THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

CYBER CRIME: ANALYSIS OF OFFENDING PATTERNS AND OFFENDER CHARACTERISTICS WITH SPECIAL EMPHASIS ON WOMEN

COREY J. LEE
Spring 2012

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Security and Risk Analysis
with honors in Security and Risk Analysis

Reviewed and approved* by the following:

Darrell Steffensmeier
Professor of Sociology and Crime, Law, and Justice
Department of Sociology
Thesis Supervisor

William McGill
Assistant Professor of Information Sciences and Technology
College of Information Sciences and Technology
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

This document analyzes the offender characteristics and offending patterns of modern day cybercriminals. A Cyber Crime Database (CCD) including 53 cases and 101 defendants involved in cyber crimes prosecuted by the Department of Justice was created for this report by analyzing press releases and indictments published for public record in 2010. The findings observed from the analysis of this dataset were compared against the findings of several comprehensive, industry-approved cyber crime reports to accurately identify consistent offender and offending patterns related to cyber crimes. By identifying these patterns, current cyber crime risk management and risk analysis efforts will be enhanced. Additionally, this study investigated the extent to which women were involved in cyber crimes to provide insight regarding their involvement and enhance modern day cybercriminal profiling. The key findings of this thesis are: (1) Men are more likely to be cybercriminals; (2) Men are more likely to be ringleaders of cyber crime networks; and (3) The nature and extent of female involvement in cyber crime appears to be shaped by their gendered focal concerns and risk-taking styles.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGMENTS

I wish to express my sincere appreciation to Dr. Darrell Steffensmeier whose familiarity with gender bias regarding different types of crimes was helpful during all phases of this undertaking. In addition, special thanks are due to Professor John Bagby, Professor Lynette Kvasny, and Professor Edward Glantz for their assistance in the preparation of this manuscript. I also thank the members of the College of IST and the Schreyer Honors College for their valuable input. This thesis represents a culmination of my research experiences in the Penn State Department of Sociology, and academic pursuits as a student in Penn State's College of Information Sciences and Technology. As such, I would like to thank the following people, without whom this work could not exist:

- Dr. Darrell Steffensmeier for providing me with numerous research opportunities throughout my collegiate career, serving as my thesis adviser
- Dr. William McGill for serving as my honors adviser and for advice related to my career preparation
- The College of Information Sciences and Technology, Bunton-Waller Fellowship Program, and the Schreyer Honors College for financially supporting my academic career
- The Penn State Writing Center, Denise Conner, Keva Tranzor, Candace Carson, and Leteace Howard for editing and proofreading this manuscript
- The Dell Scholars Program for its academic and financial support during my academic career
- Roberta Hardin, Mitch Kirsch, and Friends and Family for supporting me throughout this academic endeavor

GLOSSARY

Cyber Crime. - A crime that involves the facilitation of an illegal activity through the use of a computer as a tool, or where a computer or network is a target

18 U.S.C. 1030 Statute – Refers to the Computer Fraud and Abuse Act, which is intended to address federal computer-related offenses and reduce cybercrime enacted in [1986]

Exploit – Term used to describe taking advantage of a vulnerability in computer system

Vulnerability - A flaw or hole in a security system that can lead to compromise

Insider Threat – The threat of a nefarious or malicious action being performed by a trusted source

Botnet – Group of compromised computer systems that are controlled remotely by a command center and used to conduct denial of service attacks

Gray Hat Hacker – hacker who publicly exploits a security weakness in a computer system or network in order to bring the weakness to the attention of the owners

White Hat Hacker – hackers that attack computer systems or networks to identify security vulnerabilities and report them to the entities responsible for them

Black Hat Hacker – hacker that attacks computer systems or networks with a malicious intent

Script Kiddie – low level unsophisticated hackers that download malicious software from hacker websites and follow the posted instructions to execute an attack on some target

INTRODUCTION

Cyber crimes are arguably the most costly and prevalent crimes to address in the 21st century. With the anonymous nature of the internet, widespread use of technology, and the constant desire for financial gain, cyber-crimes are becoming the primary concern for many businesses and law enforcement entities. With the increased publicity of cyber crimes, many victims and law enforcement officials find themselves asking several main questions: Who are cybercriminals? What are their offending patterns? Is the current perception of women's roles in cyber crime accurate? Therefore, the research in this thesis aim's to address these two questions by fulfilling two objectives which are: To create a searchable database of cyber-criminal activity for further study , and then test this database by studying female actors.

Currently, there is no central data source for cyber crimes and their offenders in existence, and collecting this data is quite difficult. In an effort to understand the nature of cyber-crimes and their offenders, a detailed database was developed covering all cyber crimes prosecuted by the Department of Justice in 2010 involving 101 cybercriminals. To create this Cyber Crime Database (CCD), information on cyber crimes and their offenders, including crime, gender, role, motivation, damage, was extracted from the Department of Justice cyber-crime press release archive (DOJ). This study intersects a number of different areas of interest related to sociology, but contributes in particular to the broad and rising interest in cybercriminal profiling and cyber crime risk analysis. This unique database addresses the question: What are the modern day offender characteristics and offending patterns of cyber-crimes?

The CCD was also used to investigate the question: What is the nature and extent to which women are involved in cyber-crimes? By conducting this investigation, I aim to describe the capabilities of female cybercriminals and demonstrate whether they are more or less of a threat than what they are perceived to be. With this investigation, it will also be possible to further develop Steffensmeier and Allan's gendered paradigm of criminality by drawing on the literature in criminology and gender to highlight the links between cyber crime and white-collar crime sex-typing which can potentially marginalize and minimalize the actual and perceived involvement of women in cyber crimes.

After introducing the concepts of women and technology, the gendered paradigm theory, and societal perceptions regarding women and their abilities, motivations, and opportunities to commit crimes, I address: Do the societal perceptions regarding women and their ability to use technology limit their opportunities to commit cyber crimes? Following this discussion will be an analysis of cyber crimes that have been prosecuted by the U.S Department of Justice to understand the extent to which women are involved in cyber crimes and the impact of cyber crimes carried out by women. Do women commit certain types of cyber crimes more than others? Do women typically use the same methods of attack as men when engaging in cyber crimes? By exploring these questions, I aim to improve the understanding of women as cybercriminals and compare these results to current theories.

In summary, this thesis focuses on two central questions which are: 1. What are the modern day offender characteristics and offending patterns of cyber-crimes? 2. What is the nature and extent to which women are involved in cyber-crimes? By investigating and addressing these two questions, current cyber crime risk management and risk analysis efforts can be enhanced.

Chapter 1

HISTORY OF CYBER CRIMES

Cyber crime has existed since the creation of the first computer system in the 1950s, but it did not become significant until the advent of the computer network in the 1960s. As more and more information began to be shared from system to system over networks, those systems became vulnerable to attack (Alaganandam et al. 4). Moreover, the more affordable computers and computing became, the more significant cyber crime became.

Although cyber crime existed in the early stages of computing, "Cyber crime evolved from hacking of another system, the public switched telephone network. "Phreakers", phone network hackers, are considered to be the first cybercriminals. These individuals would discover ways to circumvent the switching networks of telephone systems and make long-distance calls for free. The most notable "phreaker" was John Draper also known as "Cap'n Crunch" (Alaganandam et al. 4). This nickname was given to him because he discovered that by blowing into a pay phone using the toy whistle from a Cap'n Crunch cereal box, he could access the administration mode of the phone switching network, and make phone calls with unlimited free long distance. (Alaganandam et al. 4).

The growth of the internet and the advent of the personal computer in the 1970s, opened the door of opportunity for modern day cybercriminals. Shortly after the personal computer became publicly available, general computer users began to enhance their computer skills, and hackers began to explore their curiosities. Additionally, internet service providers began to attract more attention from the general public, and as computers became more affordable the internet also became more accessible (Alaganandam et al. 4).

Today, computers and the internet are involved in most every aspect of a person's life. From posting statuses on Facebook to sending emails through a mobile phone, people are more connected to the internet today than they have ever been. Unfortunately, with more people, services, and financial transactions moving to the web the more appealing cyber crimes become to current and potential criminals (Alaganandam et al. 4). In part because we as a society have reached a point in time where staying connected is vastly important, the probability of occurrence and impact levels of cyber crimes will continue to increase in significance.

Chapter 2

OVERVIEW OF CYBER CRIMES

Cyber Crimes Defined

According to the FBI, cyber crime is currently a top priority for the nation's primary federal investigative agency (FBI). A cyber crime, also referred to as an internet crime or computer crime, is defined as any crime that is committed using a computer or network, or hardware device (Norton). Additionally, the computer or device may be the agent, the facilitator, or the target of the crime (Norton). These crimes are not just new crimes that simply enable new criminals to exploit new vulnerabilities, but they also enable traditional criminals to commit traditional crimes more often and in new ways.

Present-day cyber crimes are crimes that seem to be feared by many nations and individuals due to their prevalence and potential impact, but the true essence of these crimes has yet to be fully understood on a large scale (PwC 1). Historically, the analysis of the crime offending patterns and offender characteristics in the form of profiling, has had a success rate of 77% in traditional investigations, and there is no empirical evidence to show that it cannot be equally effective for cyber crimes (Rogers 294). Due to the broad scale emergence of cyber crimes and the evident need for increased fundamental understanding, efforts to understand the nature of these crimes as well as their perpetrators can be of great benefit to cyber crime-related law enforcement agencies, computer forensic specialists, and risk managers (Rogers 295).

Types of Cyber Crimes

Cyber crime is a broad and encompassing category. In many cases, cyber crimes are essentially traditional crimes that involve the use of computers and the internet to commit the crime. Although the names of some cyber crimes can be somewhat confusing due to their technical nature, the majority of these crimes can be described by showing their similarity to more well-known traditional crimes. Each cyber crime listed below is accompanied by a description including a definition of the crime and its fundamental characteristics.

- *Cyber Extortion* – using a computer to unlawfully obtain money, property or services through coercion (Alaganandam et al. 6)
- *Cyber Fraud* – the use of a computer to defraud a business or individual (Alaganandam et al. 6)
- *Cyber Stalking* – express or implied threats to create fear through the use of computer technology such as email, phones, text messages, webcams, websites or videos (Alaganandam et al. 6)
- *Cyber Theft* – using a computer to steal physical or virtual goods and information. This includes activities related to breaking and entering, DNS cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, malicious hacking, plagiarism, and theft of trade secrets (Alaganandam et al. 6)
- *Cyber Threat* – threatening a person with fear for their safety or life, or the lives of their families or persons whose safety they are responsible for, through the use of a computer network such as email, videos, or phones (Alaganandam et al. 6)
- *Denial of Service* – using a computer to disrupt the availability of an application, system or service offered by a company or website (Alaganandam et al. 6)
- *Insider Threat* – using privileged or trusted computer access to conduct nefarious acts that adversely affect a business or entity (Alaganandam et al. 6)

Impact of Cyber Crimes

The increasing prevalence and impact of cyber-crimes over the last decade has caused many people to realize the true magnitude of threats posed by cybercriminals (Deloitte 2011 4). Threats posed to organizations by cyber crimes have increased at a faster pace than potential victims or cyber-security professionals can mitigate them according to the 2011 Cyber Security Watch Survey, sponsored by Deloitte and conducted in collaboration with CSO Magazine, the U.S Secret Service, and the CERT Coordination Center at Carnegie Mellon (Deloitte 2010 3). Additionally, this well-known survey reports that the average monetary loss due to cyber crime attacks in 2011 is approximately $123,000 which happens to be down from $392,000 in 2010 (Deloitte 2011 3). Although the previous statistic suggests that many companies and individuals are doing a better job of protecting themselves from becoming victims of cyber crimes and are taking more precaution to mitigate the overall impact of these crimes, the threat still deserves a great deal of attention. As technology continues to evolve and the use of the internet and computers continues to grow, the opportunity to commit computer crimes for large financial gains will continue to exist. Therefore it is reasonable to believe that computer crimes will continue to be a problem for many years to come.

Although many companies and individuals have adapted to the current age of technology-based crimes by using better security practices, the changing drivers of security continue to allow for new vulnerabilities to be created faster than they can be identified and controlled (Symantec 10). The number of cyber crimes investigated in 2010 increased dramatically while data loss was at an all-time low, according to the Verizon 2011 Data Breach Investigation Report (2).

Nonetheless, all aspects of cyber crimes deserve much needed attention to prevent the commission of these crimes from becoming uncontrollable.

Cyber Crime Studies and Prior Research

In this section I will highlight and discuss several prominent cyber crime reports that provide annual updates on the trends and patterns associated with cyber crimes. It is important to use the information collected by several sources when analyzing cyber crimes due to the global and economic nature of the crimes. Although global and domestic collaboration regarding the analysis of cyber crime is in its early stages, I believe that as time progresses cyber crime will be understood and its patterns and trends will become more noticeable.

The 2011 State of Security Survey is a survey created by Symantec Corporation, the largest maker of security software for computers. The purpose of this survey is to update the global perspective of key security threats, trends, and responses worldwide. In April and May of 2011, Symantec commissioned Applied Research to conduct the 2011 State of Security Survey (Symantec 6). To collect the sample used for this survey, researchers contacted about 3,300 businesses that included varying sizes of companies ranging from 5 to more than 5,000 employees (Symantec 6).

One major finding in this survey was that the top 3 sources of security threats stemmed from Hackers (49%), Insiders (46%), and Targeted Attacks (45%) (Symantec 10). Another major finding in this survey was that the top 3 losses due to cyber-attacks were downtime, theft of employee's identity information and theft of intellectual property (Symantec 12). Lastly, the most important finding in this survey was that malicious code ranked highest among methods used by cybercriminals in a cyber-attack at 30%, then social engineering 26% (Symantec 14).

The 2011 Verizon Data Breach Investigations Report is a report created by Verizon and conducted in collaboration with the U.S Secret Service and the Dutch National High Tech Crime Unit. This report describes cyber crime offender characteristics and offense patterns from a service provider viewpoint. To collect the sample of data breach incidents used for this report Verizon investigators used an internal framework by the name of VERIS to record, validate, analyze case data using a common language for describing security incidents (Verizon 7). All Verizon case results are based on firsthand evidence collected during paid external forensic investigations conducted by Verizon from 2004 to 2010 (Verizon 7). In total about 800 new data compromise incidents and 3.8 million records confirmed stolen were collected to compile the 2011 DBIR, but only about 630 were used for analysis (Verizon 8).

One of the most notable findings in this report was a rise in breaches in the hospitality and retail sectors which currently represent smaller, softer, and less reactive targets than financial institutions (Verizon 12).Targets are considered softer and less reactive when they are perceived to not view security as a priority, and appear to lack advanced security controls and forensic technologies. Findings in this report also showed that in 2010, each of the top 4 hacking methods exceeded 40% suggesting many attacks leverage a similar combination of hacking methods (Verizon 32). In addition, this report found that attackers prefer to use the same attack vectors when using hacking as the method of attack (Verizon 34). Organized criminal groups, at 58%, were the most common external threat agents, while only 8 percent of cyber breaches had a high level of difficulty, and 83 percent of attack targeting is opportunistic (Verizon 52).

Cybercriminals

“Cybercriminals are becoming a threat that rivals terrorist groups like al Qaeda, according to FBI Director Robert Mueller the nation’s top law enforcement official” (Cowley). Unlike traditional criminals, cybercriminals have the luxury of using the internet and computers to conduct crimes with a certain level of anonymity. Since the creation of the first virus, cybercriminals have steadily evolved with the advancement of technology.

“In the early 1960s, the first cybercriminals were identified as MIT students whose motivation was often to satisfy curiosity rather than to cause harm” (Rustad 70). On the contrary, hackers today are driven mostly by financial motives (Alaganandam et al. 5) and “[t]he perpetrators of computer intrusions may be bored juveniles, disgruntled employees, corporate spies, or organized crime networks” (Moore 51).

Cybercriminals come from all backgrounds and walks of life but many of them tend to share several general characteristics that can help profilers identify potential cybercriminals. Although the following characteristics are general in nature, it is believed that those characteristics can be used to narrow down the pool of potential perpetrators and ultimately lead to the discovery of a criminals’ identity in many cases.

Determining the motive of a cybercriminal is one of the best ways of identifying the type of cybercriminal responsible for a cyber crime. Due to varying motives for cybercriminals, several different categories have been created to characterize different types of cybercriminals. The most common type of cybercriminal is typically referred to as a hacker. Hackers are essentially individuals who try to break into computer systems (Sjoholm). “The original hacker stereotype is a smart, lonely deviant - a teenage or adult male who's long on computer smarts but short on social skills. But like most stereotypes, it doesn't begin to tell the whole story" (Bednarz 1).

Underneath the umbrella term hacker, there are also several types of hackers such as: gray hat hackers, white hat hackers, black hat hackers, and script kiddies (for definitions, see Glossary in Appendix and see Batke). Another type of cybercriminal is a "Hactivist" which is none other than a hacker that hacks for political, social reasons (Batke). Other types of cybercriminals consist of cyber terrorists who are basically state sponsored hackers, and organized crime groups (Batke). Lastly, we have insiders which are considered by some to cause the most financial damage and described as legitimate or trusted sources that misuse their privileges to compromise data, systems, and networks (Verizon 19).

Profiling of cybercriminals is considered a promising but immature science (Bednarz). Even though many attempts have been made to profile cybercriminals, few have been considered to be successful. Nonetheless, research on profiling cybercriminals has continued to increase and several studies are beginning to receive attention in the field of cyber security. A current study on cybercriminals conducted by Deb Shinder, author of the book *Scene of the Cyber crime*, claims that most cybercriminals share most of the following characteristics (Shinder):

- Some measure of technical knowledge
- Disregard for the law or rationalizations about why particular laws are invalid
- High tolerance for risk or need for "thrill factor"
- "Control freak" nature, enjoyment in manipulating or outsmarting others
- A motive – monetary gain, revenge, political/religious beliefs, sexual impulses, or fun

Additionally, Shinder believes that traditional criminals have cyber-counterparts (Shinder), suggesting that the characteristics used to profile traditional criminals can also be used to profile cybercriminals. Prior literature suggests that there are several offender characteristics that can be used to accurately profile a traditional criminal.

For this study, a select number of offender and offense characteristics were used to create criminal profiles for men and women as they pertain to cyber crimes: 1. type of cyber crime committed, 2. victim targeted, and 3. method of perpetration, 4. motive, 5. complexity of scheme, and 6. offender age and gender. Taken together, these characteristics will be used to identify cyber crime offender characteristics and patterns, to distinguish male and female cybercriminals, and to compare women's and men's patterns of offense. These data will be used to determine whether female involvement in cyber crimes is similar to female involvement in white collar crimes seemingly due to socialization and gendered focal concerns (Steffensmeier, Schwartz, and Roche 4).

The compelling question that this study aims to address is whether modern day cybercriminals are gender- specific or gender neutral. Due to the current widespread use of computers and the internet, virtually all computer users with access to the internet have the opportunity to commit a cyber crime. Moreover, because of the consistent involvement of women in technology, and the increasing simplicity of many cyber-attacks, women are believed to have the necessary skills for a significant level of involvement in cyber crimes. This research shows that gendered processes influence the involvement of females in cyber crime in ways similar to white collar crimes.

Chapter 3

WOMEN AS CYBERCRIMINALS

According to the National Center for Women and Information Technology (NCWIT), women hold 56% of all professional jobs in the U.S. workforce, but only 25% of IT jobs. Additionally, the NCWIT reports that only 11% of executives at fortune 500 tech companies are women (NCWIT). Although women are not proportionately represented in tech-related fields according to statistics, many are well-equipped with the skills and aptitude to succeed in the profession. More importantly, the fact that women are poorly represented in tech-related fields does not mean that they cannot or will not commit cyber crimes

Today, and throughout history, many women have had the skills and opportunities to commit technology-related crimes; however, they also seemed to lack the motivation or interest to pursue these opportunities. There are many potential explanations for this phenomenon such as a lack of interest, societal perceptions, and the portrayal of tech criminals in mainstream media. However, the shortage of women involved in tech related fields and the perceived lack of female involvement in cyber crimes can also be explained by the gendered paradigm theory, which is described in the next section.

The Female Cybercriminal and The Gendered Paradigm Theory

Some research shows that in the fields of information technology and IT security, cyber crimes are mainly perpetrated by males. However, the research is scarce and very little in particular is known about female involvement and the gender gap. In the section that follows, I draw on two main sources for my framing of the likelihood of female involvement in cybercrime. The first source is “Gender and Crime: Toward a Gendered Theory of Female

Offending" by Darrell Steffensmeier and Emilie Allan. The second source is "Gender and 21st Century Corporate Crime: Female Involvement and Gender Gap in Enron-Era Conspiracies" by Steffensmeier, Schwartz, and Roche.

Although underrepresented in technological fields, women were instrumental in the development of the computer and advancing its technology. For example, the first computer was conceptualized by a woman, the first computer compiler was created by a woman, and the first electronic digital computer was created by 75 female mathematicians (Frieze). Today, many women have the hacking skills to engage in cyber crimes and further advances in technology make it easier to gain and use those skills. Because cyber crimes today are considered to be mainly financially driven, it is reasonable to assume that women also may have a financial motivation to commit cybercrimes. Lastly, because the only materials needed to commit a cyber crime are a computer and the internet, it is reasonable to assume that women have the opportunity to commit cyber crimes.

While women seem to have the skills and opportunities to commit cyber crimes, they are limited by access to organized cybercriminal networks and by increased risk aversion when compared to men. Because of this, the gender gap between female and male cybercriminals may be similar to the one observed between male and female corporate criminals. Additionally, women are more likely to shy away from cyber crimes that may involve serious harm (Steffensmeier, Schwartz, and Roche 5). Female cybercriminals may also be limited in their opportunities because of sex segregation, which excludes them from the opportunity to be involved in many organized cybercriminal networks. In conclusion, the overall potential of women as prospective cybercriminals is expected to be limited due to their gendered focal concerns, risk preferences, and fewer opportunities for cyber crimes involving collusion with other offenders.

Women & Cyber Crime

“Gender is the single best predictor of crime: In all known societies and throughout all historical eras, men commit more crime than women” (Steffensmeier and Allan 1995 86).

Historically, factors such as access to education and employment were thought to prevent women from committing white collar crimes. As these opportunities for women become equal to men’s, some scholars believe women are committing more white collar crime and in ways more similar to men than in the past (see review in Steffensmeier, Schwartz, and Roche). Other scholars theorize that the change in sex differences between offenses by male and female criminals is still too large to draw conclusions. As an extension of this theory, socialization rather than opportunity is considered to have a greater role in driving female criminality (Steffensmeier, Schwartz, and Roche 5). These theories are significant because with the exception of a few specific crimes, many cyber crimes are similar to white-collar crimes; they just differ in the methods used to conduct the crime. For example, crimes such as larceny, fraud, forgery, and embezzlement also exist in the cyber domain. Therefore, many of the theories describing criminality referring to white-collar crimes should essentially be applicable to cyber crimes.

Due to this correlation it seems important to discuss women’s historical involvement with white collar crime. In 1989, Kathleen Daly published a study of the cases of 1,342 women and men convicted between 1976 and 1978 of non-violent economic crimes including fraud. Her main findings were as follows: First, of these cases only 14% were female, and second, women comprised of only 5% of those convicted of serious crimes such as antitrust law violations and securities fraud. The majority of female offenders were bank embezzlers who either stole cash or altered accounts as bank tellers. Due to the fact that most of the women in the study were unemployed or working in low-level positions, few women had the opportunity to participate in upper-level white-collar crime (Daly; Steffensmeier, Schwartz, and Roche 4).

Another major study of white-collar crime was recently conducted by Steffensmeier, Schwartz and Roche in which they examined female involvement and the gender gap in corporate fraud. They found that the large majority of corporate offenders were male, only about ten percent were female; and that all-male networks formed the preponderance of group-based corporate frauds. They also found that male corporate conspirators were more likely than female conspirators to play ringleader or major roles in the fraud conspiracy, and also that males profited far more from the conspiracy than did their female counterparts.

The present study regarding sex differences in crime anticipates persistent sex differences in the level and nature of cyber crime offending. This position draws on and offers a partial test of Steffensmeier and Allan’s (1996) gendered paradigm of female offending, which attributes sex differences in serious offending “to 1- Gendered focal concerns, socialization and risk preferences that condition gender differences in motivation and 2- Gendered crime opportunities” (qtd. in Steffensmeier, Schwartz, and Roche 4).

Gendered focal concerns and risk preferences are essentially polar opposites when comparing men and women, and the risk of disapproval by their communities shapes men’s and women’s willingness to commit crimes. Gender norms for women prioritize family obligations, strong relationships, beauty, and virtue. Men’s norms stress individualism, dominance, and achievement in public, and a private role as protector and provider. Men are encouraged to act competitively and decisively and to take significant risks in doing so. Women's norms are directly at odds with criminal behavior, while men's are permissive (Steffensmeier, Schwartz, and Roche 5).

These long-standing gender-based perceptions in society condition and socialize women and men to act or to be seen a certain way, allowing or suppressing behaviors that align with criminality. For example, a woman's desire to care for others and respond to their needs may make her less likely to behave in ways that can cause serious harm to others (Steffensmeier, Schwartz, and Roche 5). Another example is the conditioning of men to be status-seeking and the tendency for men to be more competitive and independent due to socialization (Steffensmeier, Schwartz, and Roche 5). It is easier for men to commit crimes which require or reward these behaviors, although fortunately it is not a guarantee of criminality. Additionally, because risk-taking is encouraged, violation of laws can be more easily justified by a man seeking status or wealth (Steffensmeier, Schwartz, and Roche 6). There is no similar match between women's focal concerns and criminality.

Gender-specific differences in risk-taking behavior reflect gendered focal concerns and match with motivations for criminal offending. When faced with decisions as entrepreneurs and managers, research shows women are more risk-averse than men. Male managers prefer to take aggressive actions, but women are more likely to use more conservative strategies (Steffensmeier, Schwartz, and Roche 6). An example of how this could relate to cyber crimes would be the risk of simple getting involved in a cyber crime. Another example would be the careful selection of victims for financially driven cyber crimes based on the level of risk assumed, due to the victim's status and the likelihood of attribution.

Based on previous work on gendered focal concerns and on criminal behavior, I expect the research in this study to show that the involvement of women in cyber crime is low. Additionally, I expect the nature and extent of female involvement in cyber crime to reflect their risk taking styles and gendered focal concerns.

Chapter 4

DATA AND METHODS

Methods

Since 2001, the Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice has published news releases regarding all cyber crimes that they prosecuted. Almost all of the cases covered by the CCIPS are cyber crimes that fall under Title 18 U.S.C. 1030, the Computer Fraud and Abuse Act. The Department of Justice (DOJ) created a repository of primarily cyber crime indictment press releases for cases that they investigated and prosecuted with the help of other government agencies. This repository contains cases from the year 2001 to the present.

The analysis in this paper makes use of the reposited press releases from the Department of Justice’s cyber crime archive for 2010. Each case in this sample involves one or more indictments and provides specific information regarding the defendants in the case, the alleged scheme or criminal act, and charges. In total, 53 cyber crime cases involving 101 defendants were included in the analysis of this paper. The press releases used in this paper contained information about each case that allowed for detailed analysis of the cases and their defendants.

Due to the perceived lack of female involvement in cyber crimes, a major undertaking of this paper was to place special emphasis on the extent, nature, and circumstances surrounding the involvement of women in cyber crime. To supplement the information gathered from evaluating the cyber crime database, a number of different electronic sources were utilized to provide further insight about women and cyber crimes. Some of the electronic sources that were found to be most useful were official indictment reports and online newspaper articles. Based on the information collected pertaining to the participation of women in cyber crimes, several characteristics were coded and then used for further investigation.

A coding scheme was developed to organize and describe the characteristics of the cyber crime cases and their offenders. This coding scheme attempts to quantify the major characteristics of each case to include: (a) defender characteristics; (b)victim; (c) conduct; (d) method of attack; (e) complexity of scheme; (f) seriousness of crime; (g) damage; (h) official action. The Department of Justice press releases served as the primary source of information for the creation of the cyber crime database. The information gathered for analysis focuses on the offending patterns, offender characteristics, and gender differences as they pertain to cyber crimes.

Offending Characteristics

In this section, the seven main offending categories used for analysis in this study are identified. An offending category is considered a characteristic that references the nature of offending for a particular cyber crime. Each offending category and its coding criteria will be presented and defined for further clarification.

Network is characterized by the number of defendants that were involved in the conduct and describes the dynamics of cyber crime participation:

Solo refers to the criminal activity being carried out by one individual

Multiple Co-conspirators refers to the criminal activity being carried out by multiple defendants

Victim identifies the entity harmed by the offense or targeted by the offender:

Individual refers to a single individual

Previous Employer refers to a company or business that previously employed the offender

Financial Institution refers to banking institutions and e-commerce websites

Government refers to entities associated with the government

Other refers to all miscellaneous companies, businesses, and websites

Conduct gives a high level description of the computer crime committed or being investigated:

Extortion refers to the act of using force, threats, or violence to obtain property or direct benefits

Cyber Theft refers to the act of stealing an individual's personal information or a company's customer, employee, or proprietary data

Cyber Threats refers to threats via electronic transmission

Cyber Fraud refers to the act of using deception online for personal gain or to cause another person or entity to suffer damages

Cyber Stalking refers to the use of online communication or activities to harass

Denial of Service refers to the act of making services unavailable to its intended users

Other refers to system destruction or software piracy

Method of Attack describes the technique or method used by the defendant to commit the criminal act:

Social Engineering refers to the art of deceiving or manipulating individuals into performing actions or divulging confidential information

Botnet refers to a collection of compromised computers used to remotely make computer resources unavailable to intended users

Insider Threat refers to a malicious act committed by a trusted source to include the misuse of granted privileges or unauthorized escalation of privileges

Hacking refers to the act of gaining unauthorized access to a computer, system, or network

Spamming refers to the mass transmission of unsolicited messages using an electronic messaging system

Other refers to use of criminal contacts to sell stolen information

Complexity of Scheme describes the relative measure of difficulty surrounding the commission of the criminal act using a specific set of criteria. The criteria used to determine a scheme's level of complexity were based on subjective descriptions included in each press release such as; level of sophistication, resources needed, time needed, and the methods used to conduct the attack:

Simple refers to a scheme that is not very sophisticated and has a requires a low level of technical knowledge

In-between refers to a scheme that has a medium level of sophistication and requires a medium level of technical knowledge

Complex refers to a scheme that has a high level of sophistication and requires a substantial technical knowledge

Seriousness of Crime describes the damage or impact level of a crime. The seriousness of a crime was determined using information such as: amount of financial loss (implied and explicit), extent of reputational damage, and volume/importance of lost or compromised data:

Low refers to a crime that has a financial loss below $20,000, minimum reputational damage, or a low volume/importance of lost or compromised data

Medium refers to a crime that has a financial loss greater than $100,000, moderate reputational damage, or a moderate volume/importance of lost or compromised data

High refers to a crime that has a financial loss greater than $100,000, serious reputational damage, or high volume/importance of lost or compromised data

Damage classifies the type of loss or harm expected or caused by a criminal act

Financial refers to a crime where there is a monetary loss

Business refers to a loss of intellectual property, trade secrets, or availability of services

Social refers to a loss of reputation, privacy, or confidential information

Political refers to a loss of status, image, or leverage in the political arena

Governmental refers to a loss of national security

Offender Characteristics

In this section, the four main offender categories used for analysis in this studied are discussed. An offender category is a characteristic that references the demographics and interest of an offender for a particular cyber crime. Each category and its coding criteria will be presented and defined for further clarification. Where main offender categories contain sub-categories, they will be presented and defined accordingly.

Age is the age of the defendant at the time in which the press release was published. In most cases the age of each defendant was found in each press release in numerical form. When the age of a defendant was not available in a press release, online searches were conducted using the defendants name and the date of the press release to determine their age.

Gender was determined using the defendant's name. When the gender of a defendant could not be determined by the defendant's name, textual clues (e.g. he/she pronoun) or online searches were used to determine or verify a defendant's gender as male or female.

Role in Scheme describes the involvement of the defendant in planning, fostering, and executing the investigated schemes. This characteristic serves as an indicator to determine whether or not institutionalized sexism is a component of a particular type of crime, such as cyber crime. A defendant's role in a scheme is determined by using the press release's description of their participation level, the number and range of charges for each defendant, and the identification of defendant relationships (e.g. sister, cousin, and father). The levels of involvement are:

> *Ring Leader* refers to a defendant that is identified as a solo offender or as the primary offender who planned and executed the scheme
>
> *Co-conspirator* refers to a defendant who had significant involvement in the furthering of the scheme or conspiracy
>
> *Accomplice* refers to a defendant who had a minor role in the scheme or acted on behalf of a relative or superior

Motive refers to the defendant’s reason or justification for engaging in the scheme or criminal act

Financial Gain refers to a criminal act committed for profit

Revenge refers to a criminal act committed in response to a grievance

Political Interest refers to a criminal act committed for a political cause

Status/Recognition refers to a criminal act committed for acknowledgement or street credit

Special Interest refers to a criminal act committed for fun, warfare, or a miscellaneous purpose

Due to the high level of detail used to analyze the data presented in this paper, it is highly recommended for all readers to reference this section for further explanation on all descriptors and characteristics covered in the next chapter. In the next chapter, the findings from the 2010 Department of Justice Cyber Crime Dataset will be presented and discussed.

Chapter 5

ANALYSIS AND FINDINGS

In the following section, the offense and offender characteristics of cybercrimes will first be presented in general and then by gender. An in-depth analysis was performed on the results of the 2010 Cyber Crime Database (CCD) to identify key offender characteristics and offending patterns. To create the CCD, information was extracted from cyber crime press releases archived by the Department of Justice. The CCD is composed of 53 cases and 101 defendants; 15 women and 86 men. The analysis performed on the CCD allowed for each cyber crime case to be dissected using specific criteria to provide an overview of the crime, charges, and defendants involved. Information extracted from the CCD, is evaluated using descriptive and bivariate analyses, focusing in particular on gender differences.

Section 1: General Cyber Crime Offender and Offending Characteristics

Table 1 provides an overview of the general cyber crime offender characteristics for the total sample. In order to create a baseline for cyber crime offender characteristics, the results observed in the CCD that specifically relate to the general offender will be discussed. The cyber crime offender characteristic categories were chosen based on their ability to describe offenders in general: role in scheme, average age, motive, and financial gain/amount.

Table 1. General Cyber Crime Offender Characteristics

General Offender Characteristics	Count	Percentage
N(Number of Defendants) = 101		
Age		
Mean *33.6* Range *19 - 66*		
Role In Scheme		
Ring Leader	35	35
Co-conspirator	59	58
Accomplice	7	7
Motive		
Financial	70	69
Revenge	10	10
Political/Special Interest	11	11
Recognition	0	0
Special Interest	10	10
Financial Gain		
Yes	63	62
No	33	33
Unknown	5	5
Amount of Financial Gain		
Amount > 1million	39	62
Amount < 1 million	7	11
Amount Unknown	17	27

Role in Scheme. As shown in Table 2, cyber crime offenders tend to engage in crimes as co-conspirators (about 60%), rather than as ring leaders (35%) or accomplices (7%). When analyzing these numbers it seems as though collaboration, one of the key elements of the Hacker subculture is also a characteristic of the general cyber crime subculture (Holt; Moore 51). Although these results support the notion that cybercriminals tend to work as partners, it is possible that accomplices and ring leaders are less likely to get caught in comparison to co-conspirators. Unfortunately, due to a lack of information, the specific roles of many cybercriminals identified as conspirators were unable to be determined. Therefore, it is unclear whether or not conspirators had equal participation in the cyber crimes being investigated.

Average Age. The average age of a cybercriminal in this study is 34. The range of ages for cybercriminals in this dataset was 19-66, with men being both the oldest and the youngest cybercriminals. Although cybercriminals are depicted as young individuals in several movies such as *War Games* and *Hackers*, the data in this study show that the average age of a hacker is slightly higher.

Motive. In many cases determining the motive for a criminal act is a difficult process, but for cyber crimes the offender's motive is often obvious from the crime. Financial Gain (70%) was the leading motive for cybercriminals in the CCD. Supporting recent cyber crime studies or reports, this finding suggests that cyber crimes today are for the most part financially-driven (Verizon 18; PwC 6).

Among other factors, the 2008-2009 financial crisis is also believed to be one of the primary factors that contributed to financial gain becoming the leading motive for recent cyber crimes (Deloitte 2010 6). Another enabler of the cyber crime economy is the growing popularity of the cyber crime black market which facilitates the commission of many cyber crimes for financial gain (Brewster). With 83% of cyber crimes being committed primarily because of opportunity, it is not hard to understand why cybercriminals would now prefer to commit these crimes for profit (Verizon 52).

Financial Gain and Amount of Financial Gain. As is evident from Table 1, cyber crime continues to be profitable. Out of the total number of cybercriminals included in the dataset, about 63% of them were involved in schemes that had a confirmed financial gain. Additionally, 62% of those cybercriminals that had a financial gain profited more than $1 million from their illegal activities. The financial gains of cybercriminals ranged from thousands to hundreds of millions. This finding supports the claim that the majority of cyber crimes today are financially-driven, although an alternative explanation could be that the Department of Justice focuses on investigating cyber crimes that involve significant amounts of money.

Summary. Several outstanding offender characteristics were observed in Table 1. The average cybercriminal in this data set is a person in his or her mid-thirties who prefers to work with other co-conspirators for financial gain that is often more than a million in profit.

Table 2 provides an overview of key general cyber crime offending characteristics. In order to create a baseline for cyber crime offending patterns, the results of the CCD that pertain to specific offense characteristics will now be discussed. Seven offense characteristics were used to analyze the dataset and they are: victim, network, conduct, method of attack, complexity of scheme, seriousness of crime, and damage.

Table 2. General Cyber Crime Offending Characteristics

General Offending Characteristics	Count	Percentage
N(Number of Total Defendants) = 101		
Victim		
Individual	22	22
Business	38	37
Previous Employer	10	10
Financial Institution	15	15
Educational Institution	4	4
Church	2	2
Government	5	5
Other	5	5
Network		
Solo	32	32
Multiple Co-conspirators	69	68
Conduct		
Cyber Fraud	45	44
Extortion	2	2
Cyber Theft	26	26
Cyber Threats	5	5
Cyber Stalking	1	1
Denial of Service	9	9
Other	13	13
Method of Attack		
Social Engineering	24	24
Botnet	5	5
Insider Threat	26	26
Hacking	39	38
Spamming	4	4
Other	3	3
Complexity of Scheme		
Simple	26	26
In-between	19	19
Complex	56	55
Seriousness of Crime		
Low	25	25
Medium	21	21
High	55	54
Damage		
Financial	59	58
Social	18	18
Business	6	6
Political	7	7
Governmental	1	1
Business/Financial	10	10

Victim. Due to the nature of cyber crime, there are many potential victims that can fall prey to these crimes. Although there are many potential victims, cybercriminals prefer to attack businesses 37% of the time according to the 2010 CCD. Following businesses are individuals (22%), financial institutions (15%), previous employers (10%), government (5%), educational institutions (4%), church (2%), and other (5%). Taken together, the top two types of cyber crime victims, businesses and individuals, made up about 60% of all cyber crime victims.

It is widely understood in the security field that end-users are the weakest link from a security standpoint and therefore considered the most vulnerable to cyber crime victimization. On the other hand, businesses such as those in the hotel and retail sectors tend to be easier less reactive targets than, for instance, financial institutions (Verizon 12). This finding is significant because the recent rise of cyber crimes targeting businesses in the hospitality and retail sectors is an indication that cybercriminals may now be making classic risks vs. rewards decisions (Verizon 12).

Network. Considering that the number of cybercriminals that worked with co-conspirators was 60%, it is not surprising that 68% of the cybercriminals included in the CCD were indicted along with multiple co-conspirators. On the contrary, 32% of cybercriminals were identified to be solo perpetrators. This finding supports the claim that cybercriminals tend to partner or collaborate with others when committing cyber crimes. Moreover, it appears as though collaboration, a cornerstone value in the hacker subculture, is also valued among cybercriminals in general.

Conduct. When discussing the conduct or type of cyber crime committed by a cybercriminal it is important to keep in mind that each conduct is linked to a motive and an opportunity. Additionally, it is important to remember that the conduct associated with many cyber crimes is similar to that of traditional crimes. According to the results, cyber fraud is the leading type of cyber crime conduct accounting for 44% of all cyber crime conducted. As defined in the methods section of this paper, cyber fraud is a type of cyber crime conduct that involves the use of deception online for personal gain or to cause another person or entity to suffer harm or damages. The second most numerous crime is cyber theft at 26%, while the category “other” cyber crimes (for example software piracy and system destruction), accounted for about 13% of all CCD cybercrimes, as shown in Table 2. The relatively high numbers of cyber fraud and cyber theft cases identified in this study align with the 2010 Cyber Security Watch Survey report that states “There are countless opportunities for cyber crimes such as cyber theft and cyber fraud due to social networking and the recent influx of online banking and retails sales”(Deloitte 2010 6).

Some of the popular types of cyber fraud often investigated today are identity theft schemes and phishing schemes. One example of a cyber fraud cyber crime analyzed in this study is a case that involved the hacking and defrauding of online ticket vendors such as Ticketmaster. The defendants in this case fraudulently purchased best seat tickets in bulk for a number of marquee events using advanced computer software. Fictitious websites were then created by the defendants to resell these tickets to the general public. Although all cyber fraud cases are not exactly like this example, the key is to understand that one major motive of cyber fraud is to deceive a victim for financial gain using the Internet.

Method of Attack. The method of attack can be used to determine the attack vectors commonly used to commit cyber crimes. This type of information is important because it can allow security professionals to focus on the attack vectors most often exploited. According to the dataset created for this report, hacking is the leading method of attack for cyber crimes, accounting for about 38% of all cyber crimes. This statistic supports the assertion in the 2011 Verizon Data Breach report that found hacking to be responsible for about 50% of all cyber-attacks (Verizon 24). The same report also found that 76% percent of the records in their study were from compromised servers, demonstrating that attackers prefer to use specific methods of attack on certain attack vectors (Verizon 43).

Other common methods of attack, such as the insider threat and social engineering were responsible for 26% and 24% of the cybercrime methods, respectively. An example of an insider threat would be an employee of a company selling company trade secrets for personal gain. On the other hand, an example of a cyber crime carried out using social engineering as the method could involve a cybercriminal simply sending an email to a HR representative requesting company information while masquerading as one of the company's executives. Although seemingly not as common as hacking, insider threat and social engineering methods are gaining the attention of many security specialists due to their ability to go undetected and their potential for significant impacts.

Complexity of Scheme. Although difficult to determine, the complexity of a cyber crime scheme is exposed by the technical aptitude, time, and amount of resources needed to commit a particular cyber crime. Complex cyber crime schemes accounted for a slight majority (55%) of cyber crime cases in the CCD. Simple cyber crime schemes comprised only 26% of cases. These findings suggest that the majority of cyber crimes are complex in nature. However, a 2011 report found that 92% of cyber-attacks were not of high technical difficulty (Verizon 3). One explanation for the contrast in these two findings is the possible use of different criteria to determine the complexity of the cyber crime scheme. Another possible explanation for the disparity between these two findings is that cyber crimes considered to be complex in nature may be prioritized by the Department of Justice and thus make up the large majority of cases investigated.

Seriousness of Crime. The seriousness of cyber crime is typically determined by both its immediate and future impact. (For example, a denial of service attack on a website can cause an immediate financial loss due to unavailable goods or services, and a future impact due to a damaged brand reputation.) Cyber crimes with a high seriousness level (54%) were responsible for the majority of all cyber crimes in the dataset. Cyber crimes with a seriousness level of Low accounted for 25% of all cyber crimes in the CCD. As defined in the methods section in this paper, cyber crimes with a seriousness level of low refer to cyber crimes that had a financial loss below $20,000, minimum reputational damage, or a low volume/importance of lost or compromised data. Additionally, cyber crimes ranked as high in seriousness refer to cyber crimes that involved a financial loss greater than $100,000, serious reputational damage, or high volume/importance of lost or compromised data.

Damage. Determining the types of damage that cybercriminals cause most often is an essential step in the process of identifying what cybercriminals are trying to accomplish. The majority of cyber crimes in the CCD caused financial damage (58%). After financial damage there is a sharp decline between the next most frequent type of damage, social damage at 18%. As mentioned in the previous section, cyber crimes today are considered by many to be for the most part financially-driven and the results shown in Table 2 support this claim. The financial damages of many cyber crimes are not just direct cost; they also include costs related to reputational damage, lost sales, and payment of security professionals to investigate the cyber crime.

Summary. At this point many general cyber crime offending patterns have been identified, but there are a few that stand out more than others. Individuals and businesses are the primary targets for cyber crimes. A majority (60%) of cybercriminals work with other co-conspirators. The leading type of cyber crime or conduct is cyber fraud at 44%. Hacking is most common method of attack responsible for approximately 38% of all cyber crime methods. Complex cyber crime schemes (55%) accounted for the majority of all cyber crimes in this study. A similar percentage had a high seriousness level (54%). The leading type of damage caused by cybercriminals was financial damage (58%).

Section 2: Cyber Crime Offender and Offending Characteristics by Gender

The next section addresses what is a main focus of this study, female involvement and the gender gap in cybercrime. To uncover the extent and nature of female involvement in cyber crime, two distinct comparisons are utilized. First, the offender profile percentage measures the percent within each sex that is represented at varying levels of a particular case characteristic. The purpose of this comparison is to demonstrate whether the profile of a typical female corporate offender differs from the typical male in all cyber crimes. Second, the gender gap is the level or share of female offending in relation to that of males associated with a characteristic. "The gender gap is a between-sex measure that establishes the size and direction of the sex difference between women and men" (Steffensmeier, Schwartz, and Roche 15). Furthermore, patterns and preferences of female involvement revealed using the two comparisons will allow for a greater understanding of the female cybercriminal.

Table 3 displays how cybercrime offender characteristics differ by gender. Two notable findings were uncovered in this section. First, women made up only 15% of all cybercriminals in this study with men accounting for the other 85%. This sex difference is significant because it shows a similar level of female involvement in cyber crime compared to the 5-14% estimate of female involvement in Daly's 1989 white-collar crime study, and compared to the roughly 10% involvement in the Steffensmeier et al. study. Second, similar to Steffensmeier et al., there were no cases of all female conspiracy groups (Steffensmeier, Schwartz, and Roche 10).

Table 3 - Cyber Crime Offender Characteristics by Gender

Offender Characteristics	Male Profile		Female Profile		Gender Gap
	N	%	n	%	%Female
Number/Pct. of Defendants	86	100	15	100	15
Age of Offender					
Mean	33.1		36.5		
Range	19-66		21-54		
Role in Scheme					
Ring Leader	32	37	3	20	9
Co-conspirator	49	57	10	67	17
Accomplice	5	6	2	13	29
Motive					
Financial	62	72	8	53	11
Revenge	8	9	2	13	20
Political/Special Interest	6	7	5	33	45
Recognition	0	0	0	0	0
Special Interest	10	12	0	0	0
Financial Gain					
Yes	55	64	8	53	13
No	26	30	7	47	21
Amount of Financial Gain					
Amount > 1 million	31	56	8	100	21
Amount < 1million	7	13	0	0	0
Amount Unknown	17	31	0	0	0

NOTE: The Gender profile measures the percentage of representation of males and females respectively for a particular case characteristic and the Gender gap measures the percent female among offenders in cyber crimes

Role in Scheme. Almost 70% of the females in this study are identified as co-conspirators, but when compared to men they are heavily underrepresented making up only 17% of all co-conspirators. This trend holds true for roles as accomplices and ring leaders, however women appear to have the smallest gender gap when acting as accomplices. Not only are males much more likely to be involved in cyber crime, but they are also more likely to be involved as ring leaders. The majority of women were involved as co-conspirators.

Average Age. The average age of a male cyber crime offender in this study is 33, and the average age of female cyber crime offenders is about 37. Male cybercriminals ranged from 19-66 years of age whereas female cybercriminals ranged from 21-54 years of age. In this study, female cybercriminals were found to be on average about 4 years older than male cybercriminals.

Motive. Financial gain is the top motive for both female (53%) and male (72%) offenders, but women only account for about 11% of all cybercriminals who have a motive of financial gain for cyber crime. In contrast, the second most common cyber crime motive for women is political or special interest, which happens to be the second least common cyber crime motive for males. Moreover, the gender gap is smallest between men and women for cyber crimes that are driven by a political or special interest motive. The motive of a female cybercriminal is tied to the choice of victim. The largest category of victims (43%) of cyber crimes involving female offenders was individuals targeted for a political or special interest or revenge motive. This suggests that if females are involved in cybercrime, they are motivated by politics or revenge and their victims are individuals.

Building upon the claim that motive is tied to a type of victim for women; only 2 females in this study out of the total number of female cybercriminals engaged in a cyber crime were interested in revenge. This is significant because 2 out of the 3 female ringleaders in the CCD were solo offenders seeking revenge. In conclusion, the figures show that financial gain and political and special interest are the top cyber crime motives for women. Furthermore, the data suggests that when financial gain or political interests are the cyber crime motives, women tend to work with others, whereas if the motive is revenge women tend to work alone.

Financial Gain and Amount of Financial Gain. Due to the wide range of benefits associated with financial gain, whether or not a cyber crime offender profits can be a useful marker of involvement. In this study, the majority of male (64%) and female (56%) offenders had a financial gain, but women only accounted for 13% of all offenders that had a financial gain. Although women only accounted for 13% of all cybercriminals that had a financial gain, they made up 21% of all cybercriminals that had a financial gain greater than 1million. Therefore, if we assume that all co-conspirators involved in the cyber crimes referenced above received equal profits, women make just as much profit from cyber crimes as men. Unfortunately, from this limited data there is no way to determine how profits were shared among co-conspirators to confirm this assertion.

Summary. The main findings are: Males are more likely to be involved in cybercrimes, males are also more likely to be ring leaders, and there are a fairly-sizable number of all-male conspiracies but no all-female conspiracy groups. The major similarity between male and female offenders is that financial gain is the top motive for committing cyber crimes.

Table 4 - Cyber Crime Offending Characteristics by Gender

Offending Characteristics	**Male Profile**		**Female Profile**		**Gender Gap**
	n	**%**	**n**	**%**	**%Female**
Number/Pct. of Defendants	86	100	15	100	15
Victim					
Individual	15	17	7	47	32
Business	35	41	3	20	8
Previous Employer	9	10	1	7	10
Financial Institution	11	13	4	27	27
Educational Institution	4	5	0	0	0
Church	2	2	0	0	0
Government	5	6	0	0	0
Other	5	6	0	0	0
Network					
Solo	29	34	3	20	9
Multiple Co-conspirators	57	66	12	80	17
Conduct					
Cyber Fraud	42	49	3	20	7
Extortion	2	2	0	0	0
Cyber Theft	16	19	10	66	38
Cyber Threats	4	5	1	7	20
Cyber Stalking	1	1	0	0	0
Denial of Service	9	10	0	0	0
Other	12	14	1	7	8
Method of Attack					
Social Engineering	21	24	3	20	12
Botnet	5	6	0	0	0
Insider Threat	17	20	9	60	35
Hacking	36	42	3	20	8
Spamming	4	5	0	0	0
Other	3	3	0	0	0
Complexity of Scheme					
Simple	16	19	10	67	38
In-between	18	21	1	7	5
Complex	52	60	4	27	7
Seriousness of Crime					
Low	18	21	7	47	25
Medium	21	24	0	0	0
High	47	55	8	53	15
Damage					
Financial	51	59	8	53	14
Social	16	19	2	13	11
Business	6	7	0	0	0
Political	2	2	5	33	71
Governmental	1	1	0	0	0
Business/Financial	10	12	0	0	0

Table 4 displays how cyber crime offending characteristics differ by gender for each of the following: victim, network, conduct, method of attack, complexity of scheme, seriousness of crime, and damage.

Victim. Victims of cyber crimes become victims for a number of different reasons. Many cyber crimes are said to be opportunistic (83%) in nature as opposed to targeted attacks (17%), but a significant number of targeted cyber crimes are driven by specific motivations (Verizon 52). As shown in the gender gap figures in Table 4, women are severely underrepresented as offenders for most victim categories; exceptions are individuals (41%) and financial institutions (24%). Simply put, the data in this study suggests that women cybercriminals, when compared to men, target individuals and financial institutions more often than other victims. More detailed analysis, as presented in Appendix C, indicates that when women are involved, individuals as victims are typically targeted by women for political motives, while most other victims are targeted for financial gain motives.

Network. Most defendants male and female were involved in cybercrime networks. For females, three were involved as solo defendants and the remaining twelve were involved in networks. The largest network involved 19 defendants, and 5 of those defendants were women.

In addition, if involved in a cybercriminal network, females tend to be involved in a network that is larger than usual. The average size of a cybercriminal network involving female co-conspirators was 10 people. Therefore, the data indicates that women cybercriminals not only like to work with other co-conspirators, but that they prefer large networks.

Conduct. , Cyber crime refers to a number of different types of criminal conduct, and substantial sex differences exist in the types of cyber crime committed by offenders. Although cyber fraud represented 45% of the cyber crime conducts in this study, women were only represented in 7% of these crimes. In contrast, the majority of female cybercriminals (66%) in the CCD engaged in cyber theft as a cyber crime and had a gender gap near parity (38%) when compared to their male counterparts. These figures suggest that women cybercriminals prefer to commit information theft when involved in cybercriminal activity. Multivariate analysis indicates that 89% of the information theft attacks involving women were considered to be simple crimes in terms of overall complexity. Therefore, it appears that women tend to be involved in cyber thefts, which are relatively simple and to some extent low-risk. These findings are consistent with the predictions of the gendered paradigm theory.

Method of Attack. Gender differences in the methods used by cybercriminals are sizeable. Overwhelmingly, men (42%) utilized some form of hacking to carry out their cyber crimes, whereas only 20% of women used hacking at all. Conversely, women utilized insider access and social engineering tactics as 80% of their methods to conduct cyber-attack. Cyber crimes that utilize social engineering tactics or the insider threat to commit a cyber crime do not typically require a high level of technical skill; however, they do often require the individual to have good communication skills and the ability to establish a sense of trust with the victim, which is consistent with women's gendered focal concerns.

Complexity of Scheme. The majority (67%) of female cybercriminals in this study were found to have been involved in cyber crimes identified as simple, whereas the majority of males (60%)

were involved in complex cyber crimes. This finding suggests that women in many cases don’t have the interest to be involved in highly complex cyber crimes. Less likely explanations include that the majority of women don’t have the technical skills necessary to commit a highly complex cyber crime or that highly skilled women cybercriminals almost completely avoid detection. Females overall engaged in cyber crimes that were simple in complexity, but when working in large groups they engaged in more complex schemes.

Seriousness of Crime. When it comes to the seriousness of the cyber crime, female cybercriminals are pretty evenly split between their involvement in high seriousness crimes (53%) and low seriousness cyber crimes (47%) having no involvement in cyber crimes that have a medium level of seriousness. Men, on the other hand are involved at some level in cyber crimes at all seriousness levels with high being the majority (55%). The database lacks specific information about the extent to which females involved in collusion schemes shared equally in the profits.

Damage. Damage caused by cyber crimes with female involvement is typically financial (59%) and political (33%). It is apparent that damages caused by female cybercriminals are aligned with the motivations of female cybercriminals. However, these findings could also be explained by the tendency for women to work with co-conspirators who have financial and political agendas when engaged in cyber crime.

Summary. Taken together, the results portray female cybercriminals as co-conspirators who engage in simple kinds of cyber fraud and cyber theft, using mainly social engineering and insider access to target individuals and financial institutions for purposes of financial gain or political damage. By comparison, men are more likely to be involved as ringleaders who engage in highly complex cyber fraud schemes targeted mainly at businesses and typically causing considerable financial or social damage. Although some similarities exist between male and female cybercriminals, there are also many differences in their cyber crime profiles describing their extent and nature of involvement.

On par with the expectations based on the gendered paradigm theory, women were found to have minimal overall involvement in cyber crimes based on cases identified and investigated by the Department of Justice in 2010. Furthermore, the level of female involvement in cyber crime closely resembles the level of female involvement in white collar or corporate crime (Daly; Steffenmeier, Schwartz, and Roche). Several findings indicate that women are limited in their opportunities to engage in cyber crimes due to sex segregation presumably a result of the hacker/cybercriminal subculture. Based on the analysis of female cybercriminals in the CCD, findings suggest that gendered focal concerns do in fact shape the nature and extent of a female's involvement in cyber crime. Finally, the data suggest that when women do commit cyber crimes, they are more risk-averse when it comes to the method and type of crime they choose to commit.

Chapter 5

DISCUSSION AND CONCLUSION

In this study, the patterns and characteristics associated with modern day cyber crimes and cybercriminals were investigated. Consistent with the findings of several well-known cyber crime studies and reports, the findings in this paper show that the majority of cyber crimes are committed by men, many cyber crimes are similar in nature to traditional crimes, and that cybercriminals have noticeable differences when analyzed by gender.

The patterns of criminality found in this study are consistent with previous reports. The first key finding of this study is that today many cyber crimes are financially motivated. This finding is consistent with the findings of several reports such as the Global Economic Crime Survey and the 2011 Verizon Data Breach Report which also claim that cyber crimes today are mainly financially-driven (PwC 6; Verizon 18). Another key finding is that 45% of the cyber crimes in this study were considered cyber fraud. This finding is consistent with the 2010 Cyber Security Watch Survey claim that “There are increased opportunities for cyber crimes such as cyber theft and cyber fraud due to social networking and the recent influx of online banking and retails sales” (Deloitte 2010 6). The last key finding identified in this study is that businesses are the most often targeted victims for cyber crimes. Although broad in nature, this finding is consistent with the results of the 2011 Verizon DBIR cyber crime report, which indicates a rise in hospitality and retail sector victims of cyber crimes (Verizon 12). Additional findings, show that cybercriminals are individuals in their mid-thirties that tend to work as co-conspirators (70%), and use similar methods to carry out various cyber crimes

Significant gender differences were found in both the nature and extent of women’s involvement in cyber crimes, consistent with the gendered focal concerns and gendered crime opportunities used to frame this study. First, the majority of cybercriminals are male, with women only accounting for about 15% of all cyber crime offenders in this study. Although women seemingly have the skills and opportunities to commit cyber crimes, this finding suggests that the overall involvement of women in cyber crimes is low and similar to their level of female involvement found in several white collar crime studies.

Second, financial gain was the top motive for male and female cybercriminals. However, the second most common motive for females was political/special interest, as compared to general special interest for males. This finding suggests that women in this study were committing cyber crimes partly due to a strong emotional tie or relationship.

Third, cybercriminals preferred to work in conspiracy groups. However, women were non-existent in the majority of these groups. This finding suggests that women have a lack of opportunities to join cybercriminal networks possibly due to views of women that exist in the hacker sub-culture and sex segregation, which are also seen in white collar criminal networks.

Fourth, female cybercriminals mainly targeted individuals and financial institutions as victims, whereas the large majority of men targeted businesses. Because women prefer to attack individuals more than any other victim, it is possible that women's gendered focal concern of being nuturant determines who they target as cyber crime victims.

Fifth, female cybercriminals heavily relied on social engineering tactics and insider access to commit cyber crimes, whereas males most often used hacking. Although women may have the skills to be hackers, it appears they rely more on other methods of attack such as social engineering to not use this method of attack in this study. Instead, women chose to use more stealthy methods of attack such as the insider threat and social engineering. These methods of attack, in many cases, leave a light evidence trail and typically allow for more anonymity and less chance for attribution. Therefore, it is possible that women prefer to take less risk when selecting their cyber crime method of attack than men.

Sixth, the majority of female cybercriminals were engaged in cyber theft, whereas males were more involved in cyber fraud. The majority of the cyber theft crimes that women engaged in were identified to be simple in nature. Therefore, the data suggest that women tend to engage in crimes that are of low complexity and that most likely involve less risk. Additionally, this finding parallels Daly's findings regarding the types of white collar crime that women commit.

Seventh, female cybercriminals were mainly involved in cyber crimes identified to be simple in nature, whereas males were mainly involved in complex cyber crimes. This finding suggests that women tend to be involved in less complex cyber crime schemes, consistent with their conservative risk-taking style. An alternative explanation for this finding could be that women lack the opportunity to be involved in highly complex cyber schemes due to sex segregation and the cybercriminal subculture.

Taken together, the findings above show sizable differences between male and female cybercriminals. Moreover, the characteristics of cyber crime offending illustrated by the observed tendencies of female cybercriminals suggest that female cybercriminals, while small in numbers, are distinct. Whether or not females are to be feared just as much or more than males as cybercriminals cannot be determined based solely on the findings in this study. However, female offenders deserve special attention as more research on cyber crime offender characteristics is conducted in the future.

The general and gender-specific findings of this study are consistent with several highly regarded cyber crime studies and research conducted on female criminals. For instance, the general cyber crime findings in this study for types of cyber crimes and attack methods correlate with findings in the 2011 Verizon Data Breach Report and the 2011 Symantec State of Security Survey (Verizon; Symantec Survey), ultimately, supporting the claim that cybercriminals are creatures of habit. The observed small number of females that operate as ring leaders in cyber crimes, and the perceived limited opportunities for women to join cyber crime networks support the notion that women are less likely to be cybercriminals than men.

Although the findings of this study are suggestive, more comprehensive research and analysis is needed to make declarative statements regarding cyber crime offending patterns, offender characteristics. Although there is no way to determine the total number of cyber crimes that take place in any given year, we recognize that the database used in this study is small when compared to the known population of cyber crimes that occurred during 2010. Correspondingly, many cyber crimes today are not prosecuted due to a lack of detection, attribution, and reporting which is the responsibility of many different parties. Therefore, standards on cyber crime reporting, advanced cyber forensic technologies and more skilled cyber security specialist are needed to conduct effective cyber crime research. Additionally, several different sources collect information related to cyber crimes and its offenders, but the information in many cases is not complete or detailed. For this reason, more sources charged with the task of collecting detailed information on cyber crimes are definitely a future need.

In addition, more research and collaboration among security specialists on this subject will hopefully allow security to become more proactive than reactive. Further research is needed to accurately describe the true extent to which women are involved in cyber crimes. The findings in this study raise questions such as: Do women appear to be less involved in cyber crime because they are more stealthy and covert? Is the number of known female cybercriminals significantly less than that of males because they are more skilled at conducting cyber crimes? Are women less involved in cyber crimes because there are a disproportionately low number of females in technology related fields? At the current time there are many different potential explanations that need to be explored in order to explain the observed limited involvement of women in cyber crimes.

To obtain more insight about cyber crime offenders I recommend a number of different information gathering techniques. First, strategies of inquiry such as interviews and surveys of cybercriminals should be used to get a fundamental understanding of the thought processes and motivations of cybercriminals as they commit cyber crimes. Second, research that focuses on the dynamics of cybercriminal communities is needed to understand how women are viewed and treated in the cybercriminal sub-culture and hacking community.

In conclusion, research regarding offender characteristics, and offending patterns with special interest on women can contribute greatly to the area of risk analysis as it pertains to cyber crime. It is my hope that by using the findings of this study in conjunction with the strategies mentioned above, cybercriminal profiling will improve and risk assessment and management strategies in the cyber domain will become more effective. Additional research in these areas would contribute to a more global and comprehensive understanding of cyber crimes and their offenders as well as potential advances in the area of cybercriminal profiling.

BIBLIOGRAPHY

Alaganandam, Hemavathy, Pravin Mittal, Avichal Singh, and Chris Fleizach. "Cybercriminal Activity." *Sysnet.ucsd.edu*. UC San Diego, 6 Dec. 2005. Web. 6 Apr. 2012. <http://sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf>.

Batke, Kelly. "7 Types of Cybercriminals." *Faronics*. Faronics Corporation, 21 Dec. 2011. Web. 06 Apr. 2012. http://www.**f**aronics.com/2011/7-types-of-cyber-criminals/

Bednarz, Ann. "Profiling Cybercriminals: A Promising but Immature Science." *Network World*. Network World, 29 Nov. 2004. Web. 03 Apr. 2012. <http://www.networkworld.com/supp/2004/cybercrime/112904profile.html>.

Bogden, James T. "Cybercriminals: Identify and Prosecute?" *: CyberCriminals: Identify and Prosecute?* Blogger, 27 Dec. 2011. Web. 06 Apr. 2012. <http://jtbogden.blogspot.com/2011/12/cybercriminals-identify-and-prosecute.html>.

Brewster, Tom. "Panda Warns of Cyber Black Market." *SC Magazine*. Haymarket Media, 21 Jan. 2011. Web. 06 Apr. 2012. <http://www.scmagazine.com.au/News/245606%2Cpanda-warns-of-cyber-black-market.aspx>.

Cowley, Stacy. "FBI Director Says Cybercrime Will Eclipse Terrorism." *CNNMoney*. Cable News Network, 02 Mar. 2012. Web. 03 Apr. 2012. <http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm>.

Daly, Kathleen. "Gender And Varieties Of White-Collar Crime." *Criminology* 27.4 (1989): 769-94. Print.

Deloitte. "2011 Cyber Security Watch Survey Results." CSO Magazine, Jan. 2011. Web. 5 Oct. 2011. <http://mkting.csoonline.com/pdf/2011_CyberSecurityWatch.pdf>.

Deloitte. "Cyber Crime: A Clear and Present Danger Combating the Fastest Growing Cyber Security Threat." Center for Security and Privacy Solutions, 2010. Web. 5 Oct. 2011. <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf>

DOJ. "USDOJ: CRM: Computer Crime & Intellectual Property Section." *Welcome to the United States Department of Justice*. Justice.gov, 2010. Web. 08 Apr. 2012. <http://www.justice.gov/criminal/cybercrime/press-releases/2010.html>

FBI. "Addressing Threats to the Nation's Cybersecurity." FBI. Web. 5 Apr. 2012. <http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity>.

Frieze, Carol. "Pioneering Women in Computing Technology." *The Ada Project*. Carnegie Mellon, 1 Oct. 2005. Web. 06 Apr. 2012. <http://women.cs.cmu.edu/ada/Resources/Women/>.

Holt, T. J. (2005). Hacks, cracks, and crime: An examination of the subculture and social organization of computer hackers. University of Missouri – Saint Louis. ProQuest Dissertations and Theses, Retrieved from

Moore, Robert. *Cybercrime: Investigating High-Technology Computer Crime*. Burlington: Elsevier Science, 2010. Internet resource.

NCWIT. "NCWIT : About NCWIT : Fact Sheet." *NCWIT*. Web. 05 Apr. 2012. <http://www.ncwit.org/about.factsheet.html>.

Norton. "What Is Cybercrime?" *Cybercrime*. Symantec. Web. 03 Apr. 2012. <http://us.norton.com/cybercrime/definition.jsp>.

PwC. 2011 Global Economic Crime Survey. Pricewaterhouse Coopers International, Nov. 2011. Web. 01 Dec. 2011 <http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf>

Rogers, Marc. "The Role of Criminal Profiling in the Computer Forensic Process." *Tech.purdue.edu*. Purdue Univesity, 2003. Web. 6 Apr. 2012. <http://www2.tech.purdue.edu/cit/Courses/cit556/readings/Profile-Rogers.pdf>.

Rustad, Michael L. "Private Enforcement of Cybercrime on the Electronic Frontier." *Bcf.usc.edu*. Southern California Interdisciplianary Law Journal, 2001. Web. 7 Apr. 2012. <http://www-bcf.usc.edu/~idjlaw/PDF/11-1/11-1%20Rustad.pdf>.

Shinder, Deb. "Profiling and Categorizing Cybercriminals." *TechRepublic*. CBS Interactive, 19 July 2010. Web. 03 Apr. 2012. <http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069>.

Sjoholm, Hans. "Hacker." *What Is a Hacker?* SearchSecurity, June 1997. Web. 03 Apr. 2012. <http://searchsecurity.techtarget.com/definition/hacker>.

Steffensmeier, Darrell, and Emilie Allan. "Gender and Crime: Toward a Gendered Theory of Female Offending." *Annual Review of Sociology* 22.1 (1996): 459-87. Print.

Steffensmeier, Darrell, and Emilie Allan. "Gender, Age, and Crime." *Handbook of Contemporary Criminology*. Ed. Joseph Sheley. New York: Wadsworth, 1995. 86-126. Print.

Steffensmeier, Darrell, Jennifer Schwartz, and Michael Roche. Forthcoming. “Gender and 21st Century Corporate Crime: Female Involvement and Gender Gap in Enron-Era Conspiracies” *American Sociological Review*. Forthcoming. 2012.

Symantec. "Symantec 2011 State of Security Survey." *Symantec*. Symantec Corporation, 2011. Web. <http://www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf>.

Verizon. "2011 Data Breach Investigation Report." Verizon Risk Team, 2011. Web. 5 Oct. 2011. <htpt://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>.

Appendix A – Analysis of Female Cybercriminals by Conduct

Female Analysis		**Conduct**													
		Cyber Fraud		**Extortion**		**Cyber Theft**		**Cyber Threats**		**Cyber Stalking**		**Denial of Service**		**Other**	
Number/Pct. of Female Defendants		**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Network	**Solo**	0	0	0	0	1	7	1	7	0	0	0	0	1	7
	Multiple Co-conspirators	3	20	0	0	9	27	0	0	0	0	0	0	0	0

Female Analysis		**Conduct**													
		Cyber Fraud		**Extortion**		**Cyber Theft**		**Cyber Threats**		**Cyber Stalking**		**Denial of Service**		**Other**	
Number/Pct. of Defendants		**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Seriousness of Crime	**High**	3	20	0	0	5	33	0	0	0	0	0	0	0	0
	Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Low	0	0	0	0	5	33	1	7	0	0	0	0	1	7

Female Analysis		**Conduct**													
		Cyber Fraud		**Extortion**		**Cyber Theft**		**Cyber Threats**		**Cyber Stalking**		**Denial of Service**		**Other**	
Number/Pct. of Defendants		**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Complexity of Scheme	**Complex**	3	20	0	0	1	7	0	0	0	0	0	0	0	0
	In-between	0	0	0	0	0	0	1	7	0	0	0	0	0	0
	Simple	0	0	0	0	9	60	0	0	0	0	0	0	1	7

Female Analysis		**Conduct**													
		Cyber Fraud		**Extortion**		**Cyber Theft**		**Cyber Threats**		**Cyber Stalking**		**Denial of Service**		**Other**	
Number/Pct. of Defendants		**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Role in Scheme	**Ring Leader**	0	0	0	0	1	7	1	7	0	0	0	0	1	7
	Co-conspirator	2	13	0	0	8	53	0	0	0	0	0	0	0	0
	Accomplice	1	7	0	0	1	7	0	0	0	0	0	0	0	0

Appendix B – Analysis of Female Cybercriminals by Scheme

Female Analysis		Complexity of Scheme					
		Complex		In-between		Simple	
Number/Pct. of Defendants		n	%	n	%	n	%
Role in Scheme	Ring Leader	0	0	1	7	2	13
	Co-conspirator	2	13	0	0	8	53
	Accomplice	2	13	0	0	0	0

Female Analysis		Seriousness of Crime					
		High		Medium		Low	
Number/Pct. of Defendants		n	%	n	%	n	%
Role in Scheme	Ring Leader	1	7	0	0	2	13
	Co-conspirator	5	33	0	0	5	33
	Accomplice	2	13	0	0	0	0

Female Analysis		Complexity of Scheme					
		Complex		In-between		Simple	
Number/Pct. of Defendants		n	%	n	%	n	%
Network	Solo	0	0	1	7	2	13
	Multiple Co-Conspirators	4	27	0	0	8	53

Female Analysis		Seriousness of Crime					
		High		Medium		Low	
Number/Pct. of Defendants		n	%	n	%	n	%
Network	Solo	1	7	0	0	2	13
	Multiple Co-Conspirators	7	47	0	0	5	33

Appendix C – Analysis of Female Cybercriminals by Victim

Female Analysis		**Victim**															
		Individual		**Business**		**Previous Employer**		**Financial Institution**		**Educational Institution**		**Church**		**Government**		**Other**	
Number/Pct. of Defendants		**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Motive	**Financial Gain**	0	0	3	20	1	7	4	27	0	0	0	0	0	0	0	0
	Revenge	2	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Political/ Special Interest	5	33	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Recognition	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Special Interest	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Academic Vita of Corey J. Lee

Professional Profile

Energetic, detail-oriented student with an interest and strong background in the field of information security. Effective communicator with substantial leadership experience. Active learner with the ability to solve complex problems. In-depth knowledge of the field of technology. Global citizen with cross-cultural experience and excellent team building skills. Areas of strength include:

- Risk Assessment
- Information Security
- Security Management
- Geospatial Intelligence
- Biometrics
- Cyber Forensics
- PHP
- C ++
- MYSQL
- Documentation/Writing
- Project Management
- Problem Solving/Critical Thinking

Educational History

Pennsylvania State University – University Park, PA   August 2007 – December 2011
Candidate for Bachelor of Science in Security and Risk Analysis   *Expected Graduation: December 2011*
Concentration on Intelligence and Analytical Modeling
Minor: International Studies
Thesis: Cybercrime: Analysis of Offending Patterns and Offender Characteristics
Study Abroad: Beijing, China and Buenos Aires, Argentina

Employment History

Booz Allen Hamilton, Mclean, VA   **Summer 2011**
Cyber Cohort Intern

1. Built new intellectual capital for the firm around the emerging field of behavioral biometrics
2. Developed a proof of concept for a behavioral biometric system using new biometric classes
3. Assisted in the creation of a functional prototype to test the effectiveness of the biometric system

Ernst & Young, Mclean, VA   **Summer 2010**
IT Risk Assurance Intern

- Tested IT general controls for clients to evaluate SOX compliance and operational effectiveness
- Conducted client meetings to address configuration management risks within all processes
- Analyzed client risks related to segregation of duties, user access appropriateness, and logical access.

W3-Empowering the Net, Buenos Aires, Argentina   **Spring 2010**
Business Intern

4. Created proposals for existing clients preparing to enter the emerging Latino teenager market
5. Researched social networking and its impacts on new generation Latinos(NGLs)
6. Evaluated web design of existing client websites for aesthetics and up to date material

National Geo-spatial Intelligence Agency, Washington D.C   **Summer 2009**
Cyber Analysis Branch Intern   **TS/SCI Clearance**

- Assessed the cyber infrastructure and capabilities of high interest areas around the globe
- Organized and conducted outreach meetings to assist in the development of the cyber branch
- Utilized GEOINT to geographically depict and analyze cyber facilities in areas of high interest

Activities

Black Male Leadership Symposium, *Public Liaison*	**2007-2009**
Global Ambassador	**2010-Present**
Information Assurance Club, *Inter-club Liaison*	**2009-Present**
Spanish Club, *Member*	**2008-2010**
Security and Risk Analysis *Club, Member*	**2008-2010**
Race Relations Project, *Coordinator*	**Fall 2009**
PNC Leadership Assessment Center, *Participant*	**Fall 2010**
Penn State Around The World, *Coordinator*	**Spring 2011**
Freddie Mac Externship, *Participant*	**Fall 2010**
IA Club iCTF Competition Team,	**Spring 2011**
Colorado Advantage PhD Preview Program, *Participant*	**Fall 2011**

Research

Gender bias in Terrorism - " The amount of women involved in terrorism"	**Spring 2008**
Gender bias in White Collar Crime – " The role of women in white collar crime"	**Fall 2008**
Gender bias in Hate Crimes - " The amount of women involved in hate crimes"	**Spring 2009**
Gender bias in Cyber-Crimes - " The involvement of women in cybercrime"	**Fall 2010**
Maps Project – IPhone mobile incident reporting application for emergencies	**Spring 2011**

Certifications

CEH – Certified Ethical Hacker	**Summer 2011**
Security +	**Summer 2011**
ECSA – EC-council Certified Security Analyst	**Summer 2011**

Honors/Awards

Bunton Waller Fellowship	**Fall 2007**
Dell Scholarship	**Fall 2007**
IST Academic Scholarship	**Fall 2009**
IES Abroad Merit Scholarship	**Spring 2010**
USA Today All-USA Academic Team Nominee	**Spring 2011**
Schreyer Honors College Merit Scholarship	**Fall 2011**

Affiliations

Schreyer Honors Scholar, Member	**Fall 2009-Present**
Gamma Tau Phi IST Honor Society, Member	**Fall 2011-Present**
Strategic and Global Security Program, Member	**Fall 2011-Present**
Golden Key International Honor Society, Member	**Fall 2010 -Present**

Presentations

The Importance of Accountability and Integrity	**Fall 2008**
Behavioral Biometrics and the Insider Threat	**Summer 2011**
The Value of a Study Abroad Experience	**Fall 2011**