and penetration tests; **Black Hat:** A black hat hacker, also known as a cracker, is the type of hacker that has malicious intent when breaking into security systems without authorization using technology such as network, phone system, and/or a computer. The purpose of this breach is to attain identities, credit cards, and vandalize sites; **Grey Hat:** A grey hat hacker is someone who exhibits traits from both white hats and black hats. This hacker will surf the Internet for vulnerable systems that could be exploited. This type of hacker will not penetrate the system, but rather find loopholes within the sites; **Elite Hacker:** An elite hacker is someone who has mastered deception and has earned a solid reputation among their peers as “cream of the crop” or “the best of the best; **Script Kiddie:** A script kiddie is an amateur or non-expert hacker wannabe who break into computer systems through other software and tools written by real hackers. These tools are called prepackaged automated scripts and are used by these script kiddie’s with no underlying knowledge of how these scripts work; and a **Cracker:** A cracker is considered a violent hacker where their intent is to delete files and cause permanent damage (Kirwan and Power, 2013).

After a hacker has defined what kind of job they want to contribute to a cybercrime group, they decide the type of group they want to be part of; in most cases they fall under the same type as their mentor. Grabosky (2014) identifies Michael McGuire’s three different types of typologies of cybercrime groups. These typologies are divided between members depending on the strength of the members (p.8):
- **Type I**—groups operate essentially online and can be further divided into swarms and hubs. They are mostly ‘virtual’ and trust is assessed via reputation in online illicit activities.

- **Type II**—groups combine online and offline offending and are described as ‘hybrids’ which in turn are said to be ‘clustered’ or ‘extended.’

- **Type III**—groups operate mainly offline but use online technology to facilitate their offline activities. This group can be subdivided into ‘hierarchies’ and ‘aggregates’ according to their degree of cohesion and organization.

Corporations can protect themselves from cyber-attacks by knowing the common types of hacking attacks. The three common types of hacking attacks are infiltration, defacements, and denial of service (DoS)/distributed denial of service (DDoS) (Kirwan & Power, 2013). Infiltration is “…gaining an access or entry into a physical location, an organization, a nation, or some other target opportunity…entry without authorization” (Gragido & Pirc, 2011, p.156). Defacement, commonly associated with websites, is when a hacker makes noticeable changes on the corporation’s website. The most common style of defacement is SQL (Structured Query Language) Injection, which allows the hacker to gain administrative access and view passwords and other classified information (Kirwan and Power, 2013). Denial of service (DoS) is “an attack on a networked computer or computers that disrupts normal operations to such an extent that legitimate users can no longer access their services” (Yar, 2013, p.172). Distributed Denial of Service (DDoS) targets one particular website and attempts to overload the web servers to make the site unavailable (Yar, 2013).
Evolution of Cybercrime & Hackers

In the past, computer companies and businesses used filing cabinets as their main use of information storage, such as, employee’s personal information (i.e. social security number), business financial information, human resources files, etc. Today, most everything is now stored and kept on computer systems, making it easier for hackers’ to infiltrate information. Through the ‘70s, ‘80s, and ‘90s the idea of cybercriminals and their capabilities was still in the alpha stage.

In the early 2000s, 3 basic trends of cybercrimes were identified: sophistication, commercialization, and organization (Grabosky, 2014). Sophistication is when “…the complexity of methods by which cybercrime is executed” (Grabosky, 2014, p.2). Commercialization is when “…the salience of profits and markets as motivations for cybercrime” (Grabosky, 2014, p.2). Organization is the “…apparent diversity of organizational form of representation in recent cybercriminal activity” (Grabosky, 2014, p.2).

Pagliery (2015) reviews the history of hacking by providing a decade-by-decade description of how hackers have revolutionized. The concept of “hacking” originated 50 years ago at the Massachusetts Institute of Technology. A group of computer science students started to use the term after learning about a group of model train enthusiasts from 1969 who “hacked” electric train tracks and switches to improve the train’s performance. Hacking became associated with ways to figure out unique solutions; in the beginning hackers wanted to make technology work better and tried to find different ways to make technology have different solutions. The first generation of hackers started in 1971 and these hackers were categorized as “American punks” who began infiltrating with the nation’s telephone system. These hackers would make international phone calls just to get a sense of how the telephone network worked.
In the 1980s, this generation of hackers would use their personal computers and hook them up to the telephone network. At this time the World Wide Web was not yet sophisticated, but these hackers were able to get these computers to communicate with each other through the telephone network. Additionally, these hackers found a way to break into company computer networks and would make these computers communicate with printers that were miles away to eject paper from the machine. These hackers were the first to start a text-only bulletin board to talk about their hacking schemes and provide tips and stories about their hacking adventures; this was the beginning of hackers working in groups (Pagliery, 2015).

In the 1990s, the battle between hackers and law enforcement seemed to grow throughout this decade. These hackers were out to commit crimes, which included stealing money from banks and or wiping information off of computers. With computers becoming more relevant in homes, businesses, hospitals and credit card institutions, this opened many more opportunities for hackers to commit more cybercrimes (Pagliery, 2015).

In the 2000s, hacking was now a organized crime that involved writing malicious software, also known as malware, to compromise computer networks. The most common method hackers would use to get this malware into business computers was through spam e-mails. When the employee would open the e-mail it would infect the computer; for example, hackers would send these e-mails to banking institutions in hopes that an employee would open up the link in order to infect the computer to allowing the hacker to steal login credentials. Hackers today are using different tactics to get the information they need; they do not need to wait for an employee to open up e-mails to infect their computer. Hacking has become an out of control situation and is something that is happening globally (Pagliery, 2015).
Demographics of Hackers

There are several demographic characteristics of hackers, which include:

1. Hackers are mostly younger males. While there are some exceptions, most research to date supports this stereotype (Kirwan & Power, 2013). Today, the average age for most hacker’s ranges from 30 to 35 years old, whereas about 15 years ago it was assumed that most hackers belonged to the teenager/adolescent age group (Chiesa, Ducci & Ciappi, 2009).

2. Hackers have also been found to have good educational levels (Kirwan & Power, 2013).

3. Hackers are sometimes students or trainees, and can have above average income levels (Kirwan & Power, 2013).

4. Usually hackers dress causally and are good looking (Chiesa, Ducci & Ciappi, 2009).

5. Many hackers are categorized as having a normal lifestyle by which they are sociable, have many friends, participate in sports, gets good grades, have relationships, and are said to be pleasant individuals (Chiesa, Ducci & Ciappi, 2009).

In some cases the above profile does not apply. For example, Black Hat Hacker Kevin Poulsen, hacked by taking over the phone lines of a Los Angeles radio station to guarantee he would be the winner of a car. Poulsen was a man who was considered a loner but on some occasions would hang out with his fellow hacker friends. He also considered sports a waste of time, especially at a professional level because of the competitiveness (Chiesa, Ducci & Ciappi, 2009).
Penetration Testing

Most Common Hacking Styles

There are 10 ways a company can become hacked, as outlined by Michelle (2012):

1. **Email Social Engineering/Spear Phishing:** This is one of the most common tactics used to implant code when attacking a network to obtain access. The hacker invests time and effort to get familiar with the details about the target. When a hacker targets a high level executive, this is called “whaling,” and the hacker attempts to infiltrate the executive’s computer using infected emails to gather confidential information about the organization (Kirwan & Power, 2013).

2. **Infection Via a Drive-By Web Download:** This style of attack can affect government or company websites. Hackers will implant a code within a website so when a person opens up that website, their computer will become infected.

3. **USB Key Malware:** Malware, is a hazardous code that could contain a worm which is “a type of malware that spreads automatically over a network, installing and replicating itself” (Singer & Friedman, 2014, p. 299). Trojan horse is “malicious software programs which infiltrate into computers disguised as benign applications or data” (Yar, 2013, p. 177) or virus which are “pieces of computer code that can ‘infect’ computer systems causing disruption to their normal operation” (Yar, 2013, p.177). Malware could be downloaded into a computer through a USB key.

4. **Guessing or Social Engineering Passwords:** A hacker might send an email asking the employee to reset their password. When the employee resets their
password, the hacker is able to remotely log into the computer system. Hackers are able to obtain passwords by obtaining employee credentials.

5. **WiFi Compromises:** Wireless Fidelity, known as WiFi, is usually secured with passwords; however, hackers are able to get into a system through unsecured or poorly secured wifi. Smaller businesses may be more prone to this style of attack because of poor security.

6. **Stolen Credentials from Third-Party Sites:** In some cases people tend to use the same username and password for both home and work allowing hackers multipoint access.

7. **Compromising Web-Based Databases:** Some websites ask for emails or credit card numbers that are stored on those sites. Hackers may use that information to exploit a company’s system.

8. **Exploiting Password Reset Services to Hijack Accounts:** Like social engineering, employees are asked to reset their passwords. In this case, once the passwords are changed, the hacker would have unlimited access to e-mail accounts.

9. **Insiders:** Insiders, also known as *cyber spies*, find ways to get hired into companies and then try to get into the system. In other cases, employees can be bribed or conned into helping a hacker hack into the system.

10. **Scanning Network for Vulnerabilities and Exploitation:** When hackers find vulnerability, they will send a command or data to the server that will cause the application to crash. When the server has crashed, the hacker is able to start placing code.
Scanning and Moving Through the Network

Hackers exploit the vulnerabilities of a network by determining if there is a way inside the network without causing any suspicious activity use penetration testing. To understand how hackers access an organization, Kim (2014) explains that hackers scan the network by using external scanning, internal scanning, and web application scanning. With using these three methods, the hacker will be able to get to know the target by knowing the services and the people within that network. Using both passive and active scanning hackers learn of vulnerabilities, applications and a host(s) (Kim, 2014).

A penetration tester should become familiar with writing scripts and how to “…edit, modify, execute, and understand regardless of the language…” (Kim, 2014, p.62). Additionally, hackers usually execute a script after they have not tested it first. This allows a hacker to get familiar with the scripts because time is of the essence when testing the network. Once a hacker has selected a target and a script, he is now able to exploit the web vulnerabilities. A hacker could perform these tests by choosing either: SQL injection, cross-site scripting (XSS), session token entropy, input validation, or cross-site request forgery (CSRF) (Kim, 2014).

Ideally a hacker can move through the whole network rather than just being a limited user. A limited time user would be classified as a hacker who is working through the network without credentials (non-administrative access) and proxying through hosts. A hacker moves through the network through limited domain credentials and then eventually collects domain credentials. When a hacker has domain credentials they are able to move through the whole network successfully (Kim, 2014).

Another form of breach is identity breaching where it can affect employees from directly inside the corporation. By using hackers, known as insiders, who are employees can use their
access to breach personal and financial information of co-workers. An employee could phish though a co-worker’s computer files or trash files. In some cases, an employee could be bribed into working with an outsider to attain this information for personal financial gain (McWhinney, 2015).

**Organizational Cybercrime Costs**

A hacker’s ultimate goal is to profit from the crime, which results in cyber security costs to the organization. Rawlinson (2014) reports that an average annualized cost of cybercrime per organization is $12.7 million, an increase of $1.1 million (9%) over the average cost in 2013. The highest external cost of cybercrime for organizations is information theft, followed by business disruption. The highest internal cost is recovery and detection accounting for 49 percent of the internal annual cost.

Additionally, Ritchey (2014) reports that many organizations may experience an average of 122 hacking attacks per week. Each of these attacks can take up to 32 days to resolve these attacks and can cost $32,469 per day. Bernik (2014) identifies the categories associated with finding the cyber attack to recovering from the attack. These categories each involve expenditures of resources (p.111): 1) *detection*—activities that enable an organization to reasonably detect and possibly deter cyber attacks or advanced threats; 2) *investigation and escalation*—activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incident; 3) *containment*—activities that focus on stopping or lessening the severity of cyber attacks or advanced persisted threats; 4) *recovery*—activities associated with repairing and remediating the organization’s systems and core business processes; and 5) *ex-post responses*—activities to help the organization to minimize potential future attacks and add new enabling technologies and control systems.
It should be noted that small businesses are the most vulnerable. According to the Police Executive Research Forum (2014), most hackers attack smaller businesses that have fewer than 1,000 employees. Unfortunately, these small businesses do not have the resources to properly respond to these attacks themselves or the capital to absorb the losses they may endure. In some cases, hackers may not steal money from these businesses but rather steal personal customer data. It is reported that about sixty percent of smaller businesses that fit this profile go out of business within six months.

**Cybercrime vs. Real World Crime**

Criminals today focus on crimes that are easier to commit and are less likely to be prosecuted. Therefore, criminals are using cyberspace rather than attacking the victim personally. Nevertheless, either method of attack has the same benefits of criminal intent (profit) and outcome (stolen personal identifiable information) (Finklea & Theohary, 2015). Society and law enforcement seem to be struggling with the new development of the cyber world. These new developments provide a new level of risk for law enforcement because in some cases these officials might not be provided the protection citizens are expecting. In some cases, police department might not be provided enough money in the budget to develop a cyber unit.

Today it is not as easy as shredding paper-based personal documents, but rather worrying about being victim of a cyber-attack where one’s electronic personal documents are copied. Yar (2013) explains that making the transition from traditional pen and paper to the virtual environment gives online cybercriminals the upper hand. Furthermore, Yar (2013) warns society that one can expect the ongoing growth in cyber-frauds, scams and cons as the cyber world becomes more advanced. Holt (2013) states that, “there is a need to understand the overlap
between real-world routine activities and cyber activities and their role in online victimization as a whole” (p.63).

In the “real” world, criminals must personally and physically commit the crime; for example, a criminal could steal a victim’s wallet or mail that contains documents that identify personal information about the victim. In one case in 2011, two men were sentenced in South Florida for stealing credit and debit cards from personal mailboxes. These two men used these cards to purchase large items as well as withdrawing cash amounting $786,000 (Finklea & Theohary, 2015).

In the cyber world, using a virtual environment has given cybercriminals a sophisticated advantage. For example, one case in 2013 identified two Romanian nationals who participated in a multi-million dollar scheme to remotely attack by hacking into hundreds of U.S. merchants’ computers and stealing their personal payment information. The defendants used the method of installing “keystroke loggers” into point of sale systems. This system captured and transferred the payment information when merchants would swipe their cards. The information from more than 100,000 cardholders were then sold for a great sum of money (Finklea & Theohary, 2015). In some cases, hackers may sell the personal information online for 1-3 dollars and if they sell those 100,000 cards they could make up to $100,000 to $300,00 just off of one hack.

Humer and Finkle (2014) also state that hackers may sell someone’s medical information and can sell it for more money than selling credit card information. For example, in China over 4.5 billion patients medical information was stolen by hackers and then was sold on the black market. Furthermore, this medical information can be sold for $10 each and is 10 to 20 times more profitable than a stolen credit card number. This demonstrates that all industries need to be mindful.
Global Fraud Comparison

Globally all countries experience cybercrime. Kroll’s (2014) Global Fraud Report 2013/2014 compared and surveyed 12 different countries by their international corruption with fraud. Regardless of a country’s status in the global economy, highly developed countries such as the United States, Canada, and China have experienced regulatory and compliance fraud, information fraud, and theft of physical assets/stock. Developing countries such as Mexico, Brazil, Colombia, Malaysia, India, and Africa have experienced international financial fraud, corruption and bribery, procurement fraud, and theft of physical assets/stock. It does not matter how developed or undeveloped a country is, they can be vulnerable to cybercrimes (i.e. fraud).

Cybercrime Regulations

Cybercrime is global because of the availability to Internet access. To help combat the increasing rate of cybercrimes, Bills, Acts, and Regulations have been set into place throughout U.S. History.

Global Internet Freedom Task Force (GIFT)

The Global Freedom Task Force (GIFT), later renamed the NetFreedom Task Force, was launched in 2006 by the Department of State. GIFT’s foreign policy objective “is enhancing global Internet Freedom by monitoring human rights abuses and enhancing access to the Internet through technical and financial support for increasing availability in the developing world” (Finklea & Theohary, 2015, p.26). In other words its purpose is to, “protect and defend a free and open Internet” (Figliola, 2013, p.2).

GIFT was organized around three principles (United States Department of State, 2006):

1) Monitoring internet freedom in countries around the world by interim monitoring and spotlighting abuses of Internet freedom; 2) Responding to challenges to Internet freedom by
protecting abuses and raising awareness, sustaining persuasion in meetings with foreign officials, coordinating with international partners, maintaining and expanding Internet Freedom commitments in multilateral organizations and working with stakeholders; 3) Advancing Internet freedom by expanding access to the Internet by expanding access in developing countries, empowering users, and Grant funding. This task force overseas over 40 countries to educate and motivate individuals to circumvent political censorship and train in accessing the Internet safely (Figliola, 2013).

The Computer Fraud and Abuse Act

In the United States, the Computer Fraud and Abuse Act (CFAA) law of 1986 is a cyber security law that prohibits any malicious activities that could result in organizations being victimized through computer systems breaches. This act offers protection from threats, espionage, damage, or from any instruments that could infiltrate an organization’s computers that are connected to the Internet such as federal or bank computers. This Act covers such crimes as:

1.) 18 U.S.C. §1030—accessing a computer without authorization to collect restricted data, which could include accessing federal computers; 2.) 18 U.S.C. §1361-1362—prohibits malicious actions and computer hacking and/or website defacement (Doyle, 2014).

Common offenses under the Computer Fraud and Abuse Act are as follows (Jarrett, Bailie & Hagen, 2014, p. 3):

- Obtaining national security information
  - First offense: 10 years, Second offense: 20 years

- Accessing a computer and obtaining information
  - First offense: 1 or 5 years, Second offense: 10 years

- Trespassing in Government Information
First offense: 1 year, Second offense: 10 years

- Accessing a computer to defraud and obtain value
  - First offense: 5 years, Second offense: 10 years

- Intentionally damaging by knowing transmission
  - First offense: 1 to 10 years, Second offense: 20 years

- Recklessly damaging by intentional access
  - First offense: 1 to 5 years, Second offense: 20 years

- Negligently causing damage and loss by international access
  - First offense: 1 year, Second offense: 10 years

- Trafficking in passwords
  - First offense: 1 year, Second offense: 10 years

- Extortion involving computers
  - First offense: 5 years, Second offense: 10 years


18 U.S.C. §1030(a)(4) forbids fraud by computer intrusion. To elaborate, this section protects victims from cybercriminals who knowingly and have the intent to defraud access protected (password and or coded) computers without authorization or exceed authorization, and collect anything of value.

Violations under 18 U.S.C. §1030(a)(4) are “punishable by imprisonment for not more than five years (not more than 10 years for subsequent) and/or fine of not more than $250,000 (not more than $500,000 for organizations” (Doyle, 2014, p.53). Additionally, 18 U.S.C. §1030(a)(4) states a, “conviction of a [§1030(a)(4)] offense requires a victim restitution order
and may lead to the confiscation of the fruits and instruments of the offense. Victims may sue for compensatory damages and/or injunctive relief subsection 1030(g)” (p.53).

Jarrett, Bailie and Hagen (2014) address four categories that fall under 18 U.S.C. §1030(a)(4) and an individual could be convicted if one is knowingly accessing a computer without or in excess of authorization, if one has the intent to use a computer to defraud, using computer access to further the intended fraud, and if using a computer obtains anything of value.

**Protect the Rights of the Victim: 18 U.S.C. §3771(a)**

Law enforcement should make the effort to work one on one with companies to build a relationship between the two because, in the event of an investigation, there is a chance that they will be willing to cooperate without any hassle. When law enforcement is investigating a cybercrime, they should ensure the rights of the victim by (Jarrett et al., 2014, Appendix C): A) reasonable protection from the accused; B) accurate and timely notice of court proceedings involving the crime or any release or escape of the accused; C) not excluding the victim from any such public court proceeding, unless the court determines that testimony by the victim would be materially altered if the victim heard other testimony at the proceeding; D) allowing the victim to be heard at any public proceeding in the district court involving release, plea, sentencing, or probation; E) conferring with the government attorney on the case; F) offering full and timely restitution as provided in law; G) proceeding free from unreasonable delay; and H) fair treatment with respect for the victim’s dignity and privacy.

Furthermore, when law officials’ work with companies regarding a cybercrime, they should consider consulting with senior management, consult with information technology staff, minimize disruption to the company, and keep the company informed about the investigation
(Jarrett et al., 2014). These could be considered key variables to an investigation and how the business community views criminal justice.

**Sarbanes-Oxley Act of 2002**

President Bush signed the Sarbanes-Oxley Act into law on July 30, 2002. The Sarbanes-Oxley Act “…mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the ‘Public Company Accounting Oversight Board,’ known as he PCAOB, to oversee the activities of the auditing profession” (U.S. Securities and Exchange Commission, 2014).

Sarbanes-Oxley Act of 2002 defines the types of records that are required for recording and how long a company must hold onto these records, including company e-mails. Additionally, all businesses are required to keep paper records and electronic records (including electronic messages) to be saved and secured for not less than 5 years. This act also handles any destruction or falsification of company data and holds company executives directly responsible for any company problems.

The Sarbanes-Oxley Act of 2002 contains specific Titles that refer to corporate fraud: 

**Title VIII**—Corporate and Criminal Fraud Accountability identifies that knowingly destroying or creating any document(s) to obstruct, impede or influence a federal investigation is considered a felony and subject to being fined (under Title 11) and/or be imprisoned not more than 20 years. 

**Title IX**—White Collar Crime Penalty Enhancements identifies crimes of tampering with records and/or attempting/conspiring to commit fraud; the criminal penalties depend on the approach (i.e. mail or wire fraud) of the crime. 

**Title XI**—Corporate Fraud and Accountability identifies crimes of altering, destroying, mutilating and/or conceals a record/document with the intention to impair
the document’s integrity or make the document unable to use in an official proceeding. This is considered a felony and be fined (under Title 11) and/or be imprisoned not more than 20 years.

**The Cyber Action Team**

When a corporation has been notified that they have been victim of a hacking where hackers have infiltrated the companies network and was able to steal trade secrets, customer’s personal data, employee personal data, and other company data, the corporation should contact the Federal Bureau of Investigation (FBI)(2015). When the FBI is notified about a cyber attack, the Cyber Division will send over the Cyber Action Team, known as CAT, which was established in 2006 by the FBI’s Cyber Division. This action team is comprised of groups of cyber experts that are able to assist with investigations involving cyber-attacks. Typically, this team has about 50 members located in field offices around the United States, which include special agents or computer scientists who have advanced skill training in computer languages, malware analysis, and forensic investigations (FBI, 2015).

After a company has notified the FBI (2015), usually CAT will be at the company within 48 hours to start the investigation process and further assist in answering critical questions that will aid with moving the case forward as quickly as possible. Moreover, in some corporate cases CAT might be required to investigate cases abroad due to corporations work with international partners. Wherever this team is required to go, these professionals will use the tools, techniques, and the most successful procedures to find the hackers who have penetrated the network. In most cases, corporate victims are surprised how much of the network was compromised by the hackers. Also, there have been many cases where corporations are notified that the attack primarily began months to even years before the attack was discovered. Hackers are becoming
more and more sophisticated and can feel like they are steps ahead of the FBI and CAT (FBI, 2015).

**Summary**

When identifying a hacker and identifying the behavioral characteristics of a hacker, one must know what patterns and/or styles these cybercriminals use. While criminologists identify and implicate past cyber behaviors, these officials can prepare a standard model of what to look for in a hacker. More specifically, what to look for in a hacker that attacks corporations by understanding what type of hacker they identify themselves as (black, white or grey hat) and what kind of method they use to penetrate the network. It is beneficial to understand the difference between real world criminals and cyber world criminals and to get familiar with past cases to apply their methods to prevent current crimes whether they are real world or cyber world crimes. It is also beneficial to have a global understanding of corporate cybercrimes and how they compare to the United States Cybercrime problem. One should also understand past laws and bills set in place for global use of the Internet as well as understand laws of corporate fraud.

With a through knowledge of cybercrime and cybercriminals, corporation will be better persuaded to manage their exposure to cybercrime. Additionally, criminologists will have a better understanding of cybercriminal behaviors and methods.
Section III. Theoretical Framework

Understanding the routines and learning processes of a hacker can help facilitate a perception of their behaviors and motivations. Routine Activity Theory, Social Learning Theory, and Self Control Theory can assist in identifying the reasons of how hackers’ choose their victims and how they learn and master their craft (methodology). Consideration of these theories may assist by protecting companies from a cyber-attack and may play a contribution to the next prevention software.

Routine Activity Theory

Routine Activity Theory (RAT) originated in 1979 by Lawrence Cohen and Marcus Felson. RAT identified three factors that come together to create a high likelihood for victimization and crime (Tibbetts & Hemmens, 2010). The three factors that Cohen and Felson defined were: (1) Motivated offenders such as teenage boys, unemployed, drug addict gang member(s); (2) Suitable targets like unlocked homes, expensive cars, easily transportable goods, and electronics (i.e. cell phones, iPods, laptops/computers); and (3) Lack of capable guardians such as parents, neighbors, security systems, homeowners, and/or police officers; all three put together present opportunity for delinquency (Wadsworth & Thomson, 2006). Furthermore, places where these three elements unite in time and place are called “Hot Spots” (Tibbetts & Hemmens, 2010).

Tibbets and Hemmens (2010) ascertain that individuals commit crimes during daily routines of their victims. Therefore, their targets are more likely to be victimized if they are categorized as poorly guarded and are surrounded by a large number of motivated offenders. Tewksbury and Mustaine (2010) discuss five factors that increase the risk of victimization:
demographics, alcohol and drug use, economic status, social activities, and community structures.

Tewksbury and Mustaine (2010) discuss these five factors using Routine Activity Theory and their significance with victimization. Demographic factors are interpreted by proxy measures (indicators) of lifestyle activities. For example, a married couple might not be as likely to be victimized than a single individual. An individual living a single lifestyle may indicate that they prefer to socialize more outside the home in more public settings (i.e. nightclubs) versus staying home. It is highly beneficial for criminals get familiar with their victim’s actual lifestyle activities so that the risks of being caught are much more infinitesimal.

Alcohol and drug use patterns of potential victims allow criminals to familiarize themselves with certain locations their victim’s frequent. For instance, a victim might leave their home for a couple hours to meet up with friends at a local bar. The criminal might have observed their victim is usually out for a couple hours, which gives the criminal the opportunity to victimize the home. Tewksbury and Mustaine (2010) explain that cases dealing in alcohol and drug use usually result in violent behaviors. So, in the previous example, the criminal might want to casually “run into” their victim at the bar they are visiting. The criminals may be hoping that the victim will extend an invite for them to join him or her at their house, which may open an opportunity for the criminal to victimize the individual or the home.

Social activities of a victim can have a significant effect on what influences the risk of being victimized. Criminals who analyze their victims’ social activities know what behaviors their victims have (i.e. posting on social media such as Facebook/Twitter that the family is going on a weeks vacation); furthermore, criminals base their attack according to what will allow fast and easy outcomes. For example, this method may be used by killers/murders rather than a
criminal who is just looking to steal someone’s credit card. So the types of social activities an individual engages in can put a person at risk of being victimized (Tewksbury & Mustaine, 2010).

Economic status and community structures can play a part of routine activity theory. Individuals who are in lower income communities may be more vulnerable to being victimized; for example, lower income people may not have needed guardianship (alarms or persons) to prevent themselves from becoming victimized. These community structures allow criminals to easily get familiar with the domains within the community, allowing criminals to distinguish what targets can be effortlessly assessed (Tewksbury & Mustaine, 2010).

**Application of Routine Activity Theory to Hackers**

Holt (2013) reports that routine activity and its relation to cyberspace is limited because individuals may connect and disconnect and might be connected for short periods of time. Therefore, cyberspace users are more difficult to create a social situation contour where cybercriminals (i.e. hackers) are able to construct a lifestyle-routine activity profile of their victims. Cybercrime victimizations can come in many different forms, a couple example are cyberstalking and harassment, child predation and/or cyber fraud.

Chon and Broadhurst (2014) argue whether offender resources play a factor in their abilities to carry out any form of a cybercrime. For example, using the same kind the same routine activity model stated previously (motivated offender, lack of guardian, and suitable target), Chon and Broadhurst suggest that motivation can be used as an offender resource and can affect all three RAT factors. A hacker must be motivated to educate themselves with the current hacking techniques, an in depth understanding of operating system internals, neutralizing online criminal behavior, a knowledge of target vulnerabilities, know how to program exploit
code, reinforcing criminal behaviors influenced by the self-fulfilling prophecy of being a hacker/cybercriminal, and becoming familiar with common psychological assumptions of a hacker/cybercriminal (i.e. anti-social behaviors) (Chon & Broadhurst, 2014).

The RAT Model is currently used as a primary model to assist in analyzing future cybercrime tactics. By using the RAT Model to predict cybercrime developments, criminologists could restrict the availability of certain resources such as “crimeware”. Crimeware is malicious software used by hackers to carry out many forms of illegal online activity. Placing these limitations on hacker resources may carry huge benefits in understanding online criminal activities (Chon & Broadhurst, 2014).

Before criminologist can apply theories such as RAT to explain corporate fraud victimization, they must first understand the individual side of victimization. Fraud victimization is only going to continue to grow as opportunities for online activity keep expanding. Furthermore, people are going to become more and more comfortable using online services, which can potentially make them more vulnerable to cyber fraud. One major key factor is to understand cybercriminal targeting and by using past victim studies criminologists can apply what they have learned from previous hacker routine activities. Currently, criminologist are evaluating and uncovering key factors that are related to cyber fraud and cybercriminals/hackers methods when picking their targets. Using RAT as a framework for current prevention studies has been proven to be beneficial. The routine activity perspective for the last three decades has been a successful foundation for criminal victimization for both offline and online literature (Pratt, Holtfreter, & Reisig, 2010).

In a similar manner to real world crimes, cybercrimes can use the same kind of three factors outlined. Kirwan and Power (2013) identify these three factors using cybercrime
identifiers: (1) Suitable targets are desirable to a hacker because of the organization that owns it. (2) Unprotected guardians would be the lack of adequate antivirus or firewall software. (3) Motivated offenders are hackers who obtain private information by taking control of the computer (p.25). The use of rational choice theory can be applied to most types of malicious online behaviors and using these three factors allows further interpretation of how and why cybercrime behaviors occur (Kirwan & Power, 2013).

**Social Learning Theory**

Social learning theory originated in 1977 by Albert Bandura, who identified behaviors being learned from the environment and through observation learning techniques. Furthermore, Bandura discusses modeling/imitation which Edwin Sutherland’s differential association theory was the beginning theory that introduced observing interactions among people and studying the behavioral responses. Bandura’s Social Learning Theory has assisted in understanding criminal behaviors; for example, if one is taught and rewarded for criminal acts by people that they socialize with (peers/teachers) or live with (parents), this individual-learned behavior has been taught to have positive benefits (Tibbetts & Hemmens, 2010).

Before Bandura formulated Social Learning Theory, Bandura and a couple colleagues in 1961 designed an experiment called the BoBo Doll Experiment, which tested 36 boys and 36 girls ages 3-6 from Stanford University’s Nursery School. During the test they measured the children’s aggressiveness levels using a 5-point rating scale and then putting the childrens’ into group depending on their aggressive levels (matched pair design). The 72 children were then placed into three different models: the aggressive-model, non-aggressive model, and no model, which was considered the control condition. Throughout the experiment, they noticed that children learn aggression through watching aggressive behaviors of another person (observation
learning). The aggressive children were given aggressive toys and a Bobo doll and the children were rewarded for their aggressive behaviors. There was some aggression that was towards the Bobo doll within this setting; for instance, some of the aggressive children would punch the Bobo doll on the nose (McLoed, 2011).

Criminologist Ronald Akers and Robert Burgess also had a significant influence on the design of Social Learning Theory. Like Bandura, Akers and Burgess used Edwin Sutherland’s Differential Association Theory to assist developing their criminological theory to explain criminal behavior. Akers and Burgess’s Social Learning Theory is based on four different variables: imitation, definitions, different association, and differential reinforcement. Each of these variables explains their influence on an individual’s social observations and perceptions. Additionally, these variables provide the importance and impact by how reinforcing positive or negative behaviors have on an individual (Holt, 2013).

Tibbetts and Hemmens (2010) discuss the relation between learning theories and their relation to individual criminal behaviors. Researchers have found that during the individual’s socialization process, the individuals who might make the biggest impact on one’s behavior, criminal or non-criminal, are family members, friends, and teachers. Furthermore, researchers have found that learning theories are a major factor in understanding of criminal behavior.

Kirwan and Power (2013) states that Bandura’s Social Learning Theory explains that both non-criminal behaviors and criminal behaviors are learned from observing others. Individuals who exhibit criminal behaviors are more likely to have parents, siblings or peers who are offenders. In the cyber-world, cybercriminals will inherent the same learned observed behaviors as so real world criminals do. For example, a cybercriminal could learn how to engage
in criminal acts such as being a virus developer or continually downloading copyright materials (infringement).

**Application of Social Learning Theory to Hackers**

Studies have shown the strong bond between peer relationships that have deviant intentions and cybercrime. Additionally, this relationship bond is significantly prominent among deviant peers and hackers. Cybercrimes and individual imitation can vary depending on who the individual is imitating; for example, studies have shown that individuals who imitate family members are more likely to download files (i.e. music or movies) illegally, this is also known as piracy (Holt, 2013). Furthermore, Holt (2013) states that social leaning theory, “is one of the most commonly tested theories to account for various forms of crime, and holds particular value for cybercrime…[because] individuals must ‘learn not only how to operate a highly technical piece of equipment but also specific procedures, programming, and techniques’…” (p.125).

Hackers seem to imitate other hackers so that they are able to improve the skills and keeps up with the most recent hacking trends. Furthermore, in these hacker groups it is beneficial for the individual to be able to prove that they are able to stay current with the other skills of their deviant peer group(s). A hacker who is knowledgeable in committing fraudulent cybercrimes would have had to practice and research past crimes to gain the knowledge to know what was successful and what was not successful. Today, corporations are only able to protect themselves from hackers’ past behaviors. Unfortunately, because cyberspace is such an open domain these hackers have an upper hand and better chances of committing these crimes and not getting caught.
Self-Control Theory

Self-control theory, also known as the general theory of crime, originated by criminologists Travis Hirchi and Micheal Gottfredson and was fully established in the 1990s. This theory is used to label criminals who have low self-control and who participate in criminal and deviant behaviors. These criminals may participate in drug use, robberies, sexual assaults, burglaries, and/or cybercrime activities (Tibbetts & Hemmens, 2010). Individual self-control is a significant part of understanding criminal behaviors and in most cases criminals experience low self-control. Kirwan and Power (2013) identify that individuals who experience low self-control do not consider the repercussions of committing illegal activities. Thus, these individuals tend to be insensitive, impulsive, and more prone to seek out more risk taking behavior(s).

Moreover, Tibbetts and Hemmens (2010) identify Hirchi and Gottfredson’s six factors that an individual with low self-control would exhibit. These factors are often established by age 10, are: risk-taking propensities, impulsive behavior, temperamental, propensity for physical tasks (over intellectual activities), orientation toward simple tasks (as opposed to long-term commitments such as education), and self-centeredness. Individuals who have these qualities are more likely to engage in criminal activities.

Individuals who experience low self-control may also experience greater strain and societal rejection, thus leading into more deviant involvement. Other factors that may contribute to low self-control are personal/family traits (family members who have experienced the same behaviors), social circumstances (the social bonds the individual has established) and medical factors (mental or physical limitations) (Tibbetts & Hemmens, 2010).
Application of Self-Control to Hackers

Low self-control and social learning theory observe the individual’s social interactions with family and peers to identify if there is any relation in the individuals involvement in criminal behavior. Researchers have found a strong association between low self-control and digital piracy; individuals commit crimes like these because within their peer groups they do not see this crime as morally wrong because everyone else is downloading illegally without any repercussions.

Holt (2013) uses Gottfredson and Hirschi’s general theory of crime to explain that self-control is developed from childhood (starting as early as age 8) and can be altered through parental child-rearing techniques. Furthermore, since childhood deviance is developed at an early age, parents should introduce some form of restraint to discontinue this style of behavior. Parents should distinguish and reward positive behaviors and punish negative or destructive behaviors. Holt continues to explain that if this is continued throughout childhood into adulthood, this individual will be able to manifest one’s own self-control. Alternatively, if parents are not reinforcing the difference between appropriate and negative behaviors the child who develops a low self-control will have difficulty controlling their behaviors later in life.

Cybercriminals who have developed a low self-control have been linked to online pornography, different forms of piracy, and different hacking schemes. However, for more technical offenses such as the creation of malicious software or involvement in a complicated hack that requires a significant amount of persistence, criminological theorists’ have found that these cybercriminals may have higher levels of self control (Holt, 2013). Therefore, corporate fraud hackers may fall into the category of having higher levels of self-control because of how demanding and time-consuming cyber-fraud can be for a hacker.
Summary

Both, routine activity theory and social learning theory/self-control assist in understanding the thought process and behaviors of real world criminals and can be applied to the behavioral cues to catch cybercriminals. In order for criminologist to obstruct cyber-fraud behaviors an understanding of a hackers’ methodology, routines, and behavioral indictors must be identified. Theories like RAT and learning theories play a significant part in catching criminals by providing a basic outline for certain clues and styles a cybercriminal may use to follow through with their crimes. More specifically, the cybercriminals who are interested in attacking big corporations for that big payout will demonstrate the same thought process as someone who robs a bank in person; however, cybercriminals have one advantage and that is they are able to hide their identity and location through encryptions. In order to effectively understand cybercriminals, criminologist must realize that cybercriminals are often opposite from those real world criminals by which they are more likely more sophisticated and have higher self-control.
Section IV. Recommendations for Prevention Strategies

Access points within a corporation can determine whether or not a hacker can infiltrate the software; therefore, it is important to prevent any chance of a hacker attack. This section provides current prevention trends, new technologies, prevention recommendations, corporate prevention of customer data, and a suggested outlook of future cybercrimes.

Prevention Trends & New Technologies

Corporations/businesses need personnel to protect and provide risk awareness to customers as well as company personnel. To protect one’s business from hackers, the Identity Theft Protection Association (ITPA) (2014) suggests various ways to protect one’s business bank accounts from fraud. ITPA (2014) suggests: 1) review all bank agreements; 2) enact security and authentication controls to protect against fraudulent wire transfers and electronic transactions; 3) monitor and reconcile business accounts daily; 4) think “security” when accessing personal accounts online; 5) be wary of phishing scams; 6) when paying with company checks, enroll in Positive Pay (provide the bank with a list of check numbers and amounts); and 7) keep business checking account supplies secure.

Additionally, ITPA (2014) provides suggestions to protect business computers and networks, such as: 1) restrict the use of business computers to only business activities; 2) install and use regularly updated anti-virus/anti-spyware/Internet security software; 3) keep security patches and updates up-to-date; 4) install and utilize a firewall on business computers or networks; 5) secure the business’ wireless network; and 6) remain vigilant and be alert for suspicious or unusual activity.
User Passwords

Carey (2014) states that user passwords are still the most common form of security that stands between hackers and vital business information. As mentioned previously, if the hackers are able to penetrate the system they are able to access passwords and obtain important business information such as client and financial information. Carey (2014) identifies that hackers are able to gain access to company information by identifying a remote entry point that has an easy identifiable default password.

Another way for hackers try to guess company passwords are by viewing random employee media pages; it is very common that people use passwords that are very personal to the individual. Carey (2014) cautions that using one’s children’s or pet names are easy passwords to guess, as well as using one’s favorite sports team. Carey also advises that providing answers as one’s mother’s maiden name or the city one is born in are offering hackers the answers to the most common security questions. Plummer (2015) reports that the top five password used in 2014 were: 1) 12345, 2) password, 3) 12345678, 4) qwerty, and 5) acb123. Furthermore, Plummer (2015) states that about 91 percent of password users have used at least one of these five passwords personally and professionally.

To prevent hackers from guessing these passwords, Carey (2014) suggests creating strong passwords that entail using at least eight characters using both lower case letters and upper case letters. Using this method gives crackers a more difficult time because complex passwords are much harder to crack. Furthermore, Carey (2014) delivers a couple techniques that employees can use to create harder passwords. Employees can use numbers and symbols that look like letters. A pattern one could use is “football: by changing it to “F00tba!” (p.46). This password is easy to remember and is considered a strong password. Another suggestion is to use the first
letter of each word of a phrase as a password. An expression one could use is “it’s always darkest before the dawn” and could be broken down into “I@dbtd” (p.46). Furthermore, a couple of numbers should be added at the end of the password to make this a strong password.

Most companies, especially corporate level, use password management software that automatically creates secure passwords for each of their sites/applications that employees use. Changing these passwords regularly reduces the companies’ vulnerability to becoming hacking. Therefore, by taking these simple steps, companies can protect their personal information and protect their employees (Carey, 2014).

**Biometrics**

Yar (2013) discusses measures such as the use of biometrics (i.e. fingerprints, iris scans, and/or voice recognition) and digital signatures as the future of authentication technology. Furthermore, Sood (2015) agrees that biometric security has benefits in protecting from online fraud. Also, Sood argues that biometrics are better than using passwords. For example, other than using letter passwords, new technologies have been developed like the Nymi Wristband that uses the heart rhythm of the individual as the password. Unfortunately, keeping up with new technologies to insure against fraudulent activity costs a lot more money than companies may want to spend. Also, some may argue than using biometric security may look more secure in appearance; however, it gives users a false sense of security (Sood, 2015).

Plummer (2015) expresses concerns of certain biometric designs that have been promoted in the cybersecurity world have included brain implants, ingestible security tokens, and vein recognition systems/body scanners. Plummer (2015) quotes IT Harvest chief research Richard Stiennon by stating, “there is a time and place for biometrics in cybersecurity, but the technologies currently are too segmented.” In other words, this technology is not ready to be
implemented and usernames and passwords are not yet going to be replaced with new technological mechanisms.

**Cloud Data Security**

Professionally and personally individuals are using digital storage to store information. One of the most common forms of digital storage is called the cloud and this is where individuals can store and exchange information. Today, most people no longer rely solely on other forms of digital sharing such as emails or faxing. Additionally, the usage of USB flash drives is becoming a less common way to share digital documents. When data is placed in the Cloud it is very likely that the information is permanently kept there. Moreover, some people will place personal documents such as bank documents, confidential business work papers, and identification scans in the Cloud (Ivey, 2013).

The Cloud is a global used tool and the use of using digital storage can place business and personal information at risk. By putting personal and confidential information in the Cloud one can never be too sure if their information will be protected from hackers. Ivey (2013) provides suggestions to protect their privacy when using the Cloud: one should avoid storing sensitive information; one should read the user agreement to find out how your cloud service works; one should be serious about their passwords; one should consider encryption software; and/or find a Cloud Service that provides encryption and decryption.

When corporations invest in Cloud Security, there is always the chance of Cloud-based malware. Gonsalves (2014) reports of malware attacking corporate computers using Cloud service providers. Monitoring the network and watching for any suspicious activities can detect this malware because it may prevent the software to act differently. Some indicators that corporations should monitor are their unused TCP/IP ports (data sharing ports); corporate
employee computers reaching out repeatedly to other computer networks; watching the system’s activity while knowing that corporate system is active from 8 a.m. to 4 p.m.; and on average a corporate system sends out on average of 500MB on a normal work day, anything above that (GB) should raise caution (Gonsalves, 2014).

Corporate Prevention of Customers Personal Information

The Federal Trade Commission (2011) provides organizations with practical tips to protect personal consumer information. Many companies have consumer and employee data, which have names, social security numbers, and account data that could have credit card/financial numbers. If the information that is entrusted to these corporations is breached and stolen, also known as identity theft, the trust of their client’s/customer’s may be lost and the company maybe subject to a lawsuit. By providing one’s client’s/customer’s with assurance that their identity and financial information is safeguarded is necessary for a good business plan (Federal Trade Commission, 2011).

The Federal Trade Commission (2011) provide five key principles of a data security plan to protect personal information of employees and clients/customers (p.3): 1) Take stock—know what personal information is stored in company computer files; 2) Scale down—keep only what is needed for the company; 3) Lock it—protect the information that is provided to the company; 4) Pitch it—properly dispose of information that is no longer needed; and 5) Plan ahead—create a plan to respond to security breaches. Additionally, corporations should train their employees at all levels about what to look for in security vulnerabilities and provide the proper steps of reporting the security breach. Moreover, one suggestion companies should also implement is that every employee who needs access to personal information must be required to get approval by their direct supervisor.
As stated previously, in December 2013, Target experienced unauthorized access to customers’ credit card information between November 27 and December 15. The CEO of Target, Gregg Steinhafel, provided their customers with a letter indicating that they were aware of the attack and assured their customers that the company is taking this issue very seriously. Also, he indicated that their customer’s are not liable for charges they did not make and that Target is working on fixing the problem. Target provided the affected customers with free credit monitoring services and provided a store-wide additional 10% off discount. Target also issued new credit cards to those customers who did not cancel their patronage with the company (Fox, Pagliery, O’Toole, Pepitone & Perez, 2013).

The identity breaches on Target and other corporations like Home Depot have inspired a new credit card prevention tool. These credit cards led by Visa and Mastercard have computer-chip security that has a more reliable form of encryption than the magnetic strips. Eliminating the magnetic strip has reduced several vulnerable points, such as cybercriminals who use electronic skimmer machines at ATM machines to collect personal data. One concern customers may have is the time to authorize the credit cards; the cardholder must place the credit card in the credit card machine with the chip up and wait for the card to be authorized. Using the computer-chip security credit cards will not be as quick as swiping the magnetic strip through the credit card reader.

The Future of Cybercrimes

Not only do corporations need to be prepared for a cyber attack, individuals need to also be aware of the risks of cyberspace. Glassberg (2014) identifies 8 cybercrimes that are estimated to hit in the next 20 years: cyber-jacking—hijacking planes through hacking methods (the hijacker would not be there physically) but would take control of the plane’s computer system;
human malware—if one relies on Wi-Fi-enabled medical implants (i.e. pacemakers), hackers could be able to hack into that device and threaten the well-being of the individual; cyber assault—hackers hacking into one’s home invading electronic devices (i.e. a thermostat) and changing them or using them for personal use (cyberstalking at a new level); cyber extortion—hackers use “ransomware” to hack into personal financial accounts and demand a ransom to release an account back to them; car sploiting—viruses are likely to jeopardize cars operating systems (i.e. phone connection services- Androids) which are vulnerable to hacking attacks; brick attacks—fraud attacks where bank and credit card accounts are stolen and information is destroyed permanently; identity theft squared—biometric security is currently a new concept but when it is used for authenticating all online accounts, this biometric data will be the key information for hackers to steal one’s identity; and mini-power outages—many household are transitioning to “smart meters” which are also vulnerable to cybercriminal tampering. A hacker could tamper with these meters by turning off power to a household at will.

Summary

Corporations need to keep up with prevention trends in order to keep their companies safe from hackers. Furthermore, corporations need to keep employee and client/customer information safe from being accessed. Therefore, in order to keep this personal information safe from hackers, generating strong passwords will assist in keeping hackers away from this information. Also, keeping current with new trends like biometric security works will also be beneficial for organizations to maintain security.

Corporations that use the cloud for digital storage must research what kinds of security services will protect their confidential information. The breach on Target has demonstrated the importance of strong security measures and how important it is to keep customer information
protected from cybercriminals. Today, credit cards (Visa and Mastercard) are using a new type of security measure by installing a computer-chip in the credit card. The customer must verify their credentials in order to use the credit card. Some customers who have already used the computer-chip credit card state that the verification process takes more time than justswiping the magnetic strip but it is worth the security.

Corporations are advised to keep up with current cyber-attack trends and use the appropriate protection to provide that security umbrella for everyone associated with the company. Employees must also keep up with a company’s guidelines for security. By knowing that the Internet makes data hacking possible, employees should be educated and well prepared for any style of cyber-attack by using strong passwords to protect company information. Also, corporate employees’ should become familiar with criminal theories such as Routine Activity Theory and Social Learning/Self Control Theory to understand basic criminal behavioral cues. It is vital to be one step ahead of a hacker; if the hacker is one step ahead of their victims, it is nearly impossible to catch up.
Section V. Recommendations and Conclusions

Recommendations for Further Research

In order to begin understanding hacker behaviors one must study past attacks and analyze their methods as to the network was penetrated. One recommendation that criminologists could consider is working directly with convicted hackers and studies the methodology of their attacks. It is assumed that this approach has been attempted, but has not been successful because law officials do not want to make a deal with hackers to reduce their sentences. In the event where hackers are released, they will be likely to return to the same criminal behaviors. Nonetheless, if they were willing to cooperate, they may help law officials with solving and understanding other hacking cases that involve the same style of breaching behaviors.

Hackers value their friendships with other hackers, especially the individual who they consider their mentor. The hackers who work in groups may not want to help law enforcement because of their loyalty to their groups. The hackers who work alone might be more prone in helping criminologists; however, hackers who work alone usually will have other hacker friends and they may not want to jeopardize their friendships.

Globally, allowing the Internet to provide endless possibilities for everyone with an Internet connection could be considered a blessing or a curse. Some may argue that the Internet has taken away an individuals’ right to privacy. In today’s world almost everything is digitally and electronically recorded and stored. It is very rare to see businesses use paper documents anymore; for example, when applying at Walmart the applicant must go to the application center where there are computers to allow the applicant to electronically input their information. Corporations who use electronic storage need to assure that employee and client/customer information will be secure and safe. Furthermore, organizations need to protect themselves from
any style of hacking; therefore, organizations need to research the best and the most compatible safeguard that works with their business. It is very important that corporations provide a trusting and safe appearance.

**Conclusions**

Corporations at anytime can become vulnerable to a cyber-attack, whether it is because of an employee opening up a port by sharing information through e-mails or the organization is not equipped with the proper security software to keep out hackers. Hackers have proven to be loyal to their groups and are always learning ways to penetrate networks. It is important for criminologists to understand the behaviors cues and techniques of a hacker because they are all very different; for example, a black hat hacker will have different responsibilities and different anticipated outcomes than a grey hat hacker would. So by understanding each type of hacker, criminologists might have a better chance of profiling who they are looking for when investigating a hack.

The Internet is an ever-growing resource and may be the answer in providing the prevention needed to protect against hackers. If law enforcement around the world worked together to stop cybercrimes, more specifically, cyber fraud, there might be a chance that this type of criminal offense may decrease; furthermore, this global collaboration may also decrease identity theft as well. Unfortunately, a hope of a global understanding is highly unlikely which may allow hackers to commit these crimes without repercussions right away. The global comparison in the paper reported that certain areas of the world have different variations of crimes that are more prominent in certain countries than others.

It is also important for corporations to understand the regulations that protect them from cybercrimes. As indicated in this paper Global Internet Freedom Task Force (GIFT), The
Computer Fraud and Abuse Act, Computer Fraud: 18 U.S.C. §1030(a)(4), the Sarbanes-Oxley Act 2002, and the Cyber Action Team are just a few that are protecting corporations from being hacked; these laws hold criminals responsible for their actions. Furthermore, these laws also ensure that corporations and small businesses have a chance to succeed without worrying who will hold cybercriminals responsible.

The application of theories to hackers assist in understanding why cybercriminals behave and act the way they do. Using Routine Activity Theory, Social Learning Theory, and Self-Control Theory demonstrate what these hackers look for in a victim and how childhood development can influence a criminal to grow up and behave defiantly/criminally. Additionally, how hackers feel about themselves can play a big part in how they control their criminal behaviors. One limitation that law officials are facing today is that they are trying to analyze cybercriminals through data breaches rather than bring in the individual and interrogate them. Face to face interrogation can really assist law enforcement in identifying the root reasoning in why these criminals feel it is okay to commit criminal or deviant behaviors.

Prevention software for a corporation is vital to keep the company information secure. Corporations should mandate that their employees change passwords weekly and used strong password techniques to help prevent from being attacked by hackers. Furthermore, understanding the risks of using biometrics and digital storage, such as the Cloud, and how important it is to have protection software on that information is critical of a company’s security plan. When there is a cyber-attack on a company and client/customer information is stolen, the company’s reputation is discredited. Using Target’s cyber-attack as an example provided a structure for what the company did to regain customer trust.

As important as it is for corporations and even small business’s to protect their
customer’s information, it should also be as important to employees. Protecting oneself from identity theft is very important because as soon as a hacker has that information, it is very difficult to resolve. Preparing for the worst-case scenario can deter a hacker from stealing one’s personal access credentials. Unfortunately, some individuals are not aware of the risks and the dangers of cybercriminals and the damage a hacker can do to the information they can retrieve.

To provide awareness to employees, companies could organize an awareness campaign of the potential dangers of cybercriminals and what harm the cause. This awareness campaign may reduce identity theft and online fraud (Kirwan and Power, 2013). Overall, globally we are not prepared for how cybercriminals manipulate networks using the Internet and in the years to come it seems like the Internet’s potential is only going to grow and give hackers the upper hand if organizations and employees do not protect themselves.
Section VI. Reference List


http://www.computerworld.com/article/2858143/sony-makes-cybercrime-even-more-dangerous.html


