EXPLOITING THE DIGITAL FRONTIER:

HACKER TYPOLOGY

AND MOTIVATION

by

JOHN MCBRAYER

KATHRYN SEIGFRIED-SPELLAR, COMMITTEE CHAIR
MARK M. LANIER
CLAY POSEY

A THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science
in the Department of Criminal Justice
in the Graduate School of
The University of Alabama

TUSCALOOSA, ALABAMA

2014

ABSTRACT

The current study combined the hacker taxonomies presented by Loper (2000), Parker (1998), Rege-Patwardhan (2009), and Rogers (1999; 2006; personal communication) and proposed a simplified taxonomy which included: script kiddie, cyberpunk, password cracker, internal, and old guard hacker categories. Each category was identified by its characteristic computer deviant behaviors and analyzed against sex and seven motivational factors (i.e., addiction, curiosity, excitement/entertainment, money, power/status/ego, peer recognition, ideological, and revenge). The study had two specific aims: (1) to explore which motivations were associated with each specific computer deviant behavior, and (2) to determine if more males than females are engaging in computer deviant behavior. The study targeted computer deviants from specific websites, which discussed or promoted computer deviant behavior (e.g., hacking). Using a snowball sampling method, 120 subjects completed an anonymous, self-report questionnaire that included items measuring computer deviance, motivational factors, and demographics. Relationships were identified using zero-order correlation, then a backwards (Wald) binary logistic regression was conducted to determine the predictive ability of motivational factors on the different categories of computer deviancy.

None of the computer deviant behavior specific hypotheses were fully supported. The expectation that more males would be computer deviants than females was not fully supported since males were more likely to be script kiddies, cyberpunks, and old guard hackers compared to females. The findings suggested that these computer deviant behaviors overlapped in both motivational factors and the behaviors themselves. The study found that script kiddie, password

cracker, and old guard hacker behaviors were all only motivated by addiction. Cyberpunk behavior was found to be motivated by financial, peer recognition, and revenge motivations, and internal computer deviant behavior was found to be related to financial and peer recognition motivations. Overall, the current study suggested that there was significant motivational and behavioral overlap between computer deviant categories, and not all computer deviants were predominately male. The author concluded that using a strict computer hacker taxonomy may not accurately reflect the true nature of computer deviant behavior.

DEDICATION

This thesis is dedicated to Whitney Johnson, who always stood by me and pushed me forward.

LIST OF ABBREVIATIONS AND SYMBOLS

α	Chronbach's index of internal consistency.
DoS	Denial of Service attack. An attack designed to make a website, server, computer, or network unavailable to its intended users.
DDoS	Distributed Denial of Service Attack. A DoS attacked carried out simultaneously by a multitude of computers at once.
DNS	Domain Name System. The internet structure that translates domain names, such as google.com, into internet protocol (IP) addresses computers use to connect.
p	P-value. A value associated with the testing of a null hypothesis measuring the probability of obtaining a test statistic as extreme as or more extreme than the observed value.
r_ϕ	Pearson binary correlation.
R_L^2	Hosmer and Lemeshow pseudo-R^2, used for measuring goodness of fit in logistic regression.
R_C^2	Cox and Snell pseudo-R^2, used for measuring goodness of fit in logistic regression.
R_N^2	Nagelkerke pseudo-R^2, used for measuring goodness of fit in logistic regression.
Wald	Computed value of Wald Statistic for logistic regression.
<	Less than
>	Greater than
=	Equal to

ACKNOWLEDGMENTS

I am pleased to have the opportunity to thank all of those who have helped me throughout my work on this research project. I am most indebted to my committee chair Dr. Kathryn Seigfried-Spellar who kept me inline, helped me get back on track when I'd stumble, and motivated me to not give up. I also really appreciated all of the fireball candies I received during the course of working on this project. I would also like to thank my committee members Dr. Mark M. Lanier and Dr. Clay Posey. To Dr. Lanier, thank you for giving me constructive criticism and holding me to a high standard, for making time for me when I would show up unannounced at your office, and for reminding me of why I'm proud of being in the Department of Criminal Justice here at the University of Alabama. I would like to take the time to note that Dr. Lanier's motorcycle has also always been a source of inspiration. I hope one day to have a similar one, or a motorcycle at all, for myself. To Dr. Posey, I greatly appreciate that you allowed me to use the in-press article you collaborated on with A. J. Burns, T. L. Roberts, and R. Hightower. I am also thankful for your help in gaining attendance to the Southwest Decision Sciences Institute conferences in March of 2013, and for sharing my enthusiasm for statistics and math.

I'd lastly like to thank everyone who is close to me and who have been there for me over the last few months, specifically Whitney Johnson, for loving me even though I have no idea why you do. And of course my dogs, Che Che and Bilbo Waggins, for keeping me constantly entertained, and frustrated, throughout this whole endeavor.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

THE IMPORTANCE OF ADDRESSING CYBERCRIMINAL BEHAVIOR

The prevalence of cybercriminal activity has caused significant financial loss over the last three years (Internet Crime Complaint Center; IC3, 2011; IC3, 2013). In addition, the majority of victims of cybercrime were unaware of what to do after being victimized, if they were even aware they were victims, which often lead to victims not reporting their incidents to law enforcement (IC3, 2011; IC3, 2013; Richardson, 2011). The Internet Crime Complaint Center (IC3) functions as a data-loss database and provides victims of cybercrime a convenient reporting mechanism that alerts authorities to suspected criminal or civil violations (IC3, 2011). Each year the IC3 releases a comprehensive report of the year's overall cybercriminal activity. In 2011, the IC3 reported that the total number of cybercriminal complaints was 314,246 resulting in a total loss of $485,252,871. The average amount of money lost for each complaint was $1,544 (IC3, 2011). These numbers of complaints fell slightly in 2012, as the total number of cybercriminal complaints was 289,874; however, the financial loss increased to a total loss of $525,441,110, an increase of $40,188,239 (IC3, 2011; IC3, 2013). The average amount of money lost for each complaint also increased to $1,813, an increase of $269 (IC3, 2011; IC3, 2013). These financial losses, to both individuals and companies, suggest the severity of the cybercriminal issue.

The Computer Security Institute (CSI) releases a yearly computer crime and security survey that reports basic statistics related to cybercriminal behavior (Richardson, 2011). In the most recent CSI report of 351 security practitioners, focusing on the years 2010 / 2011, malware infections accounted for the majority or 67.1%, of attacks experienced by businesses (Richardson, 2011). The remaining attacks included: phishing (38.9%), laptop / mobile device theft (33.5%), bots on network (28.9%), insider abuse of net access or email (24.8%), password

sniffing (11.4%), financial fraud (8.7%), and exploit of wireless network (7.4%). Of these attacks, 57.6% resulted in a direct financial loss for the victim. In response to the attacks, the majority of victims would patch vulnerable software (62.3%) or hardware (49.3%) feeling that reporting the incidents to law enforcement was useless because they "did not believe law enforcement could help in the matter" (Richardson, 2011, p. 24). This mentality, coupled with the growing financial losses resulting from cybercrime victimization, suggested a need for updated and proactive policies designed to assist victims of cybercrime. The first step towards that result was to categorize and understand the different avenues of attack used by hackers, and the motivations associated with specific hacker tactics.

One of the greatest hurdles for researchers is determining a definition of hacker that is agreed upon (Rogers, 1999). The Oxford English Dictionary (2013) currently defines a hacker as a person with an enthusiasm for programming or using computers as an end in itself, and as a person who uses his skill with computers to try to gain unauthorized access to computer files or networks. Colloquially, the term hacker has swelled to encompass many types of behavior as, "popular media has co-opted the term hacker and used it to refer to any type of computer crime" (Wade et al., 2011, p. 31). The behavior of hackers is directly tied to the technology they use. "The exponential expansion of computer technologies and the Internet have spawned a variety of new criminal behaviors and provided criminals with a new environment within which to operate" (Maras, 2012, p. 1). These criminal activities fall under the realm of cybercrime. Maras (2012) defined cybercrime as simply the use of the Internet, computers, or related technologies to commit crime. Not only had computers offered would be criminals a new means of committing crimes, but they had also provided these potential offenders with powerful tools to facilitate their

other illegal pursuits. Maras (2012) suggested then that cybercriminal activity can be broken into two main categories, computer as a tool and computer targeted crimes.

The first category included all criminal activities in which the computer was used as a tool to help the offender commit a crime, such as when a computer is used to download copyrighted software. The remainder of this paper will focus on the second category that included all criminal activity that targeted a computer, computer system, computer network, or digitally stored information of individuals, organizations, or governments (Maras, 2012). An example of this kind of behavior would be if a criminal wanted to disrupt the business of a legitimate website by crashing it. To do this, an offender might use a denial of service (DoS) attack designed to crash the website's servers making the website inaccessible to potential patrons. In this scenario the website's computer networks or servers were the target.

Academic scholars have proposed that readdressing the definition of the word hacker could alleviate some of the legislative or legal issues surrounding cybercriminal law enforcement (Loper, 2000; Maras, 2012; Rogers, 1999; Sample & Swetnam, 2012). By breaking down cybercriminal activity into categories, and categorizing the behaviors of offenders caught during these activities, law enforcement resources could be delegated according to the severity or immediacy of the need in apprehending the offender. For example, if one hacker was participating in cyberbullying and another was using a program to steal funds, law enforcement could have a standard operating procedure to follow in pursuit of these offenders. This procedure could allow police to reallocate resources in the most efficient way to prioritize capturing one offender over another, or punishing one offender with more severity. This type of decision-making process is one that cyber security professionals try to make on a daily basis (Maras, 2012; Sample & Swetnam, 2012; Wade et al., 2011).

Several studies have tried to categorize what hacking is by defining subgroups within the hacker community (Holt & Kilger, 2008; Jordan & Taylor, 2004; Loper, 2000; Mann & Sutton, 1998, Rogers 1999; Rogers 2006; Turgeman-Goldschmidt, 2005). The first step in defining groups is to separate the behavior from the hacker label. Computer deviant behaviors were easier to distinguish, and offered researchers a way to separate hacking into specific behaviors (Rogers, 1999; 2006). These studies have established differential characteristics based on motivation, methodology, tactics, and skill level used by hackers to deviate from standard protocol. Motivation is unique in that it has not only been used to define computer deviant behavior categories, such as hacktivists, but also to differentiate other categories (Jordan & Taylor, 2004; Loper, 2000; Mannsfield-Devine, 2011; Murphy, 2011; Schell & Dodge, 2002). Both the computer deviant behavior taxonomy and motivations proposed are based on years of changing definitions of computer deviant behavior, and what motivates individuals to participate in these behaviors. The taxonomy in this study included a novel combination of computer deviant behavior categories, compared with motivations suggested by prior literature. The following chapter will be broken into two subsections: the evolution of the hacker, and computer deviant behavior motivations. The first section chronologically follows the development of the term hacker and how it has been categorized and conceptualized over time. The second section focuses on the dynamic changes in the way the motivations perceived to influence computer deviant behavior have adapted over time.

CHAPTER 2

LITERATURE REVIEW

EVOLUTION OF THE HACKER

The Oxford English Dictionary first recognized the term hacker in 1976 in two different manuscripts. In Weizenbaum's *Computer Power & Human Reason*, the hacker was a compulsive programmer and was usually a skilled technician (Oxford English Dictionary, 2013). In Jonas's *Crime by Computer*, the hacker was an architect of a brilliant Trojan horse attack that was orchestrated through the manipulation of data on magnetic tapes (Oxford English Dictionary, 2013). Since the term first appeared alongside the beginning development of modern computer technology, it has grown to include many types of methodologies and behaviors.

In 1988, Hollinger and Lanza-Kaduce offer an early examination of the developing law surround computer crime. Within a decade of the first laws against computer crime being passed in Florida and Arizona in 1978, 47 states had enacted computer crime legislation by 1988 (Hollinger & Lanza-Kaduce, 1988). The laws regulating computer crime were passed without direct support or opposition from the public. The media had the most direct involvement in the legislative process. For example, Donn Parker gathered newspaper clippings reporting computer abuse from the years 1976 to 1983. What he published, after nearly a decade of work, was merely the tip of the iceberg as Parker noted that the growth in his files appeared to be rapid and exponential (Hollinger & Lanza-Kaduce, 1988). The movie *War Games* (1983) also led to prolific media portrayal of vulnerable private and public computer installations with hackers often represented as juvenile and intelligent. During this period, the criminalization of hacking

was finally spreading across the country, and it was the media that portrayed hackers as young, intelligent, and dangerous (Hollinger & Lanza-Kaduce, 1988).

A decade later, the Internet had expanded into the daily lives of individuals. Mann and Sutton (1998), while researching online newsgroups, coined the terms NetCrime and NetOffenders to describe what they saw as a growing problem for neutral members of the net. NetCrime was defined as "any criminal offense committed via the Internet," while NetOffenders were "those who initiate such crimes, or take up criminal opportunities on the Net" (Mann & Sutton, 1998, p. 202). These terms were meant to provide official labels to the hackers and phreakers presented by Meyer in his 1989 investigation into members of underground computer networks. Mann and Sutton (1998) made a distinction between what they called old style hackers and new hackers. Here they suggest old style hackers became involved in computer intrusion for the challenge, whereas new hackers were attracted due to the financial rewards. These old style hackers were the predecessors of the current old guard hacker category (Mann & Sutton, 1998; Rogers, 1999). Mann and Sutton (1998) predicted that if the growth of hackers remained unchecked, law and law enforcement agencies would be ill-prepared to meet this challenge.

In the same year, Parker published a detailed account of the growth of cybercrime up to that time. In it, Parker (1998) described hackers as characterized by an immature excessively idealistic attitude. Regardless of age, he argued that hackers acted like irresponsible kids playing cops and robbers in a fantasy world that could suddenly turn real when they were caught (Parker, 1998). Parker noted that at the time most hackers gained their information through social engineering, or the use of people to gain access to unwarranted authorization. He then proposed seven types of cybercriminals: pranksters, hackers, malicious hackers, personal problem solvers, career criminals, extreme advocates, and lastly malcontents, addicts, and irrational and

incompetent people (Parker, 1998). Pranksters were the individuals who perpetrated tricks on others, but did not generally intend long-lasting harm (Parker, 1998). Parker's (1998) hacker category is not specific, and included any person who attempted to gain unauthorized access to a computer or system. Malicious hackers, which were sometimes called crackers, were intent on causing loss and damage to their victims. Personal problem solvers were individuals who were pursuing a solution to a personal problem through any means necessary regardless of the legality of the method they employed. Career criminal hackers were those which earned part or all of their income from crime. Extreme advocates were politically, socially, or religiously motivated groups which used violence against people or property to achieve their goals. Parker's (1998) last hacker category was the malcontents, addicts, and irrational and incompetent people. This group included mentally ill, those with substance addictions, or the criminally negligent, and this was the least predictable group. Through this categorization, Parker initially broke down the broad term of hacker into specific categories based on hacker's methods, tactics, skill level, or motivation. This type of taxonomical approach is again proposed the following year.

In 1999, Rogers argued the lack of an agreed upon definition of what the term hacker means has been and would be a hurdle for researchers attempting to study individuals involved in hacking activities (Rogers, 1999). Rogers (1999) argued that hackers are not a homogeneous group and proposed a new taxonomy, citing the work of Parker and others in his studies. In his proposed taxonomy Rogers (1999) defined the following hacker categories: newbie/tool kit (NT), cyber-punks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC), and cyber-terrorists (CT).

Newbie/tool kit (NT) hackers were those with limited skill and often included new hackers (Rogers, 1999). Cyber-punks (CP) were hackers with some technical knowledge, who

intentionally meant to harm their targets. This category was based on Parker's (1998) malicious hacker category. Internals (IT) were disgruntled employees who used their authorized access to computer systems often to damage the companies they felt had treated them unfairly. Old guard hackers (OG) appeared to embrace the first generation of hackers and were primarily interested in intellectual endeavors with little criminal intent. Rogers (1999) argued professional criminal hackers (PC) and cyberterrorists (CT) are the most dangerous groups of hackers as they were well trained and knowledgeable in their attacks. Unlike previous categorizations, Rogers (1999) proposed a taxonomy in which the categories exist on a continuum of technical ability from lowest (NT) to highest (OG-CT). Similar to other literature, he also warned that hacking will continue to flourish if not addressed by the security industry, law enforcement, and governments (Rogers, 1999).

The next year, Loper released his multi-part dissertation on the criminology of computer hackers. In his work, Loper (2000) immediately addressed the lack of an agreed upon definition of a hacker. He then proposed a new typology of hackers using a triangulation procedure in which names for each category were names used by hacker communities. In his proposed taxonomy, Loper (2000) defined the following hacker categories: old school hackers, bedroom hackers, larval hackers and newbies, WaRez D00dz, Internet hackers, hacktivists, script kiddies.

Loper (2000) categorized old school hackers similarly to Rogers (1999) focusing on a group of hackers which was motivated by curiosity, and the law was disregarded instead of intentionally broken. Bedroom hackers were those which hacked from home and often had limited resources and relied on the hacker subculture for more resources (Loper, 2000). Loper (2000) also defined larval hackers and newbies the same way Rogers (1999) defined his NT category: these were the new hackers who were just beginning to learn hacking techniques.

WaRez D00dz were the pirates who intentionally disregard software copyright laws, often arguing that information should be free (Loper, 2000). Internet hackers were categorized as a broad group containing all hackers which do not fit in other categories, and were only distinguished from bedroom hackers by the sense of community they received from the hacking subculture (Loper, 2000). Loper (2000) defined hacktivists as the politically, socially, or religiously motivated hackers, similar to Roger's (1999) cyber-terrorists and Parker's (1998) extreme advocates. Script kiddies were the final group Loper (2000) defined. This group was similar to the larval or newbie hackers, but they showed no interest in advancing their technical knowledge. Through his categorization, Loper (2000) distinguished hackers based on their resources, skill, and enculturation within the hacker subculture he proposed existed on the net. This typology was also unique in that it used categorical labels based on hacker jargon. Loper (2000) also recognized that hackers distinguish themselves from computer criminals, and were insulted by the label.

Looking at the relationship between hacking and democracy, Kirsty Best (2003) focused on the hacking ethics present within the hacker subculture. Best (2003) used the distinction within the hacker community of a difference between malicious and benevolent hackers. The latter group was labeled simply hackers, or whitehat hackers, whereas the malicious group was labeled as crackers, or blackhat hackers (Best, 2003). Best (2003) draws the distinction instead between what she defined as the old school and new school hackers. She suggested that old school hackers are typically the whitehat hackers, motivated by curiosity or challenge, have a commitment to open source code, and a distrust of Microsoft. Alternatively, new school hackers are the blackhat hackers, motivated by greed or political stance and challenge the current state of the Internet (Best, 2003).

Schell and Martin (2004) continued to expand upon the now recurrent theme of dividing computer deviant behaviors into the white hat and black hat categories. They also detailed multiple types of cybercrimes and described a wide variety of methods of attack. Schell and Martin (2004) then argued that the intentions of hackers can be separated from their methods. They further argued that hackers can be categorized based on which computer deviant behaviors they employed, regardless of whether they were whitehat or blackhat hackers (Schell & Martin, 2004).

Rogers revised his originally proposed taxonomy from 1999 and published a new report which focused on a new multi-dimensional model. In this new report, Rogers (2006, p. 98) suggested there were nine hacker categories which included: Novice (NV), Cyber-punks (CP), Internals (IN), Petty Thieves (PT), Virus Writers (VW), Old Guard hackers (OG), Professional Criminals (PC), Information Warriors (IW), Political Activists (PA).

The Novice (NV) category included those persons who had limited computer and programming skills (Rogers, 2006). This was a revamp of the previous Newbie/Tool kit category from Rogers (1999). Cyber-punks (CP) remained the same as his previous categorization from 1999, and included the hackers with moderate skills who used them maliciously. Internals (IN) also remained the same and represented disgruntled employees who sought revenge against the organization in which they were employed (Rogers, 2006). Petty Thieves (PT) were the individuals which used hacking as a means of financial gain through theft. The old guard hackers remained the same to Rogers (1999) previous taxonomy and included hackers which were primarily motivated by curiosity and exploration instead of criminal enterprise. The virus writer (VW) group was one Rogers (2006) had a difficult time categorizing. He suggested it was a place holder for future research and not a clearly defined group. The professional criminals (PC)

group had remained the same from Rogers (1999) previous taxonomy, and included hackers which were highly skill and utilized hacking as a means of furthering their criminal enterprise. The Information Warrior (IW) category included hackers which were trained to conduct or defend against attacks which were designed to destabilize, disrupt, or affect the integrity of data or information systems that command and control decisions were based upon (Rogers, 2006). This group was similar to Rogers (1999) prior categorization of cyber-terrorists. The political activist (PA) hacker category included the other component of the original cyber-terrorist category, which was the politically, socially, and religiously motivated hackers (Rogers, 1999; Rogers, 2006).

Rogers (2006) argued this new taxonomy followed a continuum, similar to his previous taxonomy, from the lowest technical skill to the highest, and functioned as the foundation for the development of a hacker taxonomy based on the principal components of skill level and motivation (Rogers, 2006). This taxonomy was further strengthened with a motivational component in which he chose four common motivations and correlated them to each of his hacker categories (Rogers, 2006). This was one of the earliest studies that removed motivation from the hacker category criteria and instead used it as a second dimension to strengthen the taxonomy (Rogers, 2006).

Focusing on a growth of cyber terrorism in their home countries, The Council of Europe (2007) released a collaborative work which detailed the use of cyberterrorism on the Internet. In their report, they noted that cyberterrorism was loosely defined, and ranged from use of the Internet by terrorists to real criminal cases involving either virtual or physical losses. Specifically focused on attacks made through the internet, the Council of Europe (2007) noted two types of attacks: attacks on infrastructure and attacks on human life. Attacks on infrastructure were aimed

to render systems useless and could come in many forms including large-scale denial of service (DoS) attacks, hacking attacks that exploited a weakness, a hybrid attack that may incorporate physical and technological components, or attacks that resulted in physical damage, such as a DoS attack aimed to disrupt power plants or dams (Council of Europe, 2007). The second type of attack focused on attacking human life. This type of cyberterrorist attack the Council of Europe (2007) hypothesized could occur through two different methods: A sudden catastrophe, such as hacking into a railway or flight control system to cause crashes, or a long-term development, such as hacking into machinery used to produce food or medicine and manipulating the procedure. The Council of Europe (2007) went on to list legal ramifications and statistical reports for all European countries specifically related to cyberterrorist attacks, and provided an extensive detailing of the methodology of cyberterrorism.

By 2008, hacking and hackers had been divided into multiple categories, whether it be by skill level, motivation, white vs. black hat, or old vs. new school. Holt and Kilger (2008) provided a new distinction through a presentation which focused on the differential use of technology across the hacker culture. They suggested that hackers can be broken into two groups: makecrafters and techcrafters (Holt & Kilger, 2008). The makecrafters were defined by Holt and Kilger (2008) as the producer of new scripts, tools, and products, which could be malicious, benign, or even beneficial. Alternatively, the techcrafters were the hackers who used the products created by the makecrafters. Holt and Kilger (2008) argued that this value-neutral system allowed for better understanding of the methods and tactics of a hacker by removing the black, white, or gray hat ethical connotation.

Examining a wide variety of terms related to cybercriminality, McQuade (2009) described the varying definitions associated with the word, ranging from the original benign use

in the 1970s to the then current trend of hackers that appeared to associate with a unique hacker culture. McQuade (2009) went on and discussed the annual DEFCON convention in Las Vegas, Nevada that thousands of people generally interested in the hacker subculture attend. These events blended the criminal and noncriminal sides of hacking into an amorphous topic that is shared amongst those in attendance.

Rege-Patwardhan (2009) explored the types of hacking methods used to attack critical infrastructure, and in doing so proposed a hacker typology based on cybercriminal cases. He noted that hackers typically perform solo operations, working as loners. He found that these loners varied with respect to their technical skills and motivations (Rege-Patwardhan, 2009). Building off the work of Rogers (2006) and Loper (2000), Rege-Patwardhan (2009) proposed that hackers can be categorized as novices, which included script kiddies, insiders, and professionals. Novices were defined similarly to Rogers (2006) as the new hackers who relied on pre-written toolkits to conduct their crimes. This group also included script kiddies (Rege-Patwardhan, 2009). Insiders were also defined similarly to Rogers (1999; 2006) as the disgruntled employees who sought to use their access and expertise to enact revenge. Rege-Patwardhan (2009) categorized professionals as the hackers which had a high degree of technical skill and expertise, and offered their services for a price. This category was also similar to Rogers (2006) Professional Criminal category. Rege-Patwardhan (2009) also proposed that a category of associates can be applied to hackers who collaborated and worked in groups. The majority of the attacks on critical infrastructure came from rootkits, a tool that allowed hackers to gain administrative access to computer systems (Rege-Patwardhan, 2009). These differed from employing a toolkit, which was a pre-written malware attack that could be used without extensive technical knowledge (Rege-Patwardhan, 2009).

Public acknowledgement of hacker groups had now changed the perception as to which characteristics were associated with hackers (Mansfield-Devine, 2011; Murphy, 2011; Nowak, 2011). Hacker groups like Anonymous often employed distributed denial of service (DDoS) on targets that differed from their political ideology using pre-written scripted programs such as the Low Orbit Ion Cannon (LOIC; Mansfield-Devine, 2011; Murphy, 2011), or launch raids on financial institutions, such as Bank of America© or PayPal©, where they break into private accounts and publish personal information online (Murphy, 2011). These behaviors placed Anonymous hackers into several of the computer deviant behavior categories at the time including: black hat, hacktivist, script kiddie/newbie, and techcrafter categories (Wade et al., 2011).

Since 2012, multiple academic articles have been published which focused on specific facets of the hacking phenomenon. Hatamleh (2012) focused on describing all hacking techniques that utilized the Domain Name System (DNS) method of attack. His work described in detail nine potential avenues of attack on vulnerable systems. The first technique he discussed is the DoS attack (Hatamleh, 2012). The DoS attack was one of the most common attacks that sought to prevent or delay access to information (Hatamleh, 2012). The most common method of performing a DoS attack involved manipulating the data packets exchanged between a server and computers connected to it. The attacker flooded the server with an excessive number of data packets in the hopes of slowing down its processing speed (Hatamleh, 2012).

The second technique commonly employed by hackers involved stealing, or cracking, passwords using specific programs designed to either monitor keystrokes, to steal the passwords, or to randomly generate passwords and crack them (Hatamleh, 2012). The third technique focused on using Trojan horse programs to infiltrate a computer or network to gain unauthorized

access. Trojan horses were often included in what would appear to be benign software. The programs, once run, can be used to destroy hard drives, corrupt files, record keystrokes, monitor network traffic, track Web usage, duplicate e-mails, allow remote control, and more (Hatamleh, 2012).

The fourth hacking technique Hatamleh (2012) discussed was the exploitation of defaults. Network administrators who do not change many of the default settings on their software or hardware Hatamleh (2012) argued make themselves more vulnerable to attacks. Man-in-the-middle attacks were the fifth hacking technique discussed in which attackers fool users into connecting, or giving information, to a rogue entity and not the proper resource. An example of this type of attack was the use of a phishing script injected into a logon page. An unsuspecting user would simply log into their account, and the information would be sent to both the legitimate server and a rogue third party. The user would then access the site and would likely not even know an attack had occurred (Hatamleh, 2012).

The sixth technique Hatamleh (2012) addressed were wireless network attacks. Hatamleh (2012) simply suggested that the use of insecure, often free, wireless Internet access increased the ease with which attackers could perform their attacks while maintaining their anonymity. Hatamleh (2012) went on and discussed hackers who monitored their targets before attacking. This type of pre-emptive detective work included researching an organization, learning its network security protocols and vulnerabilities, and even implementing social engineering to manipulate the employees, or those associated with their target, to expose any weaknesses (Hatamleh, 2012).

The last hacker technique addressed by Hatamleh (2012) is the threat posed by what Rogers (1999; 2006) would call internals. These hackers worked within the organization they

targeted. This position granted them a level of authority and network access that would be significantly harder to obtain for an external attacker (Hatamleh, 2012). This caused these types of hackers to be significantly more dangerous than any other type. Hatamleh (2012) offered several suggestions to help combat this type of attacker, including keystroke monitoring, not allowing external or removable hardware, disabling usb ports, extensive auditing, Internet filtering and monitoring, and tighter enforcement of the principle of least privilege to help curtail the possibility of this type of attack (Hatamleh, 2012). All of these methods can further be attributed to the shifting social value evident in the hacking culture.

Nikitina (2012) argued that hacking is a social phenomenon directly related to the current social environment. The work of hackers can be interpreted as creative outputs for youth within the current evolving digital culture (Nikitina, 2012). The techniques presented by Hatamleh (2012) operated as social contributions and helped shape our current paradigm on how hackers interact with society. Nikitina (2012) went on and argued that hackers were tricksters who desired to subvert established hierarchies. Nikitina (2012) supported this assertion by examining how hacker fit within four motifs associated with tricksters: duplicity, boundary crossing, subversion of power, and creativity and craftsmanship. Though Nikitina (2012) ultimately decided that the lack of originality and follow-through of hackers excludes them from a true trickster role, her study on the motives of hackers offered a thorough sociological perspective.

Also in 2012, Kim, Wang, & Ullrich focus on worldwide legal issues pertaining to regulating cybercriminal activity. They suggested that a treaty or set of treaties at the United Nations level on cyber security and cybercrime should be a global proposal for the 2010s that was based on a potential for consensus. Purkait (2012) provided a thorough literature review of the development and countermeasure designed related to phishing. He suggested that educating

users about the threat of phishing, combined with implementation of proper anti-phishing measures were necessary to reduce the victimization of this type of hacking. Richmond (2012) discussed the threat of cyberterrorism through an analysis of the stuxnet worm that was used to attack the Iranian nuclear facilities in 2010. Richmond (2012) proposed that cyber war can fall under the regulatory clauses of the Law of Armed Conflict through distinction, discrimination, and proportionality. Sample and Swetnam (2012) amalgamated several academic and professional articles citing the legal and jurisdictional issues surrounding cybercriminal legislation. The goal was to pursue some type of legislative efforts to curtail the exponential expansion of cybercrime, the proceeds of which had surpassed that of the drug trade -- with a lot less risk for its practitioners (Sample & Swetnam, 2012). As shown in Table 1, many of these categories overlap with the current categories being analyzed in the current study.

COMPUTER DEVIANT BEHAVIOR MOTIVATIONS

In 1999, Taylor proposed both macro and micro level theories on why individuals hack. At the macro level, Taylor (1999) suggested that a hacker subculture existed which operated off a belief in the free exchange of information. This culture had several specific elements including a direct relationship to technology, secrecy, disembodied anonymity, and youth. At the individual level, Taylor (1999) discussed several motivation factors he suggested explained why individuals turn to hacking. These factors included addiction, curiosity, boredom, power, peer recognition, and political acts. Each was directly related to a propensity to pursue hacking behavior (Taylor, 1999). Peer recognition specifically related back to the proposed hacker subculture, in which an individual would seek the admiration of his or her hacker peers.

Employing a psychological perspective, Beveren (2001) proposed a conceptual model to explain motivations towards hacking behavior based out of psychological theories. Beveren (2001) applied flow theory in an attempt to explain hacking behavior. Flow theory attempted to

explain the effortless action felt when being highly involved in an activity to the degree that attention became ordered, fully invested, and time was obscured by the involvement in the activity (Beveren, 2011). Flow theory contains four premises. The first premise required the user to perceive a sense of control over the computer interaction. The second premise required the user to perceive that his or her attention was focused on the interaction. The third premise required the user's curiosity to be aroused during the interaction. The final premise required the user to find the interaction intrinsically interesting (Beveren, 2001). Through the application of this theory, Beveren (2001) suggested that hackers would be drawn to the behavior and repeat it based on the positive feedback of finding the activity enjoyable.

Armitage and Roberts (2002) explored the cyber culture from the perspective of a battlespace. Depicted as a battlefield through which military action can occur, Armitage and Roberts (2002) argued that cyber wars will eventually be fought through cyberspace, and that individuals will have a greater impact on these types of battles. Also in 2002, Schell and Dodge discussed the psychological and social aspects of hackers as well as potential solutions to the black hat hacker problem. Psychologically, Schell and Dodge (2002) found that most hackers had traumatic childhoods, reported short-term stress and were poor stress managers, reported odd sleeping patterns, were multi-taskers, and had high creative potential. Socially, they found that hackers preferred anonymity, were self-taught, and preferred to work alone. Ultimately, Schell and Dodge (2002) suggested that aligning international legislation to the hacker paradigm of free information would likely lead to the greatest success in reducing black hat computer deviant behavior.

Applying an ethical theory and philosophical model Gordon and Ma (2003) attempted to explain the behavioral motivations behind hacking. They argued that moral obligation and social

norms would affect not only an attitude towards hacking, but hacking intention as well. Gordon and Ma (2003) found that one of the greatest predictors of a person's intent to hack was their self-efficacy, meaning their belief in their own ability, and further noted that what an individual believed influenced what he or she does. They suggested that identifying beliefs was the first step towards categorizing hackers.

Building directly from the work of Beveren (2001), Voiskounsky and Smyslova (2003) examined the flow model in comparison to a hacker's competence in information technology. In their initial testing, Voiskounsky and Smyslova (2003) also suggested that the hacker subculture was not homogeneous and contained many subgroups. Through their study of 457 self-reporting hackers, they found empirical support for the flow model as it applied to hacking; however, they found that the model was pervasive throughout all hacker levels of information technology competence (Voiskounsky & Smyslova, 2003).

It was during the 1990s that hacking first merged with a political stance (Jordan & Taylor, 2004). Jordan and Taylor (2004) dissected the concept of hacktivism, examined its history, context, and causes. They then split hacktivism into two broad streams of action: mass virtual direct actions, which used cyber spatial technologies of limited potential in order to re-embody virtual actions, and digitally correct actions, which defended and extended the peculiar powers cyberspace created (Jordan & Taylor, 2004). These two avenues both interacted and conflicted at times, and offered the hacktivist a variety of mediums through which political protests could be orchestrated. Each path allowed a politically motivated hacker the opportunity to express themselves in a new and innovative way (Jordan & Taylor, 2004).

Kilger, Arkin, and Stutzman (2004) applied a sociological analysis to the whitehat and blackhat community. Beyond recognizing the subculture, Kilger, Arkin, and Stutzman (2004)

utilized the U.S. Federal Bureau of Investigation's (FBI) counterintelligence unit's MICE (Money. Ideology. Compromise. Ego.) acronym and developed their six motivational categories of Money, Entertainment, Ego, Cause, and Entrance to social group, and Status. The appropriately labeled MEECES motivations were suggested to be associated with both whitehat and blackhat hackers (Kilger, Arkin, & Stutzman, 2004).

Some research focused on specific motivations, such as social entertainment. By interviewing hackers, Turgeman-Goldschmidt (2005) found that fun, thrill, excitement, intrinsic curiosity, computer virtuosity, and economic motivations were present within his sample. Some motivations he argued are an embodiment of Western culture, and the hacker subculture borrowed these social values to maintain its own value system. He further suggested that these motivational factors would vary based on the social structure of the primary culture in which the hacker resides (Turgeman-Goldschmidt, 2005). He went on to criticize Taylor's (1999) six motivational categories and stated that they did not describe what made the hacker continue hacking, nor what made the hacker enjoy hacking, even though it was illegal (Turgeman-Goldschmidt, 2005).

Exploring the influence of the Big-5 personality characteristics, moral decision making, and exploitive-manipulative amoral dishonesty characteristics towards computer deviant behavior, Rogers, Smoak, and Liu (2006) found that the crimes considered less egregious were reported as being more frequently committed, as there were likely less severe social and legal sanctions attached to them. A flexible ethical boundary and lower internalization of general social norms were also found to be associated with higher computer deviant scores (Rogers et al., 2006). Interestingly, the Rogers et al. (2006) noted that the hypothesis related to introversion was not supported by their results.

Some research suggested that hackers were not criminals. Taylor, Caeti, Loper, Fritsch, and Liederback (2006) argued that hackers were significantly different from computer criminals. To support their claim, Taylor et al. (2006) examined the motivations behind hackers and specifically associated hackers with the pro-social notions of the hacker subculture (Taylor et al., 2006). In this way, the hacker was ethical by self-defined standards, and was separated from the malicious hacker, known as a cracker (Taylor et al., 2006).

Further delving into the hacker subculture, Williams (2006 suggested it was futile to attempt to provide a general theory of cybercrime. Williams (2006) then incorporated a peer recognition pathway and explained the motivational force behind the hacking subculture. Williams (2006) argued that the peer relationship fellow hackers in the hacker community was weak, and resulted in a greater risk for hacking behavior (Williams, 2006). Holt (2007) further explored the influence of a deviant hacking subculture and its influence as a motivator for hacking; however, Holt provided a unique position by examining how the overlapping experiences between offline and online behavior influenced subcultural values and norms. Holt (2007) began by identifying three values consistently present in hacker subculture research: technology, secrecy, and mastery. Through his analysis, Holt (2007) suggested that the five normative orders, or motivational forces, of the computer hacker subculture were technology, knowledge, commitment, categorization, and law. The only lack of overlap was in the categorization, or labeling, of behavior between offline and online mediums. It was noted that there was little discussion on how to define hackers and what constituted a hack off-line (Holt, 2007).

Holt (2009) then focused on the attack dynamics of politically and religiously motivated hackers. In this analysis, Holt (2009) examined the Turkish hacker community, and found that

religiousness defined a mission for Turkish hackers to accomplish. These hackers then attacked targets they thought slighted either the Muslim community or Turkey specifically. This type of motivational force falls within a cause-driven, or political, motivation (Holt, 2009).

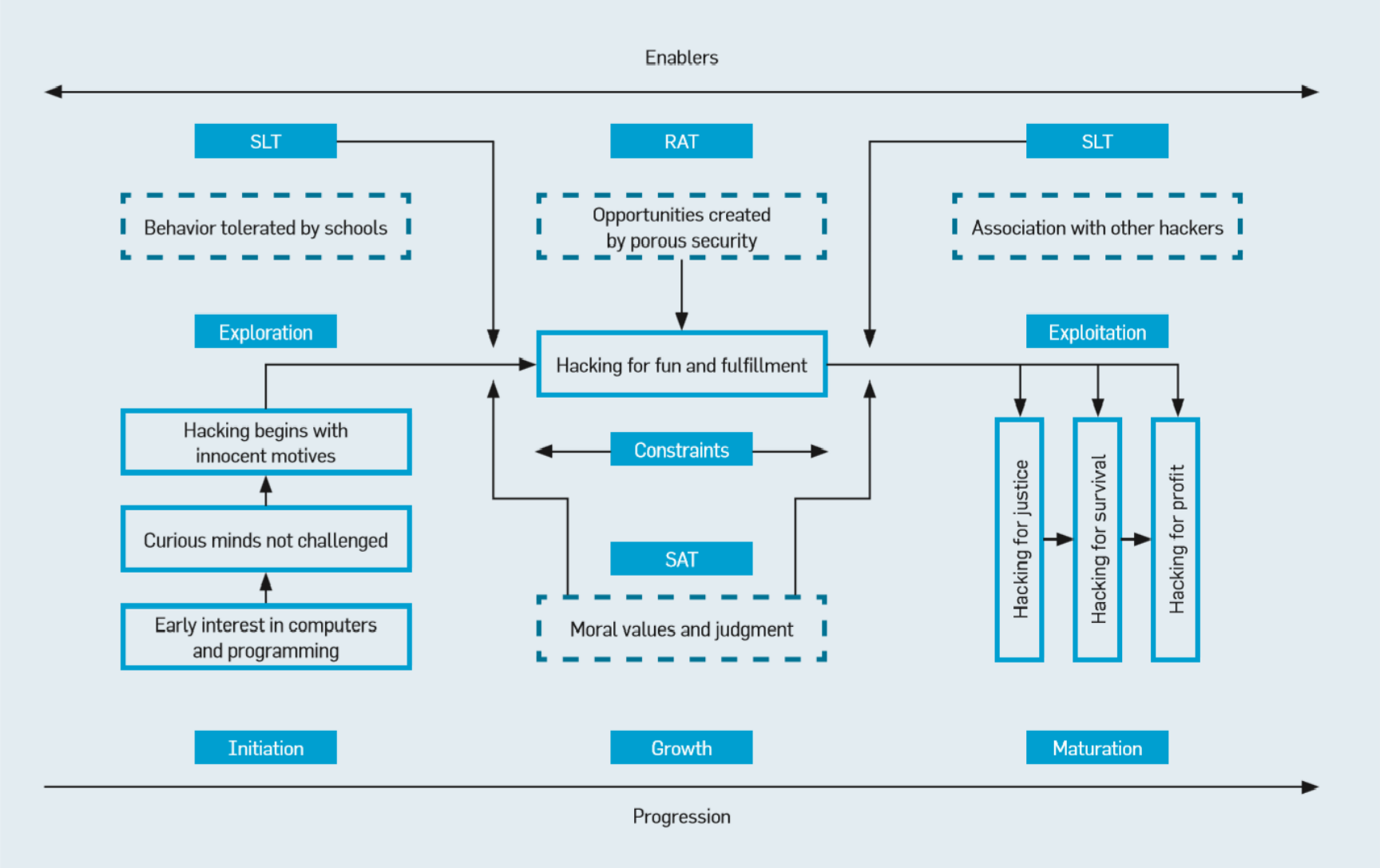
Another study focused on the difference between extrinsic and intrinsic motivation. Smyslova and Voiskounsky (2009) built off of their earlier work with the flow model, and began their study by defining the two categories of motivation. Extrinsic motivation included all bonuses, such as money, gifts, or positive feedback, whereas intrinsic motivation included human beings' interests and challenges (Smyslova & Voiskounsky, 2009). Using the flow model, they proposed that hackers experience periods of both flow, where they progress in their skill and challenges, and flow crisis, where they maintain stable and do not move. Through their research, Smyslova and Voiskounsky (2009) found that the flow model offered a comprehensive understanding for how hackers were motivated to continue hacking and hone their skill to meet challenges that were more difficult.

Containment theory has also been applied to hacking behavior. Through an analysis of cybercriminal publications between 1968 and 2009, Lu and Jen (2010) suggested that to restrain computer user's illegal behavior intention, a focus on internal social control, through education, could lead to a decrease in computer deviant behavior. Shachaf and Hara (2010) analyzed the activities of computer deviants who vandalized Wikipedia pages in an attempt to monitor their behavior and understand their motivation. They found that the behavioral characteristics of these Wikipedia vandals shared many aspects to that of script kiddies as defined by prior literature (Shachaf & Hara, 2010). Unlike most hacktivists however, Shachaf and Hara (2010) were unable to find a common motivational theme amongst their group of surveyed Wikipedia vandals.

The generalization of a psychological profile or theory to hackers was discussed and applied to different common cybercriminal activities. In a culmination of many works, Kirwan and Power (2012) suggested a plethora of motivational factors contributing to computer deviant behavior. They go on to examine many hacker categories yet were never able to establish a reliable profile for any of the behaviors (Kirwan & Power, 2012). Most hackers were perceived to be young, college aged individual who were intelligent and have an affinity for technology. Xu, Hu, and Zhang (2013) offered several explanations as to why young individuals were drawn to hacking including sociological theories in congruence with multiple motivational factors including. Specifically they argued that Social Learning Theory (SLT), Routine Activity Theory (RAT), and Situational Action Theory (SAT) worked together to transform intelligent and talented individuals into hackers (Xu et al., 2013).

SLT is a criminological theory that argues that differential association with deviant peers will lead to deviance of an individual through imitation and reinforcement of deviant behavior (Akers, 1998). RAT is a criminological theory that argues that motivated offenders will likely victimize any suitable target that lacks a capable guardian (Cohen & Felson, 1979). SAT argues individuals are likely to view all of their options through a moral lens, and will make choices according to his or her moral judgment (Wikström, 2006). The model Xu et al. (2013) proposed included all three theories working in tandem to produce hackers overtime through suitable targets, moral decision making, and peer recognition and reinforcement as shown in Figure 1. Xu et al. (2013) offered a contemporary example of how each of the motivations previously discussed in the literature are still suggested to affect computer deviant behavior.

Figure 1.
Xu et al. (2013) *Model for Progression into Cybercriminal Behavior.*



The threat of hackers inside a company, and potential solutions for identifying these individuals, was examined by Burns, Posey, Roberts, and Hightower (in-press). In their analysis of multiple motivational variables against deterrent factors they found that anger and retaliation, as well as job conditions contributed to the computer abuse of insiders (Burns et al., in-press). They go on to argue that the criminological research into malicious hacking will likely provide the next step for information security research (Burns et al., in-press). Rogers readdressed the taxonomical research he has examined since 1999. In this new update, Rogers (personal communication) focused on which classification variables can be used to differentiate types of cybercriminals. He suggested hackers can be categorized by: group affiliation, organization, motivation, and skill (Rogers, personal communication). He went on and suggested reexamining cybercriminal behavior using traditional models, given that cybercrime was simply deviant behavior dressed up in a veneer of technology (Rogers, in-press). Table 2 details a summary of all motivations presented, and the various authors that found support for each motivation.

Table 1
Previous Literature Motivations and Supporting Authors

Motivation	Author
Addiction	Beveren (2001) Smyslova & Voiskounsky (2009) Taylor (1999) Turgeman-Goldschmidt (2005) Voiskounsky & Smyslova (2003)
Curiosity	Beveren (2001) Nikitina (2012) Smyslova & Voiskounsky (2009) Turgeman-Goldschmidt (2005) Voiskounsky & Smyslova (2003)
Excitement/ Entertainment	Beveren (2001) Gordon & Ma (2003) Smyslova & Voiskounsky (2009) Turgeman-Goldschmidt (2005) Voiskounsky & Smyslova (2003)
Money	Gordon & Ma (2003) Holt et al. (2008) Kilger et al. (2004) Taylor (1999) Turgeman-Goldschmidt (2005)
Power/Status/Ego	Holt (2007) Nikitina (2012) Taylor (1999)
Ideology	Holt (2009) Jordan & Taylor (2004) Kilger et al. (2004) Schell & Martin (2004)
Revenge	Best (2003) Holt (2007) Kilger et al. (2004) Loper (2000) McQuade (2009) Taylor (1999) Turgeman-Goldschmidt (2005) Voiskounsky & Smyslova (2003) Williams (2006) Xu, Hu, & Zhang (2013)

At the time of the study, scholars within the field currently proposed several hacker categories. Script kiddies were the hackers which have the least technical skill and include all new hackers (Loper, 2000; Rogers, 1999; 2006). The cyberpunk category included hackers which have some technical skill and were malicious in their attacks (Parker, 1998; Rogers, 1999; 2006). The password crackers were the hackers which specifically focus their efforts on cracking passwords and decrypting security measures (Loper, 2000; Rogers, 1999; 2006). Internals were the disgruntled employee hackers, who were abusing their access within a system to attack (Burns et al., in-press; Rogers, 1999; 2006; in-press). Old guard hackers were the hackers which see themselves as the defenders of the internet, and often hack as a means of reporting potential security breaches to companies (Best, 2003; Loper, 2000; Rogers, 1999; 2006). Cyberterrorists and hacktivists were the hackers which were politically, socially, or religiously motivated and carry out attacks in the name of their cause (Parker, 1998; Rogers, 1999; 2006). Pirates were the category which included all users who downloaded or exchanged copyrighted software (Loper, 2000, Rogers, 2006).

Table 2
Computer Deviant Behavior Taxonomies

Author	Past Taxonomies	Current Taxonomies
Parker (1998)	Pranksters	Script Kiddie
	Malicious hackers	Cyberpunk
	Career criminals	Pirate
	Extreme advocates	Cyberterrorist
Rogers (1999)	Newbie/Tool kit (NT)	Script Kiddie
	Cyber-punks (CP)	Cyberpunk
	Internals (IT)	Internal
	Coders (CD)	Cyberpunk or Password Cracker
	Old guard hackers (OG)	Old Guard Hacker
	Cyber-terrorists (CT)	Cyberterrorist
Loper (2000)	Old school hackers	Old Guard Hacker
	WaRez D00dz	Pirate
	Hacktivists	Cyberterrorist / Hacktivist
	Script kiddies	Script Kiddie
Rogers (2006)	Novice (NV)	Script Kiddie
	Cyber-punks (CP)	Cyberpunk
	Internals (IN)	Internal
	Petty Thieves (PT)	Pirates
	Old Guard hackers (OG)	Old Guard Hacker
	Political Activists (PA)	Hacktivists

Current cybercriminal scholars also defined several motivations commonly associated with computer deviant behavior. Addiction was cited as the need to continue computer deviant behavior to satisfy a desire (Beveren, 2001; Smyslova & Voiskounsky, 2009; Taylor, 1999; Voiskounsky & Smyslova, 2003). Curiosity was the motivation to continue computer deviant behavior based on a desire to want to gain more knowledge about a topic an individual finds interesting (Beveren, 2001; Nikitina, 2012; Smyslova & Voiskounsky, 2009; Voiskounsky & Smyslova, 2003). Excitement/entertainment was the motivation to continue computer deviant behavior because of the intrinsic enjoyment of the activity (Beveren, 2001; Gordon & Ma, 2003; Smyslova & Voiskounsky, 2009; Voiskounsky & Smyslova, 2003). Financial gain was argued to be the motivation to continue computer deviant behavior because of the monetary reward it

brought (Gordon & Ma, 2003; Holt et al., 2008; Kilger et al., 2004; Taylor, 1999). Power/status/ego was the motivation to continue computer deviant behavior because of the empowering feeling it brought to the individual (Holt, 2007; Nikitina, 2012; Taylor, 1999). Ideological motivation included the political, religious, and social forces which inspired individuals to perpetrate and continue computer deviant behavior (Holt, 2009; Jordan & Taylor, 2004; Kilger et al., 2004; Schell & Martin, 2004). Peer recognition was the motivation to continue computer deviant behavior in order to remain close to a social network of others who participated in similar behavior (Best, 2003; Holt, 2007; Kilger et al., 2004; Loper, 2000; McQuade, 2009; Voiskounsky & Smyslova, 2003; Williams, 2006; Xu et al., 2013). Revenge was the motivation to perpetrate or continue computer deviant behavior to satisfy a personal vendetta against an individual, group, or entity (Holt, 2007; Turgeman-Goldschmidt, 2005; Wade et al., 2011). The current study plans on combining components of each of these concepts.

CHAPTER 3

THE CURRENT STUDY

PRETEST OF THE INSTRUMENT

McBrayer and Seigfried-Spellar (2013) conducted a pretest of the instrument by collecting a small amount of data using the instrument included in the current study to examine a computer deviant behavior typology against reported motivational factors. Six respondents were included in the final analysis, 100% ($N = 6$) reported participating in some type of computer deviant behavior (McBrayer & Seigfried-Spellar, 2013). Two respondents reported guessing, sharing, and disclosing passwords and user account information. Low levels of addiction and revenge motivations were reported, with high levels of curiosity, excitement/entertainment, financial, power/status/ego, and peer recognition motivations being reported (McBrayer & Seigfried-Spellar, 2013). The pretest sample reported being politically moderate. This pretest indicated that the use of an online survey was an appropriate method of collecting data from self-identifying computer deviants. Based in part on this pretest exploration, further research was warranted to conduct a broad examination of a full-scale set of motivations against an updated computer deviant behavior typological classification.

CURRENT STUDY

Building from a thorough literature base examining the different categorizations of computer deviant behavior and motivational factors as well as the pretest, the current study sought to address whether specific hacker motivations affected differential computer deviant behaviors. The current study intended to contribute to the body of knowledge by using the computer deviant motivations proposed within the literature to analyze computer deviant behavior subcategories (Armitage & Roberts; 2002; Beveren, 2001; Gordon & Ma, 2003; Holt,

2007; Holt, 2009; Jordan & Taylor, 2004; Kilger, Arkin, & Stutzman, 2004; Kirwan & Power, 2012; Lu & Jen, 2010; Nikitina, 2012; Rogers et al., 2006; Schell & Dodge, 2002; Shachaf & Hara, 2010; Smyslova & Voiskounsky, 2009; Taylor, 1999; Taylor et al., 2006; Turgeman-Goldschmidt, 2005; Voiskounsky & Smyslova, 2003; Williams, 2006; Xu, Hu, & Zhang, 2013). Specifically, the present study explored which motivations were associated with each unique computer deviant behavior category. By examining the interrelationships between computer deviant behaviors and their motivations, the author hoped to understand if motivations could be associated with specific computer deviant behavior. Based on prior research, this study explored the following research questions:

Q_1: Which motivations (addiction, curiosity, excitement/entertainment, financial, power/status/ego, peer recognition, and revenge) are associated with specific computer deviant behaviors?

Q_2: Which demographic characteristics (sex, age) are associated with specific computer deviant behaviors?

To gain a greater understanding of these research questions, this chapter will discuss the research hypotheses for this study, followed by the operational definitions of the constructs being measured in the study. Finally, the population of interest and sampling methods for this study will also be discussed.

RESEARCH HYPOTHESES

As previously discussed, no study had yet analyzed the association of motivations with the current computer deviant behavior taxonomy. The intent of this study was to examine the prevalence of computer deviant behavior through the implementation of a computer deviant

behavior taxonomy and determine which motivational and demographic characteristics were associated with computer deviant behavior category.

H_1: There are differences in motivational factors between computer deviant behavior categories.

H_{1_1}: Script kiddies will be associated with high levels of excitement/entertainment and peer recognition motivations.

H_{1_2}: Cyberpunks will be associated with high levels of excitement/entertainment motivation.

H_{1_3}: Password crackers will be associated with high levels of addiction, excitement/entertainment, and power/status/ego motivations.

H_{1_4}: Internals will be associated with high levels of financial and revenge motivation.

H_{1_5}: Old guard hackers will be associated with high levels of curiosity motivation.

H_2: There are more male computer deviants than females.

OPERATIONAL DEFINITIONS OF CONSTRUCTS

To define the variables, this study begins with the research question: are differential computer deviant behavior associated with specific motivations? The independent variable is the synthesized hacker typology developed from the literature. This typology offers a categorization of hacking based on methods, tactics, or skill levels. The dependent variables are the hacker motivations cited throughout the cybercriminal research.

DEPENDENT VARIABLE. The literature provides the hacker typological framework based on methodological delineations (Burns et al., in-press; Loper, 2000; Rogers, 1999; Rogers, 2006). The computer deviant behavior typology was operationalized into mutually exclusive and exhaustive computer deviant behavior subcategories based on the specific behaviors of each category. These groups were constructed by overlaying the hacker categories of Loper (2000),

Parker (1998), Rege-Patwardhan (2009), and Rogers (1999; 2006; personal communication) with the removal of categories defined intrinsically by motivation and not methods, tactics, or skill. Using the work of these authors, the hacker typology utilized within the current study included the following categories: Script Kiddies, Cyberpunks, Internals, Password Crackers, and Old Guard Hackers. Cyberterrorists and hacktivists were removed because each category was defined by the political, social, or religious motivation which lead to the behavior (Parker, 1998; Rogers, 1999; 2006). Additionally, cyberterrorists and hacktivists overlap significantly in the literature, and would not provide mutually exclusive categories (Parker, 1998; Rogers, 1999; 2006). Though the category of pirates was a computer deviant behavior, pirating software fell under the category of using the computer as a tool to commit theft (Loper, 2000, Rogers, 2006). Pirates therefore did not fall within the group of computer deviant behaviors which target other computers or computer systems, and were excluded for this reason (Maras, 2012).

The operationalization of the hacker taxonomy came from the Computer Crime Index - Revised and including Internals (CCI-RI) which was first proposed by Rogers (1999) and then was later revised and further validated in several research studies on computer deviant behavior (Rogers, 2006; Rogers et al., 2006). The most recent version included a never before published addition to the scale which accounted for the internals category (Rogers, personal communication). The CCI-RI has been modified to reduce the length and only included items relevant to the categories being measured. The result was a 27 item version of the original CCI-RI which measured the prevalence of self-reported computer deviant behavior. The instrument uses a 5-point Likert scale with 1 being "does not apply to me" and 2 (16 or less) through 5 (21 or older) asking respondents to report the age when they first participated in a computer deviant behavior. Based on item response, respondents were classified as script kiddies, cyberpunks,

password crackers, internals, and old guard hackers. The following statements are examples from the modified CCI-RI, which were used to classify the respondents' computer deviant behavior:

1. Script Kiddies: used a wireless access point that you did not have permission or authorization to use
2. Cyberpunk: defaced/altered a website without authorization or permission
3. Password Cracker: tried to guess another's password to get into his/her computer account or files
4. Internal: Made copies or backups of data, or other proprietary information without authorization or permission.
5. Old guard hackers: monitored network/internet traffic without authorization or permission

INDEPENDENT VARIABLE. The literature explicitly provided eight motivations commonly cited in hacker research: addiction, curiosity, excitement/entertainment, money, power/status/ego, peer recognition, ideological, and revenge (Armitage & Roberts; 2002; Beveren, 2001; Gordon & Ma, 2003; Holt, 2007; Holt, 2009; Jordan & Taylor, 2004; Kilger, Arkin, & Stutzman, 2004; Kirwan & Power, 2012; Lu & Jen, 2010; Nikitina, 2012; Rogers et al., 2006; Schell & Dodge, 2002; Shachaf & Hara, 2010; Smyslova & Voiskounsky, 2009; Taylor, 1999; Taylor et al., 2006; Turgeman-Goldschmidt, 2005; Voiskounsky & Smyslova, 2003; Williams, 2006; Xu, Hu, & Zhang, 2013). Ideological motivation was removed because it was directly tied to the cyberterrorists and hacktivist computer deviant behavior categories (Jordan & Taylor, 2004; Loper, 2000; Parker, 1998, Rogers, 1999; 2006). The remaining seven motivations provided the framework for the independent variable. Each of these motivations has its own unique definition and operationalization.

The operationalization of addiction as a motivational factor used the compulsive internet use scale (CIUS) developed by Meerkerk, Eijnden, Vermulst, and Garretsen (2009). The CIUS was a 14 item, 5-point Likert scale ranging from 1 (Never) to 5 (Very Often) asking how often respondents feel a certain way. The Chronbach's alpha of the CIUS used in the current study was ($\alpha = .903$). The following statement is an example from the CIUS, which was used to measure respondents' addiction motivation: "Do you find it difficult to stop using the Internet when you are online?"

The operationalization of curiosity as a motivation factor used the curiosity and exploration inventory (CEI-II) developed by Kashdan et al. (2009). The CEI-II was a 10 item, 5-point Likert scale ranging from 1 (Very Slightly or Not at all) to 5 (Extremely) which asked respondents to rate how they generally feel and behave. This scale offers both stretching and embracing questions. The Chronbach's alpha of the CEI-II used in the current study was ($\alpha = .894$). The following statement is an example from the CEI-II, which was used to measure respondents' curiosity motivation: "Everywhere I go I am out looking for new things or experiences."

The operationalization of excitement/entertainment as a motivational factor came from the Internet gratification scale used by Song, Larose, Eastin, and Lin (2004). The Internet gratification scale was a 36 item, 5-point Likert scale ranging from 1 (Very Unlikely) to 5 (Very Likely) which asked if respondents would experience gratification from specific online situations. The Internet gratification scale was modified to include only the items directly relevant to the concept being measured and was reduced to 10 items. The Chronbach's alpha of the modified Internet gratification scale used in the current study was ($\alpha = .800$). The following statement is an example from the modified Internet gratification scale, which was used to

measure respondents' excitement/entertainment motivation: “While online how likely are you to feel relaxed?”

The operationalization of financial incentives as a motivational factor used the power-prestige component of the money attitude scale (MAS) developed by Yamauchi and Templer (1982). The MAS was a nine item, 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) which asked respondents how they generally felt towards money. The MAS included the nine strongest items from Yamauchi and Templer's (1982) factor analysis on a 62 item scale. The Chronbach’s alpha of the MAS used in the current study was ($\alpha = .863$). The following statement is an example from the MAS, which was used to measure respondents' financial motivation: “People I know tell me that I place too much emphasis on the amount of money a person has as a sign of his or her success.”

The operationalization of power/status/ego as a motivational factor used the objective measure of ego identity statuses (OMEIS) questionnaire developed by Marcia (1993). The OMEIS was a 64 item, 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) which asked respondents to answer questions about how they felt about specific scenarios. The OMEIS was modified to include only the items directly relevant to the concept being measured and was reduced to 10 items. The Chronbach’s alpha of the modified OMEIS used in the current study was ($\alpha = .225$) and was later removed from the analysis for this reason. This will be discussed further in the limitations section. The following statement is an example from the modified OMEIS, which was used to measure respondents' power/status/ego motivation: “I only pick friends my parents would approve of.”

The operationalization of peer recognition as a motivation factor used cyber lives index (CLI) which was originally developed by Chao, Yu, and Cheng (2013). The CLI was a 22 item,

5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) which asked respondents to describe how well the statements reflect their current online relationships. The CLI was modified to include only the items directly relevant to the concept being measured, which was accomplished by removing the online gaming section. The modified CLI had 10 items. The Chronbach's alpha of the modified CLI used in the current study was ($\alpha = .879$). The following statement is an example from the modified CLI, which was used to measure respondents' peer recognition motivation: "My online relationships have improved my communication skills."

The operationalization of revenge as a motivational factor used the social interaction norms scale which was analyzed by Eisenberger, Lynch, Aselage, and Rohdieck (2012). The social interaction norm scale was a 24 item, 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) which asked respondents to rate statements based on which best reflect their attitude. The scale included both negative reciprocity norms and positive reciprocity norms questions. The social interaction norms scale was modified to include only the items directly relevant to the concept being measured, which was accomplished by only including the items which received the highest factor analysis score (Eisenberger et al., 2012). The modified social interaction norms scale had 12 items. The Chronbach's alpha of the modified social interaction norm scale used in the current study was ($\alpha = .812$). The following statement is an example from the modified social interaction norms scale, which was used to measure respondents' revenge motivation: "If a person wants to be your enemy, you should treat them like an enemy."

CHAPTER 4

METHODOLOGY

POPULATION AND SAMPLE

The computer deviant behavior typologies proposed by Loper (2000) and Rogers (1999; 2006) specifically focused on computer deviants. This study will also focus primarily on computer deviants as the population being studied. The computer deviant population was sparsely distributed and has limited contact with outside groups (Best, 2003). To sample from this population with a probabilistic sampling technique would be difficult given the small proportion of computer deviants to non-computer deviants and the high risk associated with disclosing criminal information (Loper, 2000; Rogers, 1999; 2006; Parker, 1998). The nature of the potential subjects also made it difficult to develop a sampling frame. Because the study intended to reach a difficult demographic to survey, the study utilized the snowball sampling strategy (Hagan, 2010). This technique was appropriate to this study given the exploratory nature and uncommon characteristics of the population. There were no boundaries other than time with this sampling method and using an Internet survey instrument allowed for subjects to accrue as time passed.

Gathering the subjects began with advertising of the survey along with a short informative introduction letter through targeted popular forums, chat rooms, IRC channels, and Facebook pages, where hackers are known to congregate. The “thank you” splash page at the end of the survey asked subjects to recommend friends to the survey, which created a self-perpetuating sample that was in accordance with the operation of the snowball sampling

technique (Hagan, 2010). The author sought to achieve a sample size of 300 subjects. To facilitate this, the author attempted to oversample, seeking 500 potential respondents.

Prior to filling out the survey, the respondents were asked to click "I Agree" on the consent page, which informed them of the purpose and potential risks of the study as well as required they be at least 19 years of age or older. If the respondents indicated that they were not 19 years of age or older, they were not able to complete the survey due to their status as a minor in the state of Alabama. It was required for the respondent to give consent to begin the survey, and they were able to exit the survey at any time. Following completion of the survey, the respondents were directed to a page which thanked them for their participation, provided contact information for further questions about the study, and asked that they share the study with others who may be interested in the subject.

DESIGN AND PROCEDURE

The data was collected through the use of an internet self-report survey hosted by the program Qualtrics©. Qualtrics© allowed for the survey to be completely anonymous as the program did not collect IP information which prevented identification of respondents by the researcher and further increased the confidentiality. Additionally, Qualtrics had several features that allowed for easy implementation of partitions, Likert scales, and consent forms within the survey.

Once the respondent was on the website of the survey they were prompted to give consent to completing the survey. After the respondent had clicked "I Agree", they were taken to the first page of questions and shown an estimated time of completion. Once the survey began, the respondent was prompted to enter their age and sex. After this, the survey was broken into three parts, the first part contained the modified CCI-RI which identified the dependent variable

of computer deviant behavior categories. The author placed this scale first as it was the most essential component of the study. The second part of the survey contained the independent variable scales, which measured motivations. The final part of the survey contained the demographic variables, and an open ended question which asked for additional comments. After completing the survey, the respondents were directed to a thank you page which provided them the contact information of the researcher and asked them to invite others to complete the survey. The data was collected electronically and stored in accordance with Internal Review Board (IRB) and American Psychological Association (APA) guidelines.

PLAN FOR ANALYSIS

The data was analyzed using a zero-order correlation to determine any significant relationship between the computer deviant behavior categories and motivational factors. Afterwards, a backwards (Wald) binary logistic regression was conducted to determine the influence of motivational factors on predicting computer deviant behavior. A Hosmer and Lemeshow test determined if the predictive model fits the data. A second zero-order correlation determined any significant relation between the computer deviant behavior categories a sex of the respondent. Finally, a binary logistic regression determined the influence of sex of the respondent on predicting computer deviant behavior.

CHAPTER 5

STATISTICAL ANALYSIS

Due to the exploratory nature of this study, two-tailed statistical significance was set at the alpha level of 0.10 prior to any analyses. First, zero-order correlation was conducted to determine if any of the computer deviant behavior types (e.g., script kiddies) were significantly related to any of the motivation factors being measured (e.g., addiction). Logistic regression was used to measure the variables significantly related to each behavior according to the zero-order correlation, as it is a robust measure and appropriate for exploratory analyses (Field, 2009). Specifically, a backward stepwise (Wald) logistic regression was run in order to identify the best predictive model for each computer deviant behavior in order to identify which motivation factors were significant predictors of computer deviant behavior.

RESULTS

Based on the item response, the majority of respondents have engaged in some sort of computer deviant behavior. Of the original 250 respondents who answered the survey, only 120 respondents were included in the final analysis. The remaining 130 respondents were dropped based on either incomplete data or response set (answering all questions with the same answer). Of the remaining 120 respondents included in the final analysis, 93% (n = 112) reported participating in some type of computer deviant behavior. Of these specific computer deviant behaviors, 81% (n = 98) identified with script kiddie behaviors, 79% (n = 95) identified with password cracker behaviors, 77% (n = 92) identified with old guard hacker behaviors, 50% (n = 61) identified with cyberpunk behaviors, and 50% (n = 59) identified with internals behavior. As shown in Table 3, of all computer deviants there were slightly more males (51.4%, n = 55) than females (48.6%, n = 52). The majority of computer deviants, were young, as 50.9% (n = 57)

reported being between the ages of 19 to 24, and an additional 33% (*n* = 37) reported being between the ages of 25 to 30. Of computer deviants, 73.2% (*n* = 82) reported living within the United States, 68.8% (*n* = 77) reported being single, having never married, 89.3% (*n* = 100) reported being Caucasian or white, 72.3% (*n* = 81) reported having no religious views, and 75% (*n* = 84) were most familiar with the windows operating system.

Table 3
Demographics of Computer Deviants vs. Non-Computer Deviants

		Computer		
Variable		**Deviant** (*n* = 112)	**Non-Deviant** (*n* = 8)	**Total** (*N* = 120)
Sex	Male	55 (51.4)	4 (50)	59 (51.3)
	Female	52 (48.6)	4 (50)	56 (48.7)
Age	19-24	57 (50.9)	3 (37.5)	60 (50)
	25-30	37 (33)	1 (12.5)	38 (31.7)
	31+	18 (16.1)	4 (50)	22 (18.3)
Country of Residence	United States	82 (73.2)	7 (87.5)	89 (74.2)
	Other	30 (26.8)	1 (12.5)	31 (25.8)
Marital Status	Single, Never Married	77 (68.8)	4 (50)	81 (67.5)
	Married	17 (15.2)	4 (50)	21 (17.5)
	Other	18 (16.1)	0 (0)	18 (15)
Ethnicity	Caucasian/White	100 (89.3)	8 (100)	108 (90)
	Other	12 (10.7)	0 (0)	12 (10)
Religion	Non-Religious	81 (72.3)	6 (75)	87 (72.5)
	Religious	31 (27.7)	2 (25)	33 (27.5)
Most Familiar Operating System	Windows	84 (75)	5 (62.5)	89 (74.2)
	Apple/Mac	16 (14.3)	2 (25)	18 (15)
	Other	12 (10.7)	1 (12.5)	13 (10.8)

Note. Values represent frequency with percentages in parentheses.

Based on the item responses, each computer deviant behavior was treated as a dichotomous variable (0 = did not participate in behavior, 1 = participated in behavior). There was significant overlap between the different computer deviant behaviors. As shown in Table 4, 9.2% (*n* = 11) reported participation in at only one computer deviant behavior, 10.8% (*n* = 13) reported participation in two computer deviant behaviors, 16.7% (*n* = 20) reported participation

in three computer deviant behaviors, 17.4% (n = 21) reported participation in four computer deviant behaviors, and 30% (n = 36) reported participation in *all* five computer deviant behaviors.

Table 4
Classification of Respondents by Self-Reported Computer Deviant Behaviors

Computer Deviant Behavior	**Total** (N = 120)
None	8 (6.7)
Script Kiddie Only	5 (4.2)
Password Cracker Only	3 (2.5)
Internal Only	2 (1.7)
Old Guard Hacker	1 (0.8)
SK + PC	6 (5.0)
SK + Int	1 (0.8)
SK + OGH	3 (2.5)
PC + OGH	3 (2.5)
SK + CyP + PC	1 (0.8)
SK + PC + OGH	12 (10.0)
SK + Int + OGH	2 (1.7)
CyP + PC + Int	1 (0.8)
CyP + Int + OGH	2 (1.7)
PC + Int + OGH	2 (1.7)
Sk + CyP + PC + Int	1 (0.8)
SK + CyP + PC + OGH	19 (15.8)
SK + PC + Int + OGH	1 (0.8)
All Deviant Behaviors	36 (30.0)

Note. Values represent frequency with percentages in parentheses. SK = Script Kiddie, CyP = Cyberpunk, PC = Password Cracker, Int = Internal, OGH = Old Guard Hacker.

There were statistically significant zero-order positive correlations between all computer deviant behaviors. As seen in Table 5, script kiddie behavior was significantly related to cyberpunk behavior (r_ϕ = .35, p < .01), password cracker behavior (r_ϕ = .45, p < .01), internals behavior (r_ϕ = .16, p = .07), and old guard hacker behavior (r_ϕ = .45, p < .01). Cyberpunk behavior was significantly related to password cracker (r_ϕ = .40, p < .01), internals behavior (r_ϕ = .37, p < .01), and old guard hacker behavior (r_ϕ = .44, p < .01). Password cracker behavior was

significantly related to internal (r_ϕ = .18, p = .05) and old guard hacker (r_ϕ = .49, p < .01) behaviors. Lastly, internals behavior was also significantly related to old guard hacker behavior (r_ϕ = .35, p < .01).

Table 5
Zero-order Correlation between Computer Deviant Behaviors

	Computer Deviant Behaviors				
	Script Kiddies	Cyberpunks	Password Crackers	Internals	Old Guard Hackers
Script Kiddies	1.0	.35**	.45**	.16†	.45**
Cyberpunks		1.0	.40**	.37**	.44**
Password Crackers			1.0	.18†	.49**
Internals				1.0	.35**
Old Guard Hackers					1.0

**p < .01, two-tailed. *p < .05, two-tailed. †p < .10, two-tailed.
Note. N = 120

H_1: There are differences in motivational factors between computer deviant behavior categories.

H_{1_1} : Script kiddies will be associated with high levels of excitement/entertainment and peer recognition motivations.

As shown in Table 6, each computer deviant behavior was analyzed through a one-way ANOVA to determine any motivational difference between deviants and non-deviants. As shown in Table 7, there was marginal relationship between script kiddie computer deviant behavior and addiction motivation (r_ϕ = .16, p = .08). As shown in Table 8, a backward (Wald) binary logistic regression was conducted to determine the best predictive model for self-reported script kiddie computer deviant behavior. Results suggested the best predictive model for distinguishing between script kiddies and non-script kiddies included high score in addiction motivation (Wald = 2.92, p = .09). The Hosmer and Lemeshow test was non-significant, $\chi^2(8)$ =

7.80 with $p = .45$, indicating the final model fit the data. The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 4% of the variance in script kiddie computer deviant behavior ($R_C^2 = .03$; $R_N^2 = .04$). The overall model was able to correctly classify 100% of script kiddies and 0% of non-script kiddies, for a weighted average of 82%. There was no improvement from the model with only the intercept, which reported the same weighted average of 82%. There was no significant relationship between script kiddie computer deviant behavior and peer recognition motivation ($r_\phi = .13$, $p > .10$).

Table 6

Means and Standard Deviations for Motivational Differences by Computer Deviant Behavior

	Motivation					
Computer Behavior	A	C	E/E	M	PR	R
Script Kiddie	2.73 (0.76)†	3.27 (0.83)	3.54 (0.60)	1.75 (0.72)	3.43 (0.67)	2.21 (0.56)
Non-Script Kiddie	2.41 (0.86)†	3.13 (0.58)	3.36 (0.53)	1.52 (0.38)	3.20 (0.68)	2.17 (0.50)
Cyberpunk	2.82 (0.81)*	3.26 (0.87)	3.49 (0.66)	1.86 (0.78)*	3.50 (0.69)†	2.29 (0.58)†
Non-Cyberpunk	2.51 (0.74)*	3.22 (0.72)	3.52 (0.51)	1.54 (0.52)*	3.27 (0.63)†	2.11 (0.50)†
Password Cracker	2.76 (0.79)**	3.25 (0.82)	3.53 (0.59)	1.77 (0.72)*	3.43 (0.66)	2.21 (0.57)
Non-Password Cracker	2.30 (0.69)**	3.20 (0.71)	3.43 (0.56)	1.47 (0.39)*	3.20 (0.70)	2.21 (0.46)
Internal	2.78 (0.79)	3.31 (0.84)	3.50 (0.65)	1.83 (0.75)*	3.52 (0.67)*	2.14 (0.58)
Non-Internal	2.56 (0.78)	3.18 (0.75)	3.51 (0.52)	1.58 (0.58)*	3.25 (0.65)*	2.27 (0.51)
Old Guard Hacker	2.81 (0.77)	3.21 (0.85)	3.51 (0.61)	1.78 (0.72)*	3.46 (0.68)*	2.25 (0.58)
Non-Old Guard Hacker	2.20 (0.67)	3.35 (.0.59)	3.48 (0.54)	1.45 (0.42)*	3.13 (0.59)*	2.07 (0.40)

**$p < .01$, two-tailed. *$p < .05$, two-tailed. †$p < .10$, two-tailed.

Note: Values represent means with standard deviations in parentheses. A = Addiction, C = Curiosity, E/E = Excitement/Entertainment, M = Money, PR = Peer Recognition, R = Revenge. Scales range from 1 (Extremely Low) to 5 (Extremely High).

Table 7

Zero-Order Correlation between Computer Deviant Behaviors and all Motivational Factors

	Motivation					
Computer Behavior	A	C	E/E	M	PR	R
Script Kiddie	0.16†	.07	.11	.13	.13	.03
Cyberpunk	.20*	.03	-.03	.23*	.17†	.17†
Password Cracker	.24**	.03	.07	.18*	.14	.00
Internal	.14	.08	-.01	.18*	.20*	-.13
Old Guard Hacker	.33**	-.08	.03	.21*	.21*	.14

**$p < .01$, two-tailed. *$p < .05$, two-tailed. †$p < .10$, two-tailed.

Note: A = Addiction, C = Curiosity, E/E = Excitement/Entertainment, M = Money, PR = Peer Recognition, R = Revenge.

Table 8

Backward Stepwise (Wald) Logistic Regression of Computer Deviant Behaviors by Motivations

Variable	*B*	*SE B*	*Exp* (*B*)
		Script Kiddie	
Step 1			
Addiction†	.57	.33	1.76
		Cyberpunk	
Step 1			
Addiction	.22	.29	1.25
Money*	.74	.33	2.10
Peer Recognition†	.61	.34	1.83
Revenge†	.72	.38	2.06
Step 2			
Money**	.82	.31	2.26
Peer Recognition*	.72	.31	2.04
Revenge†	.71	.38	2.03
		Password Cracker	
Step 1			
Addiction*	.76	.35	2.15
Money	.63	.44	1.88
Step 2			
Addiction*	.86	.34	2.36
		Internal	
Step 1			
Money*	.65	.30	1.91
Peer Recognition*	.72	.30	2.05
		Old Guard Hacker	
Step 1			
Addiction*	.96	.40	2.62
Money†	.74	.43	2.09
Peer Recognition	.42	.39	1.52
Step 2			
Addiction**	1.14	.37	3.13
Money	.68	.43	1.96
Step 3			
Addiction**	1.22	.35	3.40

**$p < .01$, two-tailed. *$p < .05$, two-tailed. †$p < .10$, two-tailed.

H_{1_2}: Cyberpunks will be associated with high levels of excitement/entertainment motivation.

As shown in Table 6, cyberpunk computer deviant behavior was analyzed through a one-way ANOVA to determine any motivational difference between cyberpunks and non-cyberpunks. As shown in Table 7, Cyberpunk behavior was significantly related to financial (r_ϕ = .23, p = .01) motivation, and marginally related to peer recognition (r_ϕ = .17, p = .07) and revenge (r_ϕ = .17, p = .07) motivations. As shown in Table 8, a backward (Wald) binary logistic regression was conducted to determine the best predictive model for self-reported cyberpunk computer deviant behavior. Results suggested the best predictive model for distinguishing between cyberpunks and non-cyberpunks included high scores in financial (Wald = 6.75, p < .01), peer recognition (Wald = 5.26, p = .02), and revenge (Wald = 3.49, p = .06) motivations. The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 4.59$ with p = .80, indicating the final model fit the data. The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 9% of the variance in cyberpunk computer deviant behavior (R_C^2 = .12; R_N^2 = .16). The overall model was able to correctly classify 66% cyberpunks and 61% of non-cyberpunks, for a weighted average of 63%. This was a statistically significant improvement from the model with only the intercept, which reported a weighted average of 51%. There was no significant relationship between cyberpunk computer deviant behavior and excitement/entertainment motivation (r_ϕ = -.03, p > .10).

H_{1_3}: Password crackers will be associated with high levels of addiction, excitement/entertainment, and power/status/ego motivations.

As shown in Table 6, password cracker computer deviant behavior was analyzed through a one-way ANOVA to determine any motivational difference between password crackers and

non-password crackers. As shown in Table 7, password cracker behavior was significantly related to addiction (r_ϕ = .24, p = .01) motivation. As shown in Table 8, a backward (Wald) binary logistic regression was conducted to determine the best predictive model for self-reported password cracker computer deviant behavior. Results suggested the best predictive model for distinguishing between password crackers and non-password crackers included high scores in addiction motivation (Wald = 6.42, p = .01). The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 4.01$ with p = .86, indicating the final model fit the data. The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 6% of the variance in password cracker computer deviant behavior (R_C^2 = .06; R_N^2 = .09). The overall model was able to correctly classify 100% password crackers and 0% of non-password crackers, for a weighted average of 79%. There was no improvement from the model with only the intercept, which reported the same weighted average of 79%. There was no significant relationship between password cracker computer deviant behavior and excitement/entertainment motivation (r_ϕ = .07, p > .10).

H_{1_4}: Internals will be associated with high levels of financial and revenge motivation.

As shown in Table 6, internal computer deviant behavior was analyzed through a one-way ANOVA to determine any motivational difference between internals and non-internals. As shown in Table 7, internal behavior was significantly related to financial (r_ϕ = .18, p = .05) and peer recognition (r_ϕ = .20, p = .03) motivations. As shown in Table 8, a backward (Wald) binary logistic regression was conducted to determine the best predictive model for self-reported internal computer deviant behavior. Results suggested the best predictive model for distinguishing between internals and non-internals included high scores in financial (Wald =

4.78, p = .03) and peer recognition (Wald = 5.72, p = .02) motivations. The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 15.14$ with p = .06, indicating the final model fit the data. The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 6% of the variance in internal computer deviant behavior (R_C^2 = .08; R_N^2 = .11). The overall model was able to correctly classify 61% internals and 64% of non-internals, for an overall success rate of 63%. This was a statistically significant improvement from the model with only the intercept, which reported an overall success rate of 51%. There was no significant relationship between internal computer deviant behavior and revenge motivation (r_ϕ = -.13, p > .10).

H_{1_5}: Old guard hackers will be associated with high levels of curiosity motivation.

As shown in Table 6, old guard hacker computer deviant behavior was analyzed through a one-way ANOVA to determine any motivational difference between old guard hackers and non-old guard hackers. As shown in Table 7, old guard hacker behavior was significantly related to addiction motivation (r_ϕ = .33, p < .01). As shown in Table 8, a backward (Wald) binary logistic regression was conducted to determine the best predictive model for self-reported old guard hacker computer deviant behavior. Results suggested the best predictive model for distinguishing between old guard hackers and non-old guard hackers included high scores in addiction motivation (Wald = 11.46, p < .01). The Hosmer and Lemeshow test was non-significant, $\chi^2(8) = 7.04$ with p = .53, indicating the final model fit the data. The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 11% of the variance in old guard hacker computer deviant behavior (R_C^2 = .11; R_N^2 = .17). The overall model was able to correctly classify 97% old guard hackers and 11% of non-old guard hackers, for a weighted average of 77%. There was no improvement from the model with only the intercept, which reported the same weighted average of 77%. There was no significant relationship between old guard hacker

computer deviant behavior and curiosity motivation (r_ϕ = -.08, p > .10).

Overall, expectations of varied motivational factors being related to the computer deviant behaviors is supported. However, of the sub-hypotheses, none were fully supported. Only two sub-hypotheses were partially supported: password cracker behavior had a significant relationship to addiction motivation and internal behavior had a significant relationship to financial motivation. No support was found for any of the remaining sub-hypotheses.

H_2: There are more male computer deviants than females.

For this hypothesis, sex was measured as a dichotomous variable (1 = male, 2 = female). As shown in Table 9, each computer deviant behavior was analyzed through a frequency distribution to determine if sex of the respondent being male was significantly different between self-reporting deviants and non-deviants. As shown in Table 10, sex of the respondent being male was significantly related to script kiddie computer deviant behavior (r_ϕ = -.19, p = .04) and marginally related to cyberpunk (r_ϕ = -.18, p = .05) and old guard hacker (r_ϕ = -.16, p = .09) computer deviant behaviors.

Table 9
Demographics for Sex Differences by Computer Deviant Behavior

	Sex (N = 115)	
Computer Behavior	Male	Female
Script Kiddie	52 (55.9*	41 (44.1)*
Non-Script Kiddie	7 (31.8)*	15 (68.2)*
Cyberpunk	35 (60.3)†	23 (39.7)†
Non-Cyberpunk	24 (42.1)†	33 (57.9)†
Password Cracker	48 (52.7)	43 (47.3)
Non-Password Cracker	11 (45.8)	13 (54.2)
Internal	32 (57.1)	24 (42.9)
Non-Internal	27 (45.8)	32 (54.2)
Old Guard Hacker	49 (55.7)†	39 (44.3)†
Non-Old Guard Hacker	10 (37.0)†	17 (63.0)†

**p < .01, two-tailed. *p < .05, two-tailed. †p < .10, two-tailed.
Note. Values represent frequency with percentages in parentheses.
N = 115 due to missing data on variable "sex".

Table 10
Zero-Order Correlation between Computer Deviant Behaviors and Sex

Computer Behavior	Sex
Script Kiddie	-.19*
Cyberpunk	-.18†
Password Cracker	-.06
Internal	-.11
Old Guard hacker	-.16†

*$p < .05$, two-tailed. †$p < .10$, two-tailed.

As shown in Table 11, a binary logistic regression was conducted to determine the best predictive model for self-reported script kiddie computer deviant behavior. Results suggested the best predictive model for distinguishing between script kiddies and non-script kiddies did include the sex of the respondent being male (Wald = 3.95, $p = .05$). The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 4% of the variance in script kiddie computer deviant behavior ($R_C^2 = .04$; $R_N^2 = .06$). The overall model was able to correctly classify 100% of script kiddies and 0% of non-script kiddies, for a weighted average of 81%. There was no improvement from the model with only the intercept, which reported the same weighted average rate of 81%.

Table 11
Stepwise Logistic Regression Model Prediction Computer Deviant Behaviors vs. Sex

Variable	*B*	*SE B*	*Exp* (*B*)
		Script Kiddie	
Step 1			
Sex*	-1.00	.50	.37
		Cyberpunk	
Step 1			
Sex†	-.74	.38	.48
		Old Guard Hacker	
Step 1			
Sex†	-.76	.45	.47

**$p < .01$, two-tailed. *$p < .05$, two-tailed. †$p < .10$, two-tailed.

As shown in Table 11, a binary logistic regression was conducted to determine the best predictive model for self-reported cyberpunk computer deviant behavior. Results suggested the best predictive model for distinguishing between cyberpunks and non-cyberpunks did include the sex of the respondent being male (Wald = 3.79, p = .05). The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 2% of the variance in cyberpunk computer deviant behavior (R_C^2 = .03; R_N^2 = .04). The overall model was able to correctly classify 60.3% of cyberpunks and 57.9% of non-cyberpunks, for a weighted average of 59.1%. This was a statistically significant improvement from the model with only the intercept, which reported a weighted average of 50.4%.

Lastly, as shown in Table 11, a binary logistic regression was conducted to determine the best predictive model for self-reported old guard hacker computer deviant behavior. Results suggested the best predictive model for distinguishing between old guard hackers and non-old guard hackers did include the sex of the respondent being male (Wald = 2.81, p = .09). The Hosmer and Lemeshow's Measure (R_L^2) suggested this model explained 3% of the variance in old guard hacker computer deviant behavior (R_C^2 = .03; R_N^2 = .04). The overall model was able to correctly classify 100% of old guard hackers and 0% of non-old guard hackers, for a weighted average of 76.5%. There was no improvement from the model with only the intercept, which reported the same weighted average rate of 76.5%.

The expectation that more males would be computer deviants than females was partially supported. Script kiddies, cyberpunks, and old guard hackers were all found to have a significant relationship with the reported sex of the respondent being male, and all were found to have slightly more males than females.

CHAPTER 6

DISCUSSION

The current study was the first to examine the script kiddie, cyberpunk, password cracker, internal, and old guard hacker computer deviant behaviors against motivations scholars in this field have suggested were related to computer deviant behavior. The study aimed to assess the prevalence of computer deviant behavior, which motivational factors were related to each specific type of computer deviant behavior, and if one sex was participating in each computer deviant behavior more than the other. The current study found that 93% of the respondents included in the final analysis had participated in some form of computer deviant behavior. The current study also found half of computer deviants to be young, as 50.9% reported being between the ages of 19 to 24. The group was also primarily single, having never married (89.3%) and was evenly split between males (51.4%) and females (48.6%). All of these findings are consistent with prior research (Loper, 2000; Parker, 1998; Rogers, 1999; 2006).

The current study found that each hacker category was significantly related to all other hacker categories, which was consistent with prior findings (Loper, 2000; Parker, 1998; Rogers, 1999, 2006). The current study found that the internals group had the weakest, though significant, relationship with all of the other behaviors. This finding was consistent with the Guttman-like progression that Hollinger (1998) applied to computer deviant behavior. When applied to the behaviors in the current study, a typical computer deviant progresses through behaviors in an order similar to: script kiddie, cyberpunk, password cracker, old guard hacker. This order was established based on the development of a technical skillset, as an individual advanced up the Guttman-like progression, their technical skills increased. This model also allowed for apprenticeship. The computer deviants farther through the progression assisted new

computer deviants below them. Internal computer deviant behavior is independent of this progression as it was contingent on the computer deviant's occupation (Burns et al., in-press; Rogers, 1999; 2006).

Previous research on script kiddie computer deviant behavior proposed that the behavior would be associated with excitement/entertainment and peer recognition (Loper, 2000; Parker, 1998; Rogers, 1999; 2006). The current study found that script kiddie computer deviant behavior was only marginally associated with addiction motivation. Within the predictive model, addiction only explained 4% (R_L^2) of the variance. The effect of including addiction motivation as a predictor of determining whether a respondent was a script kiddie or non-script kiddie had no effect on the predictive model due to the small number of non-script kiddies (n = 22).

The current study differed from prior research in that it found no support for excitement/entertainment nor peer recognition motivations related to script kiddie computer deviant behavior. There were several possible explanations for these differences. One was that the current study only surveyed individuals over the ages of 19. Prior research suggested that script kiddies typically were in a younger demographic, often being teenagers less than 19 years old (Loper, 2000; Rogers et al., 2006). It was possible that these younger script kiddies, who may be seeking the peer recognition to enter the hacker subculture, were simply not eligible to fill out the survey. Another explanation was that of the computer deviant behaviors, the study found that while 81% identified with script kiddie behaviors, only 4.2% reported *only* participated in script kiddie behaviors. It was possible that there was too much overlap, and other significant relationships were unable to be detected. Lastly, because 81% identified as script kiddies, the model found it easier to assume that everyone participated in script kiddie behaviors, which

explained why addiction motivation, though found to be significantly related to script kiddie behavior, was not used in the final predictions.

Previous research on cyberpunk computer deviant behavior proposed that the behavior would be associated with excitement/entertainment motivation (Murphy, 2011; Rogers, 1999; 2006). The current study found that cyberpunk computer deviant behavior was significantly related to financial motivation, and marginally related to peer recognition and revenge motivations. Within the predictive model, the addition of these variables explained 9% (R_L^2) of the variance. The effect of including financial, peer recognition, and revenge motivations as predictors of determining whether a respondent was a cyberpunk or non-cyberpunk improved the accuracy of the model predictions by 12%.

The current study differed from prior research in that it found no support for excitement/entertainment motivation, but instead found strong support for financial motivation and marginal support for peer recognition and revenge motivations. There were several possible explanations for these differences. One possible explanation was that cyberpunk computer deviant behavior was a step up the Guttman-Like progression for computer hackers from script kiddies, and differs from script kiddies through a refinement of motivation (Hollinger, 1998). Parker (1998) and Rogers (1999) first defined the category as the group of hackers out to cause damage. Perhaps, when a computer deviant progressed into cyberpunk behaviors, they abandoned the pointless, excitement driven, script kiddie behavior for a cold, calculated, and malicious cyberpunk behavior. A strong financial motivation could also be interpreted as simply the changing in priorities as these individuals age and advance through the Guttman-like progression (Hollinger, 1998). As individuals mature out of adolescence into early adulthood, money becomes an increasingly important commodity. Parsimony might suggest that the

maturation of script kiddies into cyberpunks occurs at a similar time, and could explain this financial motivation. Cyberpunk may also be motivated to cause financial damage as opposed to making money for themselves. Prior research could support this conclusion, as cyberpunks have specifically targeted institutions like Bank of America© and PayPal© (Mansfield-Devine, 2011; Murphy, 2011).

Prior literature could also support the peer recognition motivation for cyberpunks. Cyberpunks were also known to leave a signature, or claim ownership for an attack. Groups like Anonymous and Lulzsec have *YouTube* videos and *Twitter* accounts where the boast about their successful malicious accomplishments (Mansfield-Devine, 2011; Murphy, 2011). Lastly, a final factor to explain these differences was that though 50% of respondents identified with cyberpunk behaviors, no respondents reported only participating in cyberpunk behaviors. It was possible that there was too much overlap, and other significant relationships were unable to be detected.

Previous research on password cracker computer deviant behavior proposed that the behavior would be associated with addiction, excitement/entertainment, and power/status/ego motivations (Loper, 2000; Turgeman-Goldschmidt, 2005; Hashcat, 2013). The current study found that password cracker computer deviant behavior was significantly related to addiction motivation. Within the predictive model, addiction only explained 6% (R_L^2) of the variance. The effect of including addiction motivation as a predictor of determining whether a respondent was a password cracker or non-password cracker had no effect on the predictive model due to the small number of non-password crackers (n = 25).

The current study differed from prior research in that it found no support for excitement/entertainment motivation, but did find strong support for addiction motivation. There were several possible explanations for these differences and similarities. In relation to the finding

of a strong addiction motivation, it had been presented in prior research that some computer deviants approached password cracking as if it was a game (Hashcat, 2013). At DEFCON there were yearly password cracking competitions "Crack Me If You Can" in which individuals could compete to see how many passwords they can crack (Hashcat, 2013; McQuade, 2009). Prior literature supported the finding of an addiction motivation related to password cracking through the behavior being treated like a game (Hashcat, 2013). In relation to the differences found in the current study, one possible explanation was that of the computer deviant behaviors, the study found that while 79% identified with password cracker behaviors, only 2.5% reported *only* participating in password cracker behaviors. It was possible that there was too much overlap, and other significant relationships were unable to be detected. It could also be possible that because 79% identified as password crackers, the model found it easier to assume that everyone participated in password cracker behaviors, which explained why addiction motivation, though found to be significantly related to password cracking behavior, was not used in the final predictions.

Prior research suggested that internal computer deviant behavior was motivated by money and revenge (Burns et al, in-press; Rogers, 1999, 2006). The current study found that internal computer deviant behavior was significantly related to financial motivation and peer recognition motivations. Within the predictive model, the addition of these variables explained 6% (R_L^2) of the variance. The effect of including financial and peer recognition motivations as predictors of determining whether a respondent was an internal or non-internal improved the accuracy of the model predictions by 12%. Prior research supported the finding of a financial motivation with internal computer deviant behavior (Burns et al., in-press).

The current study differed from prior research in that it found additional strong support for peer recognition motivation, and no support for a revenge motivation. There were several possible explanations for these similarities and differences. The peer recognition among internals could be related to the relationships an internal had with his/her co-workers or peers. The prior literature suggested that internal computer deviant behavior often resulted from the perception being treated unfairly (Burns et al., in-press; Rogers, 1999; 2006). It was possible that it was not the unfair treatment itself, but the shared perception of unfair treatment amongst co-workers or peers that motivated internal computer deviant behavior. This could also explain the lack of support for a revenge motivation. It was possible that the peer recognition of their colleagues and financial motivations outweighed the input revenge had on participating in internals computer deviant behavior. Another factor to consider was that in the current study 50% identified with internal behaviors, but only 1.7% reported *only* participating in internal behavior. It was possible that there was too much overlap, and other significant relationships were unable to be detected.

Prior research suggested that old guard hacker computer deviant behavior was motivated by curiosity (Best, 2003; Holt & Kilger, 2008; Kilger et al., 2004; Loper, 2000, Rogers, 1999; 2006; Schell & Dodge, 2002; Schell & Martin, 2004; Taylor et al. 2006). The current study found that old guard hacker computer deviant behavior was significantly related with an addiction motivation. Within the predictive model, addiction explained 11% (R_L^2) of the variance. The effect of including addiction motivation as a predictor of determining whether a respondent was old guard hacker or non-old guard hacker had no effect on the predictive model due to the small number of non-old guard hackers (n = 28).

The current study differed from prior research in that it found no support for curiosity motivation related to old guard hacker computer deviant behavior, but did find strong support for

addiction motivation. There were several possible explanations for these differences. Prior research suggested that old guard hackers typically were in an older demographic, often being members of the original computer boom in the 1970s and 1980s (Loper, 2000; Rogers, 1999). It is possible that old guard hackers do not congregate on the websites where the survey was solicited. Another explanation was that of the computer deviant behaviors, the study found that while 77% identified with old guard hacker behaviors, only 0.8% reported *only* participating in old guard hacker behaviors. It was possible that the motivations of true old guard hackers were missed as the sample had significant overlap between the computer deviant behaviors. Lastly, because 77% identified as old guard hackers, the model found it easier to assume that everyone participated in old guard hacker behaviors, which explained why addiction motivation, though found to be significantly related to old guard behavior, was not used in the final predictions.

Prior research suggested there were more male computer deviants than females (Holt & Kilger, 2008; Jordan & Taylor, 2004; Loper, 2000; Mann & Sutton, 1998, Rogers 1999; 2006; Turgeman-Goldschmidt, 2005). The current study found that sex of the respondent being male was marginally related to script kiddie, cyberpunk, and old guard hacker computer deviant behaviors. Within the script kiddie predictive model, sex of the respondent being male explained 4% (R_L^2) of the variance. The effect of including sex of the respondent being male as a predictor of determining whether a respondent was a script kiddie or non-script kiddie was so small that the final model ignored sex of the respondent entirely and simply guessed everyone participated in script kiddie computer deviant behavior. Within the cyberpunk predictive model, sex of the respondent being male explained 2% (R_L^2) of the variance. The effect of including sex of the respondent being male as a predictor of determining whether a respondent was a cyberpunk or non-cyberpunk improved the accuracy of the model predictions by 8.7%. Within the old guard

hacker predictive model, sex of the respondent being male explained 3% (R_L^2) of the variance. The effect of including sex of the respondent being male as a predictor of determining whether a respondent was an old guard hacker or non-old guard hacker was so small that the final model ignored sex of the respondent entirely and simply guessed everyone participated in old guard hacker computer deviant behavior.

The current study differed from prior research in that it found support that sex of the respondent being male related to whether the respondent was a computer deviant. Sex of the respondent being male was found to only be related to script kiddie, cyberpunk, and old guard hacker computer deviant behaviors. There was no support in the current study that sex of the respondent being male was related to password cracking or internal computer deviant behaviors. One possible explanation for this is that these two categories of computer deviant behavior are the most specific within the literature (Burns et al., in-press; Turgeman-Goldschmidt, 2005; Hashcat, 2013, Loper, 2000; Rogers, 1999; 2006). Password crackers are argued to crack passwords because they treat it like a game (Hashcat, 2013). It was possible that both sexes were equally represented in this behavior given its addictive and competitive nature (Hashcat, 2013; McQuade, 2009). Internals were tied specifically to their employment (Burns et al., in-press). It was possible that both sexes were equally represented in this behavior because both sexes were equally represented within the workforce in roles where internal computer deviant behavior could occur.

The current study also differed from prior research in that it found no support for any of the computer deviant behaviors being related to curiosity or excitement/entertainment motivations. One possible explanation for this finding was the small sample size and where the sample was obtained from. It was possible that inclusion of more respondents could have made

an impact on this variable's influence. It was also possible that, should any potential respondents have been motivated by these variables, they did not view the current study's solicitation at the time of its posting.

LIMITATIONS

The first limitation to discuss was the removal of the power/status/ego scale. The OMEIS scale was developed by Marcia (1993) was a 64 item, 5-point Likert scale and was modified to include only the items directly relevant to the concept being measured and was reduced to 10 items. After modification, the scale had a low Chronbach's alpha score ($\alpha = .225$) which indicated that the scale was not measuring one latent variable and that the scale was modified in a way that decreased its reliability. Principal factor analysis with varimax rotation was performed on the 10 items from the OMEIS. With a cutoff of .30 for inclusion of a variable in interpretation of a factor, all 10 items were deemed related to factors based on their acceptable communality values. Five factors had an eigenvalue of 1.0 or greater, meaning there were a total of five factors being measured by the modified scale: Factor 1 explained 17.7%, Factor 2 explained 14%, Factor 3 explained 13%, Factor 4 explained 11%, and Factor 5 explained 10% of the variance in the dataset. Overall, the eigenvalues suggested there were probably 4 to 5 factors. Potential relationships between a power/status/ego motivational factor and the included computer deviant behaviors may have been missed entirely. It is recommended that future studies include a stronger scale, or included the entire instrument of Marcia (1993) to measure this variable.

A second limitation involves the overlap of the computer deviant behaviors. 90% (n = 101) of the respondents who did identify as computer deviant (n = 112), reported participating in two or more behaviors. This overlap may have skewed the motivational influences on any one computer deviant behavior, although it was expected based on the Guttman-like progression

presented by Hollinger (1998), future studies may want to analyze respondents who reported participating in only one category separately and increase the sample size to get more variability in the data.

A third limitation involved the removal of several computer deviant behavior categories, including pirates, cyberterrorists, and hacktivists, as well as the ideological motivational factor. Piracy was removed because it was both a behavior that used a computer as a tool for theft (as opposed to a computer as a target) and that the behavior is rather marginalized (Rogers, 2006). Cyberterrorists and hacktivists and their related ideological motivation were removed because of tautological reasons. The categories were defined by their motivation, not by their behaviors. It would be impossible to separate these classifications of computer deviant behavior from their motivation, meaning an analysis of this type of hacker could not be conducted in the current study. Future studies may want to include these variables, to analyze them in congruence with those presented in the current study.

A fourth limitation the sample size and age. The initial study intended to obtain 300 respondents, however the final sample size was only 120 respondents. These respondents were also intentionally solicited on websites where hacking was commonly discussed and promoted. The sample was not representative of all computer deviants, only the individuals who were on the chosen sites at the time of solicitation. Future studies may wish to expand their sampling to include, not only non-computer deviants, but methods of gaining access to computer deviants who may not be members of the hacker community or subculture. Future studies may also want to include respondents under the age of 19 to identify computer deviants in the first stage of the Guttman-like progression (i.e., script kiddies).

CHAPTER 7

CONCLUSION AND RECOMMENDATIONS

The current study, comparable with previous research, found most computer deviants were engaged in multiple types of computer deviant behavior; in fact, they may be more likely to participate in additional computer deviant behaviors if they already participate in one. In addition, the possibility of a predictive risk model for each computer deviant behavior including multiple motivation variables and the sex of the respondent was considered. Each behavior was related to some form of motivation, script kiddie, password cracker, and old guard hacker computer deviant behaviors were all found to be related to an addiction motivation. Cyberpunks were found to be related to financial, peer recognition, and revenge motivations, and internal computer deviant behaviors were found to be related to financial and peer recognition motivations. Script kiddie, cyberpunk, and old guard hacker computer deviant behaviors were also found to be related to the sex of the respondent being male.

Essentially, computer deviant behaviors are all interlinked, share common motivations, and had slightly more males than females participating in the behaviors. By better understanding the relationship between computer deviant behaviors and addiction, curiosity, excitement/entertainment, money, peer recognition, revenge, and sex, researchers may begin to understand the differences between individuals who are at high-risk and low-risk for participating in computer deviant behaviors. By understanding who is at high-risk for computer deviant behaviors, researchers and law enforcement professionals may be able to prevent some of the severe damage some of these computer deviant behaviors can cause, such as in the case of Bank of America©. Future research should assess whether individuals who are motivated by these factors are more likely to initial computer deviant behavior. The majority of research

focuses on computer deviant behaviors as a broad category including multiple types, or only addresses a small number of motivational factors, the current study illustrates that computer deviant behaviors have significant overlap but varying motivational factors, and future research should be conducted to better understand who is at risk for engaging in computer deviant behavior, what motivates them, and how the criminal justice system should handle these individuals.

REFERENCES

Akers, R. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston, MA: Northeastern University Press.

Armitage, J. & Roberts, J. (2002). *Living with cyberspace*. New York, NY: Continuum.

Best, K. (2003). The hacker's challenge: Active access to information, visceral democracy and discursive practice. *Social Semiotics, 13*(3), 263-282.

Beveren, J. (2001). A conceptual model of hacker development and motivations. *Journal of E-Business, 1*(2), 1-9.

Burns, A., Posey, C., Roberts, T., & Hightower, R. (in-press). The insider threat: A multifactor examination of the deterrents to and motivators of employees' computer abuse. In Seigfried-Spellar, K., & Lanier, M. (Eds.), *Essential readings in cybercrime theory and policy* (pp. 59-74). United States: Cognella, Inc.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Reviews, 44*(4), 599-608.

Council of Europe. (2007). *Cyberterrorism – the use of the Internet for Terrorist Purposes*. Strasbourg Cedex, France: Council of Europe Publishing.

Chao, C., Yu, T., and Cheng, B. (2013). Modeling predictors of adolescents' attitude towards cyber lives index. *Malaysian Journal of Library & Information Science, 18*(1), 87-104.

Eisenberger, R., Lynch, P., Aselage, J., & Rohdieck, S. (2004). Who takes the most revenge? Individual differences in negative reciprocity norm endorsement. *Personality and Social Psychology Bulletin, 30*(10), 1-13.

Field, A. (2005). *Discovering statistics using spss* (2nd ed.). London, UK: SAGE Publications Ltd.

Gordon, S., & Ma, Q. (2003). Convergence of virus writers and hackers: Fact or fantasy? *Symantec*. Cupertino, CA.

Greenwald, G., & Ackerman, S. (2013). How the NSA is still harvesting your online data. *The Guardian*.

Hacker [Def. 3.] (1976) *Oxford English Dictionary,* Retrieved September 24, 2013, from http://www.oed.com/view/Entry/83045?rskey=rBOq05&result=is...

Hagan, F. (2010). *Research methods in criminal justice and criminology* (8th ed.). New York: Allyn & Bacon.

Hashcat. (2013). Hashcat advanced password recovery. *Hashcat.net*. Retrieved October 13, 2013, from http://hashcat.net/wiki/

Hatamleh, H. (2012). A review and comparing of all hacking techniques and domain name system method. *Contemporary Engineering Sciences, 5*(5), 239-250.

Hollinger, R. (1988). Computer hackers follow a guttman-like progression. *Phrack Inc, 2*(22), 1-3.

Hollinger, R., & Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws*. *Criminology, 26*(1), 101-126.

Holt, T. J. (2007). Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*, 171-198.

Holt, T. J. (2009). The attack dynamics of political and religiously motivated hackers. *Cyber Infrastructure Conference*. New York, NY

Holt, T., & Kilger, M. (2008, April). Techcrafters and makecrafters: A comparison of two populations of hackers. *Worldwide Observatory of malicious Behaviors and Attack Threats Conference*. Amsterdam, Netherlands.

IC3. (2012). *Internet Crime Report 2011*. National White Collar Crime Center (NW3C).

IC3. (2013). *Internet Crime Report 2013*. National White Collar Crime Center (NW3C).

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyber wars.* London, UK: Routledge.

Kashdan et al. (2009). The curiosity and exploration inventory-ii. Development, factor structure, and psychometrics. *Journal of Research in Personality, 43*, 987-998.

Kilger, M., Arkin, O., & Stutzman, J. (2004). Profiling. In The Honeypot Project (Ed.), *Know your enemy: Learning about security threats*. Addison-Wesley Professional. Retrieved from http://old.honeynet.org/book/chp16.pdf

Kim, S., Wang, Q., & Ullrich, J. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66-73.

Kirwan, G., & Power, A. (2012). *The psychology of cyber crime*. Hershey, PA: Information Science Reference.

Loper, K. (2000). *The criminology of computer hackers: A qualitative and quantitative analysis*. Unpublished dissertation, Michigan State University, East Lansing, Michigan.

Lu, C., & Jen, W. (2010). A historical review of computer user's illegal behavior based on containment theory. *Journal of Software, 5*(6), 593-599.

Mann, D., & Sutton, M. (1998). Netcrime: More change in the organization of thieving. *British Journal of Criminology, 38*(2), 201-229.

Mansfield-Devine, S. (2011). Anonymous: Serious threat or mere annoyance? *Network Security, 2011*(1), 4-10.

Maras, M. (2012). *Computer forensics: Cybercriminals, laws, and evidence.* Sudbury: Jones & Bartlett Learning

Marcia, J. (1993). Development and validation of ego-identity status. *Journal of Personality and Social Psychology, 3*, 551-558.

Maxwell, A. (2013). The very unofficial dummies guide to Scapy. Retrieved from http://itgeekchronicles.co.uk. 1-47.

McBrayer, J. & Seigfried-Spellar, K. (2013, March*). Exploiting the Digital Frontier: Hacker Typology and Motivation*. Presentation given at 42nd Annual Southwest Decision Sciences Institute Conference, Albuquerque, NM.

McQuade, S. (2009). *Encyclopedia of Cybercrime*. Westport, Connecticut: Greenwood Press.

Meerkerk, G., Eijnden, R., Vermulst, A., and Garretsen, H. (2009). The compulsive internet use scale (CIUS): Some psychometric properties. *CyberPsychology & Behavior, 12*(1), 1-6.

Murphy, S. (2011). Agents provocateurs. *New Scientist, 211*(2829), 46-49.

Nikitina, S. (2012) Hacker as trickster of the digital age: Creativity in hacker culture. *The Journal of Popular Culture, 45*(1), 133-152.

Nowak, G. (2011). Taming the cyber frontier. *Computer Fraud & Security, 12*, 5-9.

Richardson, R. (2011). *15th Annual 2010 / 2011CSI computer crime and security survey*. Computer Security Institute.

Richmond, J. (2012). Evolving battlefields does stuxnet demonstrate a need for modifications to the law of armed conflict? *Fordham International Law Journal, 35*, 842-893.

Rogers, M. (1999, February). The psychology of hackers: A new taxonomy. *RSA World Security Conference*. San Jose, CA.

Rogers, M., Smoak, N., & Liu, J. (2006). Self-reported computer deviant behavior: A bit-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior, 27*, 245-268.

Rogers, M. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*, 97-102.

Rogers, M. (personal communication, October 24th 2012).

Sample, T. & Swetnam, M. (2012). *#Cyberdoc No Borders – No Boundaries*. Arlington, VA: Potomac Institute Press

Schell, B., & Dodge, J. (2002). *The hacking of America: Who's doing it, why, and how*. Westport, CT: Quorum Books.

Schell, B. & Martin, C. (2004). *Cybercrime*. Santa Barbara, CA: ABC CLIO Inc.

Shachaf, P., & Hara, N. (2010). Beyond vandalism: Wikipedia trolls. *Journal of Information Science, 36*(3), 357-370.

Smyslova, O., & Voiskounsky, A. (2009). Usability studies: To meet or not to meet intrinsic motivation. *PsychNology Journal, 7*(3), 303-324.

Song, I., Larose, R., Eastin, M., & Lin, C. (2004). Internet gratification and internet addiction: On the uses and abuses of new media. *CyperPsychology & Behavior, 7*(4), 384-394.

Taylor, P. (1999). *Hackers: Crime in the digital sublime*. London, UK: Routledge.

Taylor, R., Caeti, T., Loper, K., Fritsch, E., Liederbach, J. (2006). *Digital Crime and Digital Terrorism*. Upper Saddle River, NJ: Pearson Prentice Hall.

Turgeman-Goldschmidt, O. (2005). Hacker's accounts: Hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8-23.

Voiskounsky, A. & Smyslova, O. (2003). Flow-based model of computer hackers' motivation. *CyberPsychology & Behavior, 6*(2), 171-180.

Wade, C. Aldridge, J., Hopper, L., Drummond, H., Hopper, R., & Andrew, K. (2011). Hacking into the hacker: Separating fact from fiction. In Holt, T. (Ed.), *Crime on-line* (pp. 29-55). Durham, NC: Carolina Academic Press.

Williams, M. (2006). *Virtually criminal crime, deviance, and regulation online.* London, UK: Routledge.

Wikström, P. (2006). Linking individual, setting, and acts of crime: Situational mechanisms and the explanation of crime. In Schmallenger, F. & Pittaro, M. (Eds.) *Crimes of the Internet*. Cambridge, UK: Cambridge University Press.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 58*(4), 64-74.

Yamauchi, K., & Templer, D. (1982). The development of a money attitude scale. *Journal of Personality Assessment, 46*(5), 522-528.

Appendix

December 18, 2013

Office for Research

Institutional Review Board for the Protection of Human Subjects

THE UNIVERSITY OF ALABAMA RESEARCH

John McBrayer
Department of Criminal Justice/Sociology
College of Arts & Sciences
The University of Alabama

Re: IRB # 13-OR-072-R1 "Motivation of Computer Behaviors"

Dear Mr. McBrayer:

The University of Alabama Institutional Review Board has granted approval for your proposed research

Your renewal application has been given expedited approval according to 45 CFR part 46. You have also been granted the requested waiver of written documentation of informed consent. Approval has been given under expedited review category 7 as outlined below:

(7) Research on individual or group characteristics or behavior (including, but not limited to, research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices, and social behavior) or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.

Your application will expire on December 17, 2014. If your research will continue beyond this date, complete the relevant portions of the IRB Renewal Application. If you wish to modify the application, complete the Modification of an Approved Protocol Form. Changes in this study cannot be initiated without IRB approval, except when necessary to eliminate apparent immediate hazards to participants. When the study closes, complete the appropriate portions of the IRB Study Closure Form.

Please use reproductions of the IRB-stamped consent form to obtain consent from your participants.

Should you need to submit any further correspondence regarding this proposal, please include the above application number.

Good luck with your research.

Sincerely,

[redacted]

Carpantato T. Myles, MSM, CIM, CIP
Director of Research Compliance & Research Compliance Officer
Office of Research Compliance
The University of Alabama

358 Rose Administration Building
Box 870127
Tuscaloosa, Alabama 35487-0127
(205) 348-8461
FAX (205) 348-7189
TOLL FREE (877) 820-3066