Factors Encouraging and Deterring Illegal Computer Hacking: Replicating and Extending Young and Zhang's Treatise on Illegal Computer Hacking

Dissertation Manuscript

Submitted to Northcentral University

Graduate Faculty of the School of Business
in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

Kevin Crouse

San Diego, California
March 2019

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

Approval Page

Factors Encouraging and Deterring Illegal Computer Hacking: Replicating and Extending Young and Zhang's Treatise on Illegal Computer Hacking

By

Kevin Crouse

Approved by the Doctoral Committee:

DocuSigned by: Garrett Smiley 458DFCD61B5A4C7...	Ph.D.	04/18/2019 | 17:22:06 MST
Dissertation Chair: Garrett Smiley	Degree Held	Date
DocuSigned by: Brian M. Allen 4592EFB246F44EF...	DBA	04/19/2019 | 07:45:32 MST
Committee Member: Brian M. Allen	Degree Held	Date
DocuSigned by: Marie Bakari 8F10EBB525784DB...	DBA, MBA	04/19/2019 | 14:53:07 MST
Committee Member: Marie Bakari	Degree Held	Date

Abstract

From 2000 to 2016 computer hacking has increased to epidemic proportions. This quantitative replication study seeks to examine Young and Zhang's study of factors that encouraged and deterred illegal computer hacking behavior. The proliferation of the internet has increased the environment for hacking. In addition, there has been an expansion in hacking activities beyond fun or profit and has become a platform for social issues. The purpose of this quantitative non-experimental replication study was to analyze hacker behavior through the lens of general deterrence theory, social bond theory, and social learning theory in an online setting. The constructs of punishment certainty, commitment, involvement, and belief demonstrated significant positive relationships to an individual's propensity to engage in illegal hacking. This is counter-intuitive to both general deterrence theory and social bond theory. These findings demonstrate that deterring hacking attacks through technical means or punishment alone are ineffective. Upon examination, the picture of who becomes a hacker is very different from the profile developed by Young and Zhang. It includes both men and women who subscribe to generally conceived societal norms. These results further indicate that general deterrence theory and social bond theory have limited, if any, application in reducing engagement in illegal computer hacking. This is very different from other studies of criminality that have shown increased punishment or social connectedness generally reduce illegal behavior.

Acknowledgements

I would like to thank my wife Ginger and children Caleb, Katie and Kira for all of the support and encouragement they have giving me while completing this work. Undertaking doctoral studies is a huge commitment, which often conflicts with family life and activities. Throughout this entire process, my family never faltered in their support and always understood the time commitments and pressures that this process required. I would also like to thank Dr. Roger Whitlow and Dr. Gary Foster for their insight, encouragement, and editorially review. I hope my future academic endeavors will honor the spirit of scholarship, mentorship, and friendship that they have freely offered to me throughout my life. Finally, I would like to thank my committee, Dr. Garrett Smiley, Dr. Brain Allen, and Dr. Marie Bakari, for their efforts and assistance completing this work.

If it were not for my wife, Ginger Crouse, I would have never pursued or been able to complete a doctorate and this research. I dedicated the work to her.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

The Federal Bureau of Investigations reported the cost of overall computer crime has risen to over 1.33 billion dollars a year (FBI, 2016). Additionally, between the years 2013 and 2016, hacking related breaches grew by 78% (ITRC, 2017), indicating that computer hacking is epidemic. This research re-examined Young and Zhang's 2007 study, which focused on factors that encourage and deter illegal computer hacking. Since this 2007 study, the landscape and environment for hacking emerged as a worldwide issue, via a proliferation of the Internet. Between June of 2007 and June of 2017, worldwide Internet users increased from 1.173 billion to 3.885 billion (Internet World Stats, 2017). This growth makes it possible to replicate this study in an online environment, enabling this study to reach a larger population pool.

Despite significant advances in defensive information-security technologies and government-enacted criminal penalties, hackers continue to misappropriate information, damage computer networks, deface websites, or deny authorized users access to online services (Collister, 2014; Prislan, 2016). In responding to this threat, some governments have enacted laws criminalizing this behavior, relying on deterrence to curb hacking activities (Hui, Kim, & Wang, 2017), instead of seeking to gain an understanding of the factors that compel a person to become a computer hacker (Chatterjee, Sarker, & Valachich, 2015). However, illegal computer hacking continues. According to the cyber-security firm Fortinet, the second quarter of 2017 saw 184 billion computer exploit detections and 62 million malware detections (Fortinet, 2017). Additionally, the Equifax breach compromised the personally identifiable information of over 145 million people (Fortinet, 2017).

An early hacker theorist contended that hackers were primarily technological practitioners, who manipulated systems to improve technology or in the pursuit of knowledge

(Levy, 1984). In the mid-1980's, the study of hackers evolved into the cracker-criminal mindset (Levy, 1984), and theories of deviant behavior and criminology began to be applied (Hafner & Markoff, 1995). The theories of criminal and deviant behavior are still prevalent and ingrained in the general deterrence models for dealing with hacker behavior by many world governments (Computer Fraud and Abuse Act of 1984, 1986; Computer Misuse Act of 1990; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 2002; Xiang, 2013; Young & Zhang, 2007). General-deterrence theory posits that harsh penalties deter undesirable actions (Beccaria, 1775); therefore, depriving someone of freedom or fining them will deter them from committing unwanted acts (*United States of America v. Dennis Owen Collins, et-al.*, 2014; Xiang, 2013; Young & Zhang, 2007).

As an example, a person convicted of second-degree murder, on average, will spend eight years in prison in the United States, but a hacker who defaces a website of a nationally regulated bank can receive a 25-year sentence, without the chance for parole (*United States of America v. Dennis Owen Collins, et-al.*, 2014). In addition, organizations failing to provide adequate protection of the personally identifiable information of individuals held within their systems can incur fines and penalties (EU-GDPR, 2017). These penalties have trans-national boundaries and can reach up to 4% of an entity's general revenues or 20 million Euros, whichever is greater (EU-GDPR, 2017).

As hacker rationale matured, the focus shifted to the counter-culture open-internet movement, which espoused that all information should be free and open to everyone (Levy, 1984). This signaled a change from the idea that hackers operated alone and began examining hacker culture as social and political movements (Collister, 2014).

Statement of the Problem

The general problem is that since 2007 illegal computer hacking has continued to increase (Farrell & Birks, 2018; Levi, 2017). Between 2013 and 2016, illegal computer breaches increased in the United States by 78% (ITRC, 2017). Researchers disagree on the degree to which hacking behaviors correlate with economic incentives and deterrence certainties (Hui et al., 2017), or socio-cultural motivators (Madarie, 2017; Udris, 2016). If the trend demonstrated by the 2011 through 2016 Identity Theft Resource Center surveys continue, hacking breaches will increase between 12% and 40% per year (ITRC, 2017) and individuals, corporations, and other organizations will continue to lose billions of dollars (FBI, 2016) or expend millions of dollars on cyber defenses (Wellisz, 2016; Wolff, 2016).

A possible cause of the increase in illegal hacking could be the limited understanding of exactly what factors encourage or discourage hacker behavior; factors such as 1) legal deterrence; 2) social/peer bonds; 3) personal attachment to people generally; 4) interactions with other hackers; 5) intellectual challenge; 6) revenge/retaliation; or 7) financial incentives (Chatterjee et al, 2015; Young and Zhang, 2007). Future study of these seven behavioral factors should illuminate more clearly the true motives behind illegal hacking (Chatterjee et al., 2015; Madarie, 2017). In particular, future research is needed to examine the relationships that exist between illegal hacking activity and punishment, the social bonds of commitment, belief, involvement, attachment, and the relationship that exists between interactions with other hackers that act as enablers or detractors for participating in this illegal activity (Young & Zhang, 2007).

Purpose of the Study

The purpose of this quantitative correlational non-experimental replication study was to draw together the independent variables of 1) punishment severity; 2) punishment certainty; 3) attachment to other socially conforming individuals; 4) commitment to actions deemed acceptable by society; 5) involvement a person has with activities deemed acceptable by society; 6) belief (the degree to which an individual accepts the rules of society); and 7) interactions with other hackers to the dependent variable of self-reported engagement in illegal hacking. The study group consists of individuals that self-identify as hackers on the Internet. Online study participant identification occurred through online posts in the DefCon, LulzSec, and Anonymous Facebook and Twitter pages; as well as open Facebook and Twitter pages developed for this survey. Using the G*Power calculator for a z-test logistic regression, a total sample size of 578 was determined to be the necessary minimal sample size at the minimally accepted power level of 80%, or .80 with a .05 alpha level, which is the standard level for eliminating Type I errors (Bennet, Briggs, & Triola, 2014; Houser, 2007). Testing Young and Zhang's 2007 study in an online setting contributes to current research by offing a fresh analysis of the factors tested over a decade ago and provides results from a larger and more disbursed online population.

Theoretical Framework Overview

The framework for this study examined the self-reported engagement in illegal hacking by individuals from the constructs of general-deterrence theory, social-bond theory, and social-learning theory, as utilized in Young and Zhang (2007), from whose study this research is replicating. Early cultural, economic, and political theorists, such as Karl Marx and Friedrich Engels, argued that people moved to action to improve their economic condition or correct the political injustices they perceived in society (Buechler, 1995; Marx & Engels, 1883). In contrast, new social-movement theory motivators, which are a conglomeration of several theories that include general-deterrence theory, social-bond theory, and social-learning theory, view the actions of individuals, in this case hackers, in society through individual or group identity and social connectivity (Udris, 2016), lifestyle, and cultural development (Buschler, 1995; Collister, 2014), as well as through economic and political factors (Collister, 2014; Kendall, 2006). This modernist view, as theorized by Buschler (1995) and Kendall (2006), casts actions as less dependent on personal economics, such as hacking for financial gain (Hui et al, 2017), or political condition, as theorized by Marx and Engels (1883), and more on an individual's search for self-fulfillment (Collister, 2014), attachment with others (Udris, 2016), intellectual challenge, or a general dislike for the intended target (Madarie, 2017).

Conceptually, this study assessed specific variables of three sociological theories. They include 1) the general deterrence theory independent variables of punishment severity and punishment certainty; 2) the social bonding theory independent variables of attachment to other socially conforming individuals, commitment to actions deemed acceptable by society, involvement a person has with activities deemed acceptable by society, belief (the degree to which an individual accepts the rules of society), and 3) the social learning theory independent variable of interaction with others encourages or discourages individuals to engage in self-reported illegal hacking, the dependent variable. For this study, self-reported illegal hacking, or hacker activities, are purposeful actions designed to disrupt the normal operation of information-technology systems. Young and Zhang (2007) focused their attention on these variables and theories in an attempt to explain behavioral factors that deter and encourage illegal hacking.

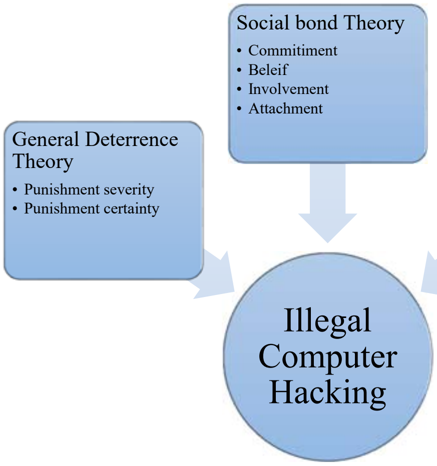

Figure 1. Research Model

Research Questions

The purpose of this study is to test and expand Young and Zhang's analysis of hacker motivations, within the context of general deterrence, social bond, and social learning theories. To achieve this goal, a survey is necessary to answer the following questions:

RQ1. What is the relationship between punishment severity and self-reported engagement in illegal hacking?

RQ2. What is the relationship between punishment certainty and self-reported engagement in illegal hacking?

RQ3. What is the relationship between attachment to other socially conforming individuals and self-reported engagement in illegal hacking?

RQ4. What is the relationship between commitment to actions deemed acceptable by society and self-reported engagement in illegal hacking?

RQ5. What relationship exists between the involvement a person has with activities deemed acceptable by society and self-reported engagement in illegal hacking?

RQ6. What relationship exists between belief, which is the degree to which an individual accepts the rules of society, and self-reported engagement in illegal hacking?

RQ7. What relationship exists between interaction with other hackers and self-reported engagement in illegal hacking?

Hypotheses

The following hypotheses are designed to test these research questions:

H1$_0$. Punishment severity is negatively related to self-reported engagement in illegal hacking.

H1$_a$. Punishment severity is positively related to self-reported engagement in illegal hacking.

H1$_n$. There is no relationship between punishment severity and self-reported engagement in illegal hacking.

H2$_0$. Punishment certainty is negatively related to self-reported engagement in illegal hacking.

H2$_a$. Punishment certainty is positively related to self-reported engagement in illegal hacking.

H2$_n$. There is no relationship between punishment certainty and self-reported engagement in illegal hacking.

H3$_0$. Attachment to other socially conforming individuals is negatively related to self-reported engagement in illegal hacking.

H3$_a$. Attachment to other socially conforming individuals is positively related to self-reported engagement in illegal hacking.

H3$_n$. There is no relationship between attachment to other socially conforming individuals and r self-reported engagement in illegal hacking.

H4$_0$. Commitment to actions deemed acceptable by society is negatively related to self-reported engagement in illegal hacking.

H4$_a$. Commitment to actions deemed acceptable by society is positively related to self-reported engagement in illegal hacking.

H4$_n$. There is no relationship between commitment to actions deemed acceptable by society and self-reported engagement in illegal hacking.

H5$_0$. The involvement a person has with activities deemed acceptable by society is negatively related to self-reported engagement in illegal hacking.

H5$_a$. The involvement a person has with activities deemed acceptable by society is positively related to self-reported engagement in illegal hacking.

H5$_n$. There is no relationship between the involvement a person has with activities deemed acceptable by society and self-reported engagement in illegal hacking.

H6$_0$. Belief, the degree to which an individual accepts the rules of society, is negatively related to self-reported engagement in illegal hacking.

H6$_a$. Belief, the degree to which an individual accepts the rules of society, is positively related to self-reported engagement in illegal hacking.

H6$_n$. There is no relationship between belief, the degree to which an individual accepts the rules of society, and self-reported engagement in illegal hacking.

H7$_0$. Interaction with hackers is positively related to self-reported engagement in illegal hacking.

H7$_a$. Interaction with hackers is negatively related to self-reported engagement in illegal hacking.

H7$_n$. There is no relationship between interaction with hackers and self-reported engagement in illegal hacking.

Nature of the Study

The research sought insight into the engagement motivators affecting the hacker culture. A quantitative study provided an avenue to such knowledge (Cozby & Bates, 2012). The procedures used replicate those of a study on hacking deterrence conducted by Young and Zhang in 2007. This online study utilized the Qualtrics survey tool. Young and Zhang (2007) used the DefCon venue to conduct their original study of hacker motivations because of the lack of hacker mailing lists or the availability of individuals publicly identified as hackers (Young & Zhang, 2007). Since there are no membership lists for hackers, self-identification through social media was the primary method for gaining study participants. At DefCon, Young and Zhang (2007) gathered 155 respondents over the three-day conference. Posts were developed, with survey links, and placed in online hacker and hacktivist forums; like the DefCon user groups, the LulzSec Facebook page, and the Anonymous Facebook and YouTube feed. In addition, Facebook and Twitter pages with links to the survey were deployed. The survey included appropriate disclosures and assent clauses.

The researcher posted the survey online with a disclosure statement preceding the survey and a 'checkbox' with a forward button to ensure agreement by the respondent to complete a survey. This ensured that the participants were aware of the purpose of the study, that only non-identifying information was collected, that their participation was voluntary, and that their responses are anonymous (CITI, 2012).

Young and Zhang did not have a direct instrument to base their survey on, so they created a survey tool by utilizing measurements from several instruments. The independent variables of punishment severity and punishment certainty are based on Grasmick and Dryjak (1980) discussion on the means of measuring these variables. Punishment severity was assessed in general terms, to avoid specifics about penalties and the possibility of perceptions on severity of penalties based on socio-economic status. The social-bonding theory independent variables of attachment to other socially conforming individuals, commitment to actions deemed acceptable by society, involvement a person has with activities deemed acceptable by society, belief (the degree to which an individual accepts the rules of society) are based in Armsden and Greenberg's (1987) Inventory of Parent and Peer Attachment. The independent variable of interaction with other hackers encourage or discourage individuals to engage in self-reported illegal hacking is measured based on Akers, Krohn, Lanza-Kaduce, Radosevich's (1979) instrument to measure social learning and deviant behavior. All independent variables are measured against the dependent variable of self-reported engagement in illegal hacking on a 5-point Likert scale ranging from 'strongly disagree (1)' to 'strongly agree (5)'.

SPSS was used to encode results and conduct appropriate statistical tests. These tests include, but are not limited to, tests of significance, correlation analysis, cross-tabulations, and regression analysis. Descriptive characteristics of study participants were also analyzed.

A quantitative non-experimental replication survey study was chosen so that inferences can be made and results generalized to a greater population. Qualitative research is generally conducted on a circumstance or event; therefore, it is not appropriate for this study (Cozby & Bates, 2012). In addition, most examination of illegal computer hacking is by qualitative case study and examines only a specific event or circumstance. While difficult to examine, assessing motivations generically from a larger population could expand the body of such knowledge by helping confirm and expand the operationalization of behavioral enablers and detractors in the real world.

Significance of the Study

This quantitative non-experimental replication study sought to test and expand Young and Zhang's 2007 study of behavioral factors that encourage and deter illegal computer hacking. This is important to the field of information-security because understating the motivations of those that hack systems is a critical component in IT risk management, threat analysis, and security-incident attribution (Shamsi, Zeadally, Sheikh, & Flowers, 2016). As an example, understanding who is attacking your information, and why they might want that information, can help form a better understanding of the risks faced by an organization and inform choices related to the protective measures needed to defend the organization.

Additionally, in the evolving world of information-security, the concept of active, or offensive, cybersecurity is gaining attention (Neal & Ilsever, 2016). Active Cyber Defense, or Offensive Cyber-Security, is the concept of using hacker tools, such as hack backs, malware deployment, denial of service or distributed denial of service attacks, social engineering, and ransomware against the hackers that attack an organization (Neal & Ilsever, 2016). In relation to this concept, one must understand who is hacking their system in-order to 'hack-back' the hackers, especially when you consider the legal, ethical, and moral dilemmas that can be associated with offensive cyber actions (Harrington, 2014). This understanding of behaviors will become even more important as artificial security intelligence, behavioral analysis, and threat intelligence sharing grow out of their infancy in cybersecurity and become a security driving force (Craig, Shackelford & Hiller, 2015).

This research will help organizations, public and private, come to a better understanding of the shortcomings of static defensive technologies, and the benefits of adaptive behavioral-based defensive strategies. In addition, offensive cyber security requires the understanding of motivations, and end-goals, of hackers to implement the concepts of proportional response (Harrington, 2014). Finally, this study can help entities gain further insight into understanding how they should lobby governments for the enactment of laws, regulations, or programs that will deter hacking. Currently, public and private entities must rely on governments for certain aspects of the protection doctrine. That doctrine, general deterrence (or punishment), may best be understood by all entities in-order to advocate for the continued use or strengthening of the doctrine, or to understand its limitation, as well as other possible solutions to mitigate the continuing damage done by hackers.

Definition of Key Terms

Activism. Activism refers to the concept of directed efforts to bring about change, specifically, social, political, and economic change (Buechler, 1995).

Attachment. Attachment refers to the effective ties one has to others (Hirschi, 1969).

Belief. Belief refers to an individual's commitment to following the rules and norms of society (Young & Zhang, 2007).

Commitment. Commitment is the level of time, energy, effort, or expense one will expend on investing or participating in activities deemed acceptable by society (Becker, 1960).

Culture. Culture refers to the totality of beliefs, attitudes, customs, and norms that distinguishes one group from another, noting that culture can include many groups with similar or complementary interests and espouses a larger and broader set of overarching themes. For example, different hacker groups make up hacker culture, in that they may have different objectives, but use similar methods for achieving their goals (Buechler, 1995; Fuist, 2013).

Cultural development. Cultural development is the process of developing a cultural identity. It is the process that engages community members to build upon their shared cultural experiences (Fuist, 2013).

Group identity. Group identity refers to the shared social characteristics, such as world views, values, and ideology that evolve through membership in a particular group or association (Buechler, 1995; Kendall, 2006).

Hacker. A hacker is a person who uses electronic means to manipulate a system or data (Young & Zhang, 2007).

Hacking. Hacking is the use of electronic means to manipulate systems or data (Young & Zhang, 2007).

Hacktivism. Hacktivism is the use of electronic means to bring about social or societal change through the manipulation of systems or data (Collister, 2014).

Hacktivist. A hacktivist is a person that uses or attempts to use electronic means to bring about social or societal change through the manipulation of systems or data (Hampson, 2012).

Involvement. Involvement refers to the overall commitment of time and effort one expends on doing conventional, or societally accepted, activities (Young & Zhang, 2007)

Individual identity. Individual identity is the beliefs and personality attributions to which the individual self-ascribes (Buechler, 1995).

Attachment. Attachment is the degree to which one ascribes belief, including the degree of "faithful" support for a specific political cause or party (Krips, 2012).

Summary

Even with significant advances in information-systems protection and defenses, hackers are still able to disrupt the legitimate use of technological systems (Scheuerman, 2016). While the original intention of hackers was not criminal, the last three decades have seen an explosion of hacker activities across the globe (FBI, 2016; Xiang, 2013). In response, governments have enacted laws to criminalize this behavior and employ measures to punish hackers (Scheuerman, 2016), instead of seeking an understanding of the motivational factors that cause a person to become a hacker (Drmola, Bastl & Mares, 2015).

For this replication of Young and Zhang's 2007 research into hacker encouragements and deterrents, the research sought, through a quantitative study, to gain insight into this global problem. Much of the research on hackers does not probe behavioral factors (Madarie, 2017). This study sought to gain a deeper understanding of the behavioral factors that influence a person's decision to hack. This understanding is critical for the cyber-defenders of organizations; who must be able to understand and attribute proper behavioral context, if they are to deploy defensive and offensive strategies that are proactive, and not reactive, to current and future cyber threats. To achieve this, the survey instrument allowed for the collection of data to determine what correlations or relationships might exist between or among the study constructs. Conclusions are drawn based on the analysis of the survey data, which, after appropriate statistical tests, will be generalized, to a larger population of hackers.

Chapter 2: Literature Review

The purpose of this quantitative non-experimental replication study was to test Young and Zhang's 2007 study on behavioral enablers and deterrents to engaging in illegal computer hacking. This study provides a fresh analysis of the independent variables of 1) punishment severity; 2) punishment certainty; 3) attachment to other socially conforming individuals; 4) commitment to actions deemed acceptable by society; 5) involvement a person has with activities deemed acceptable by society; 6) belief (the degree to which an individual accepts the rules of society); and 7) interactions with other hackers to the dependent variable of self-reported engagement in illegal hacking. The target population for this study was individuals that self-identify as hackers in an online environment to reach a larger and more disbursed Internet-based population pool.

This literature review was developed to provide an overview and analysis of the concepts associated with hacking literature. These topics included 1) the ethical use of technology; 2) the concepts of activism and movement culture; 3) early and modern concepts of hacking; 4) common hacker tactics and vectors; 5) currently accepted standards in hacker defenses; 6) and a brief discussions of the sociological theories to hackers in the literature. Additionally, the specific theories of general deterrence, social-bonding, and social learning applied in the original study are reviewed. The literature search strategy includes three main groupings. The first group was a broad search related to the topic through online library searches. It included searches of journal articles, dissertations, and other materials related to social movement theories, general-deterrence theory, social-bond theory, social-learning theory, studies of hackers, ethical technology uses, cyber-crime, defensive strategies, and research methods. The libraries used were both Northcentral University and Illinois State University's Milner Library.

Once this was completed, and the hypothesis formed, the research direction changed to search online and the aforementioned libraries for peer-reviewed work on the specific hypothesis. The third group consists of researching online through industry and government sources for information related to the most current state of hacker/hacktivist activities or movements. Time parameters were initially not defined so that a large view of related material could be assessed and key themes developed. After the key themes were developed, searching was limited to the previous five years, based on the dissertations initial start date and works that were considered seminal or of high importance remained. As time progressed literature review sections were updated to as many sources as found within the past five years.

Conceptual Framework

The framework for this study examined the self-reported engagement in illegal hacking by individuals from the constructs of general-deterrence theory, social-bond theory, and social-learning theory, as utilized in Young and Zhang (2007), from whose study this research is replicating. Early cultural, economic, and political theorists, such as Karl Marx and Friedrich Engels, argued that people moved to action to improve their economic condition or correct the political injustices they perceived in society (Buechler, 1995; Marx & Engels, 1883). In contrast, new social-movement theory motivators view the actions of individuals, in this case hackers, in society through individual or group identity and social connectivity (Udris, 2016), lifestyle, and cultural development (Buschler, 1995; Collister, 2014), as well as through economic and political factors (Collister, 2014; Kendall, 2006). This modernist view, as theorized by Buschler (1995) and Kendall (2006), casts actions as less dependent on personal economics, such as hacking for financial gain (Hui et al, 2017), or political condition, as theorized by Marx and Engels (1883), and more on an individual's search for self-fulfillment (Collister, 2014), attachment with others (Udris, 2016), intellectual challenge, or a general dislike for the intended target (Madarie, 2017).

Conceptually, this study assessed whether: 1) the general deterrence theory independent variables of punishment severity and punishment certainty; 2) the social bonding theory independent variables of attachment to other socially conforming individuals, commitment to actions deemed acceptable by society, involvement a person has with activities deemed acceptable by society, belief (the degree to which an individual accepts the rules of society); and 3) the social learning theory independent variable of interaction with other hackers encourage or discourage individuals to engage in self-reported illegal hacking, the dependent variable. For this study, self-reported illegal hacking, or hacker activities, are purposeful actions designed to disrupt the normal operation of information-technology systems. Young and Zhang (2007) focused their attention on these variables and theories in an attempt to explain behavioral factors that deter and encourage illegal hacking.

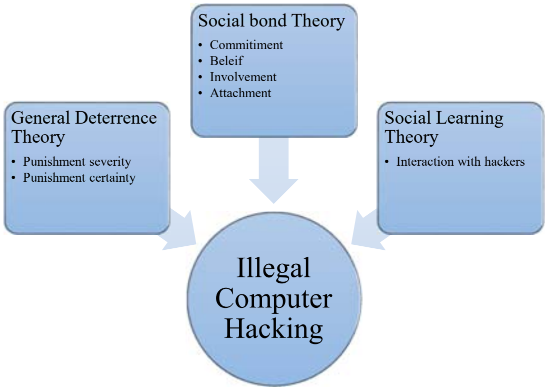

Figure 2. Research Model Reprised

Through the filter of worldviews, theoretical perspectives related to the behavior of engagement in illegal computer hacking. The postpositive perspective, as demonstrated through social bond and learning theory or general deterrence theory, seeks to understand behavior through the lens of cause and effect (Durkheim & Wilson, 1981). Within this area of theory, researcher seeks to determine what caused an individual or group to engage in a certain behavior, such as learning or being bonded to a group, and how labeling that individual leads to the outcomes associated with that group or how the use of punishment or other deterring factors will cause a modification of behavior (Lederman, 2015; Young & Zhang, 2007).

This differs from the transformative view, which attributes every action to political motivations and a social agenda for change. As an example, theory based on this perspective is attributed to the social movement theory espoused by Marx and Le Bon (Kendall, 2006). In Marx and Le Bon's view of social movement theory, groups are moved to action by either economic or political desires and that all actions happen in groups (Kendall, 2006; Marx & Engles, 1883). The constructionist view, in relation to hacker behavior, is summarized through conflict theory. Conflict theory posits that an adversarial relationship exists between everyone and everything and that once meaning of the world around the individual is understood, conflict will emerge as individuals or groups seek to take what they perceive as 'rightfully theirs' (Collister, 2014).

The pragmatic worldview typifies the new social movement theory. This theory is framed within groupings of constructs in which the movement culture has evolved beyond basic conflicting positions, such as social movement theory or conflict theory, and is now based on loose social affiliations in relation to culture, group identity and individual identity or what is more commonly known as social bond theory (Fuist, 2013; Husu, 2013; Turner, 2013). Pragmatism provides the flexibility to merge differences in the world (Creswell, 2014). This is critical in the area of hackers, since it is a worldwide phenomenon, and there is no single absolute bond or unity when examining the motivations of diverse groups within different cultures. We are not examining a single race or gender; we are examining a sub-culture within (a global) society that has emerged with the advances in contemporary technology.

This leads to the theoretical framework for this qualitative non-experimental replication study through the examination of hackers via the constructs of general-deterrence theory, social-bond theory, and social-learning theory. The original study uses these constructs to examine behavioral factors that encourage or deter engagement in illegal hacking. Young and Zhang (2007) search for causal connection of behaviors and do not primarily seek to examine or explain the hacker sub-culture as a whole or through the loose affiliations that exist between hacker collectives.

Therefore, this study employs Young and Zhang's replicated worldview of postpositivism. Postpositivism is particularly useful when examining view culture within the framework of society. While the transformative and pragmatic worldviews could also be employed based on the theory constructs, general-deterrence theory, social-bond theory, and social-learning theory also have a place in both social movement theory and new social movement theory, it would not fit the studies design, purpose, or questions which seek cause and effect answers.

Information Technology and Societal Ethical Changes

There are many ethical issues and challenges related to technology and information systems. Developing and teaching a code of ethics in information technology holds unique challenges (North, Richardson, & North, 2017). This is primarily due to the enhanced pace of societal changes brought about by the rapid development of technology and the massive incorporation of technology into the everyday lives of individuals and organizations (Davis, 2014). To understand these issues, several critical dimensions to the information technology ethics conundrum must be examined.

With the multitude of scandals and violations related to ethical and moral breaches of the public's trust by businesses, governments, and individuals, concerns about ethics in information technology have reached an all-time high (Kaptein, 2017). The emergence of new and more integrated technologies in the workplace and in everyday life have brought about a multitude of ethical concerns and expectations (Jamal, Ferdoos, Zaman, & Hussain, 2015). Adequately addressing ethical issues in information technology has moved beyond the concerns of a small group of IT managers or technical professionals and become increasingly demanded by the public (Kaptein, 2017).

Additionally, academicians are increasing their focus on the human elements of cyber security and threats to information systems from the unethical use of technology (Chatterjee, Sarker, & Valacich, 2015). This is because information technology is now a part of everyday life for almost everyone on the planet (Davis, 2014). Issues such as trust, transparency, security, privacy, the accuracy of information, fraud, intellectual property rights, social responsibility, trade restrictions, and open access to information are all demands that society now places on information technology professionals (Steinmetz & Gerber, 2015).

While some argue that the underlying moral and ethical dilemmas faced in information technology have plagued society since the time of Aristotle (Kaptein, 2017), access to information and new technologies that enable nefarious, corrupt, or criminal exploitation of individuals and organizations have grown exponentially over the past 30 years (Rechtman, 2017). Citizens of the world now demand information technology professionals address these issues at the corporate and government institutional levels (Prislan, 2016). This is because these institutions are the entities responsible for collecting and maintaining information, building and developing new technologies, and training information-technology professionals. Ethical considerations must be incorporated into all phases of technology development (Rechtman, 2017). It is critical throughout the design, development, production, distribution, and maintenance phases to analyze not only the use of the development, but the users and potential consequences that the technology will bring with it (Cao 2015). 20 years ago, few people imagined that the United States government would record the telephone conversations of its citizens (Nolan, 2017) or that corporations would maintain huge amounts of data on customers that could be compromised, either internally or externally, for criminal purposes (Rechtman, 2017). This demonstrates how the ethical uses of technology can be conceptually difficult and rely on every individual's socialized and internalized experiences of what they believe to be right and wrong (Wakunuma & Stahl, 2014).

Additionally, ethics in information technology has been written about a great deal, but the majority of these writings are based on Western ethical traditions (Avci, 2017). Since information technology is worldwide and multicultural, the ethical use of information technologies must consider the ethical and moral foundations of all world cultures (Avci, 2017). Information-technology ethics are not just a discussion for technology professionals. Business executives, government officials, educators, and ordinary individuals must consider how they interact with technology and what they do with the almost instantaneous multitudes of information available to them (Chatterjee et al, 2015).

Ethics is a critical consideration when discussing hacking. Hacker groups, such as Anonymous and Wikileaks, or other ‘information dump sites’, are viewed as a bastion for individuals to be able to bring the unethical behavior of others to the public eye (Cammaerts, 2014). As an example of retribution carried out by hacktivists for perceived ethical violations, on December 8, 2010, MasterCard and others were attacked by a coordinated, bundled, multi-layer DDoS attacks (Arora, Kumar, & Sachdeva, 2011; Herberger, 2011). This attack, daubed ‘Operation Payback’ and carried out by the hacktivist group Anonymous, was a retribution attack for stopping the processing of payments to WikiLeaks (*United States of America v. Dennis Owen Collins, et-al*). This coordinated Low Orbit Ion Cannon (LOIC) attack was designed to flood the MasterCard websites with a huge amount of irrelevant Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic to make their systems resources unavailable to legitimate users (Sauter, 2013; *United States of America v. Dennis Owen Collins, et-al*). As a result, MasterCard's website was knocked offline for several hours and their SecureCode payment verification system was slowed and temporarily disrupted (*United States of America v. Dennis Owen Collins, et-al*).

As stated above, MasterCard was targeted by Anonymous because it discontinued processing payments for WikiLeaks after receiving pressure from the United States government, when WikiLeaks published thousands of classified and secret documents from the United States Department of State (Sauter, 2013; *United States of America v. Dennis Owen Collins, et-al*). Anonymous is a hacktivist group that believes all information should be open and accessible (Sauter, 2013). In this attack, the group urged people to join the attack to punish MasterCard and the other victims (Sauter, 2013; *United States of America v. Dennis Owen Collins, et-al*). Anonymous published statements that MasterCard and others were going to be punished; however, MasterCard countered with a statement that they were stopping the process because of the contractual violations of WikiLeaks engaging in, or encouraging others to engage in illegal activities (*United States of America v. Dennis Owen Collins, et-al*).

The Concept of Activism and the Movement Culture

Activism, as a theoretical concept, dates back millennia, as exemplified by Spartacus' revolt against the Roman Empire, Moses leading the Jews from Egypt, or the Boston Tea Party, but it has only been studied theoretically by scholars since the late 1800s (Buechler, 1995; Kendall, 2006). From that time to the present, much of the work on social activism is based on the premise that social activism is motivated in individuals, based on economic or political reasons (Kendall, 2006; Marx & Engels, 1883). In das Kapital (1883), Marx posited that, by rising up against the bourgeoisie class, the proletariat takes what rightfully belongs to the people. During the early 1900s, social-movement theorists advocated that action was a random occurrence of emotional reactions by people to situations and circumstance beyond their control (Buechler, 1995; Husu, 2013). Le Bon was the first to postulate that collective behavior, such as a random crowd, can move to action (Buechler, 1995; Kendall, 2006; Krips, 2012). This was followed by Smelser's collective-behavior theory in the 1960s, which noted that social movements require organization and group-action for motivating social change by individuals with like political philosophies and political agendas (Buechler, 1995; Kendall, 2006).

These motivational factors are still echoed in much of today's work. Thomas' work argued that social change is now corporatized and that economic power translates into political power and now drives social change (Thomas, 2015). Students of anarchism have long argued that new social activism is based, primarily, on the tenants of the anarchist movement (Lederman, 2015). Anarchists advocate that without political motives, social movements are not possible (Lederman, 2015). Cleveland (2003) and Marchart (2012) argued the middle class now leads social change based on their economic status and rebellion from the political ideals held by their non-working-class families and therefore, economic and political motivators drive social change.

Additionally, Marchart (2012) argued that political motivators drive the area of study due to the relative ease for identifying the ‘why’ factor of a social movement. Marchart (2012) asserted that this factor has gained dominance due to the relative ease in analyzing this factor. Contrary to these arguments, Bourdrieu argued that factors, such as social position and cultural competences, build the identity movement, not political identity (Husu, 2013). Husu (2013), suggests that the social-movement theory tenant of individual and group identity were equally, or even more important than political motivators. Fuits (2013) argued that culture matters in relation to social movements and that cultural shifts are the main factor in social movements, or change (Fuist, 2013). Fuist (2013) further argued that culture serves as a resource and provides a wider context than political discourse for understanding societal movements.

By the decade of the 1990s, social-movement theory, and the collective-behavior theory, began to give way to the new-social-movement theory (Buechler, 1995). Buschler (1995) argued that there was not one theory under the new-social-movement theory construct, but that it was a grouping of theories in which identity, lifestyle, and culture were the dominant forces in social activism. Kendall (2006) further argued that the theory focuses on, what he calls, "the movement culture" as the primary vehicle for social change. Touraine, Laclair, Offe, and others surmised that the new-social-movement theory's primary motivations for social action were based on social and cultural factors, including social learning and social bond; and secondarily, if at all, on political and economic factors (Husu, 2013; Kendall, 2006).

The second area of controversy within social-movement theory is the debate over how social movements are organized. Much of the early research, which continues today, focuses on the organizational structure of movements (Gahan & Pakarek, 2013). Organizational structure research asserts the premise that social movements need structure and organization to be successful (Cleveland, 2003; Gahan & Pakarek, 2013; Thomas, 2015). This position sites unions, and other socially bonded organizations such as Greenpeace, as examples of effective social movements (Gahan & Pakarek, 2013). Other tenants postulate that modern technologies have eliminated the need to structure movements, as evidenced in the uprising in Syria and the Anonymous hacktivist group (Leenders, 2014; McKane, 2013). These decentralized movements held loose affiliations, based on various tenants of technological activism, thus making it more difficult to classify the exact motives of participants (Collister, 2014; Leenders, 2014; McKane, 2013; Turner, 2013).

Movement theory, in relation to hackers, also is applied in relation to the human, or 'people', elements for this behavior. The behavioral constructs of hacker theory are rooted in the area of social-movement and new-social-movement theory. This construct of the theory is applicable to social-change research in relation to economic and political factors, but often overlooks the other social change factors of identity, group identity, culture, and lifestyle choices (Bueschler, 1995; Leenders, 2014; McKane, 2013; Turner, 2013). Some scholars have argued that the theory focuses on "the movement culture" as the primary vehicle for social change and theorize that the prime motivation for social action is not political or economic factors, but rather social and cultural factors, as described within the new-social-movement theory construct (Buechler, 1995; Kendall, 2006; Turner, 2013).

Since hackers, and the sub-group of hackers known as hacktivists, are diverse and geographically dispersed, this theory provides a framework for understanding actions, due to its constructs of self-determination and autonomy over the ability to manifest power and exert lasting influence (Turner, 2013). This application is not over-reaching, since the hacker theory borrows heavily from many proven sociological and psychological theories such as general-deterrence, conflict-theory, social-movement theories, including social-bond theory and social-learning theory (Hampson, 2012; Xiang, 2013; Young & Zhang, 2007). Application of theory related to cultural movements is often misapplied, since the primary approach to the research mostly considers only part of the theoretical perspective (Jampson, 2012; Xiang, 2013).

Commonly, the application of theory in this area look at applying tenants that are easy to understand and implement, such as conflict and deterrence, and negates or ignores individual identification, group identity, culture or social learning, and social bond (Buechler, 1995; McKane, 2013). The motivational factors of political and economic change are prevalent in today's theoretical application (McKane, 2013; Thomas, 2015). Thomas' work (2015) argued that social change is corporatized and that economic power translates into political power and drives social change (Thomas, 2015).

Students of anarchism have long argued that new-social-movement theory is primarily based on the tenants of the anarchist movement (Lederman, 2015). The anarchist political movement generally argues for a 'stateless society' based on voluntary human associations (Lederman, 2015). Anarchists advocate that without political motives, social movement is not possible (Lederman, 2015). Therefore, anarchism bases its argument on social change through political movement (Leederman, 2015).

Cleveland (2003) and Marchart (2012) argue that the middle class now leads social change based on their economic status and rebellion over the political ideals held by their non-working-class families and, therefore, economic and political motivators drive social change (Cleveland, 2003; Marchart, 2012). Additionally, Marchart (2012) argues that political motivators drive the area of study due to the relative ease for identifying the ‘why’ factor of a social movement (Marchart, 2012). He asserts that this factor has gained dominance due to the relative ease in analyzing this factor (Marchart, 2012).

While all of these factors can play a part in applying theory, they do not look beyond the two factors of political and economic motivation for social movement to seek understanding into the 'whole person'. Bourdrieu argued that factors, such as social position and cultural competences build the identity movement, not political identity (Husu, 2013). Bourdrieu's research suggests that the social-movement theory tenants of individual and group identity, or social bonds, were equally, or even more, important than political motivators (Husu, 2013). Fuits (2013) argued that culture matters in relation to social movements, and those cultural shifts are the main factor in social movements, or change (Fuist, 2013). He further argued that culture itself serves as a resource and provides a wider context than political discourse for understanding societal movements and hacker/hacktivist behavior (Fuist, 2013). This approach to theory application more aptly addresses root cause analysis and allows for greater understanding in a wider context. It has a limitation in that it is not easy to apply behavior motives to general populations, since every person is different (Hampson, 2012; Xiang, 2013; Young & Zhang, 2007).

Early Concepts of Hacking

Early hacker theorists, from the 1950s to the 1990s, advocated that hackers were primarily technological practitioners that would manipulate systems to improve technology, or would hack systems in the pursuit of knowledge (Collister, 2014; Levy, 1984). The so-called ‘white hat or ethical hacker’ was one whose intentions were not to destroy or profit, but to improve systems or their own personal knowledge (XU, HU, & Zhan, 2013). As the concept progressed into the mid-1980s, hacker theory espoused the motivation to hack into a cracker-criminal mindset, which is where theories of deviant behavior and criminology began to dominate, and the theory that the hacker was a lone actor seeking criminal gain or motivated to act for political purposes (Collister, 2014). These hackers, known as ‘black hat hackers or gray hat hackers,’ use their talents for gain with the primary distinguishing factor between ‘black hat’ and ‘gray hat’ being ‘gray hat’ hackers generally conduct their activities for ideological or moral purposes (XU et al, 2013). The theories of criminal and deviant behavior are still prevalent today and are deeply ingrained in the general deterrence models for dealing with hacker behavior by most world governments (Computer Fraud and Abuse Act of 1984, 1986; Computer Misuse Act of 1990; Identity Theft Enforcement and Restoration Act of 2008, 2008; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 2002; Xiang, 2013; Young & Zhang, 2007). As an example, a person convicted of second-degree murder, on average, will spend eight years in prison in the United States, but a hacker that defaces a nationally regulated bank can receive a 25-year sentence without the chance for parole (*United States of America v. Dennis Owen Collins, et-al*, 2014).

As hacker theory began to mature, the focus shifted to the counter-culture open-internet movement, which espoused that all information should be free and open to everyone (Collister, 2014; Levy, 1984). This signaled a change from the idea that hackers operated alone, and began the progress into examining hacker culture as social movements and political movements; thus, the concept of the hacktivist was born. Since the 1990s, the dominant theories towards hackers have centered on hacking for economic gain, or political or social manipulation and centered on loosely-affiliated groups acting in concert without centralized leadership to affect change (Collister, 2014).

Hacktivism is an example of a loosely affiliated group action. Hacktivism is a relatively new concept where social activism blends with new technologies to use computers, networks, and the internet to promote or further social causes (Collister, 2014). There are many definitions of hacktivism. Theoretically, hacktivism and conflict-theory are linked through the premise of an adversarial relationship between the hacktivist and the targeted organization or group (Collister, 2014). While this theory makes sense at the contextual level, it does not specifically address the factors that motivate individuals to hacktivist actions. Conflict-theory forces the concept of confrontation and emphasizes that social, political, or material inequities of a social group bring about collective action (Fitri, 2011; Husu, 2013; Kendall, 2006). It presupposes that a conflict between the 'haves' and the 'have not's' must exist to bring individuals together into groups for action (Husu, 2013; Marx & Engels, 1883).

Conflict-theory emphasizes class difference as the main source of conflict within society and that in order for a social movement to happen, a power differential must exist (Marx & Engels, 1883). This theory is used in supporting the thesis that power must be exercised by the collective group that perceives itself as only powerful within the group, and that they must act to 'take what is rightfully theirs.' Conflict theory’s basis is in control of the means of a productive society and power by a central collective group and does not look at the individual (Kendall, 2006; Marx & Engels, 1883). Some theories, such as those espoused in Young and Zhang’s (2007), believe that hacktivism is a sub-group of hacking, which causes are rooted in social-bond theory, social-learning theory, and general-deterrence theory. This form of action could be summarized as individuals acting as ‘free wolves’, acting on their own accord without the control of oversight of any sort of governing structure.

Common Hacker Tactics

Most often the methods hackers employ are the only known elements of an attack, and typically only general reasons are stated (Marechal, 2013). An examination of attack and defensive methods help build a deeper understanding of the individual or groups confronted by security professionals. Additionally, hackers/hacktivists, using techniques such as social engineering, prey on the fear and lack of understanding or awareness related to information security (Dahbur, Bashabsheh, & Bashabsheh, 2017). What is known is that hacker behavior, such as denial of service attacks and social engineering, instills fear in victims, which, in turn, can offer new opportunities to those engaged in this behavior (Dahbur et al., 2017; Pike, 2013). It is also known that many of the accepted ways of countering this, such as defensive technologies (Suroto, 2017) and punishment (Collister, 2014; Xiang, 2013; Young & Zhang, 2007) are not effective.

Defensive-strategy applications view the hacker/hacktivist theory issues from the perspective of preventing or responding to an actual attack (Holtfreter & Harrington, 2014; Maan & Sharma, 2015). They do not seek to apply behavioral reasons, or outside factors that contribute to the attack (Collister, 2014; Young & Zhang, 2007). They focus strictly on developing better methods for defending systems (Marechal, 2013; Prislan, 2016). Much of the research focuses on specific attacks and/or system architectures to defend against attacks (Marechal, 2013; Prislan, 2016). While providing mini-level theories for defensive strategies is critical from a practical perspective, this sub-area does not provide a context for remedying this phenomenon or is not able to provide concepts that apply across the entire range of information systems. Each system is different, so the general constructs can provide guidance, but each will have to be tailored to meet the individual context of systems operations.

As an example, DDoS defense through packet filtering can be applied to any environment, but since the backbone architecture of each system has grown over time through the development of different system administrators, each system will respond differently to these processes (Gordon, 2017; Preetha, Kiruthika Devi & Mercy Shaliniem 2014). This difference in systems makes it difficult to reach a shared agreement as to how to handle most information-systems defenses (Gordon, 2017). Additionally, this area of theory application must also embrace outside factors, such as risk-level and risk-tolerance. These levels differ between organizations, and most theory in this area fails to address this difference (Altuhhov, Matulevičius, & Ahmed, 2013; Bhuyan, Kashyap, Bhattacharyya, & Kalita, 2014).

Common Hacker Attack Vectors

Hacker attacks can come from inside and outside the organization. An inside attack originates from someone who has valid login credentials and is authorized to access the information infrastructure (Spyridopoulos, Karanikas, Tryfonas, & Oikonomou, 2013). Attacks from the outside come from individuals that do not possess valid login credentials and are attempting to flood the server in an attempt to prevent it from functioning or deny authorized users the ability to access the resource (Spyridopoulos et al., 2013). Attacks can come from individuals or groups, including criminal organizations, hacktivists, cyber-terrorists, and nation-states (Macrae, 2013). The most common methods of attack are in the form of network attacks, intrusion attacks, social engineering attacks, and cyber-attacks.

An infinite number of attack variations exist. Technology itself grows so rapidly that new and more complex attacks are continually developed. Organizations are under constant assault from attackers attempting to bring down or disrupt their services, steal intellectual or financial data, misappropriate money or ruin an organization's reputation (Macrae, 2013). Attacks against networks occur on typical wired or wireless networks that are either traditional infrastructure-based networks or ad hoc networks. Ad hoc networks do not have a typical infrastructure, such as hybrid Cloud networks or Cloud only networks that offer Infrastructure as a Service. Each network node operates as a router and communicates directly with other nodes that are in range (Chhabra, Gupta, & Almomani, 2013).

Generally speaking, network attacks are associated with increased traffic to and from the server (Ye, Aranda, & Hurley, 2013). Attacks against networks can come from both internal and external sources. According to the annual State of Cybersecurity and Digital Trust survey by Accenture and HFS Research Limited, internal attacks were reported by 69% of all respondents (Accenture, 2016). Insiders often have unique knowledge about the organization's systems and network security and protection tools typically do not protect against attacks from inside the organization (Spyridopoulos et al., 2013). For example, firewalls are designed to prevent outside traffic from getting into the system and typically do not prevent movement within the system.

While traffic in and out of the network passes through the firewall, rule sets are often less restrictive for outbound traffic than inbound traffic (Kamiya, Aoki, Nakata, Sato, Kurakami, & Tanikawa, 2015). Furthermore, organizations' Internet firewall, or border layer between the internal network and the Internet, does not check the internal network traffic, meaning traffic between systems within the environment only runs through a firewall if internal firewalls are in place to segment the networks (Kamiya et al., 2015). Internal hackers generally conduct attacks for profit, or some other sort of personal gain, to gain access to confidential information, or in retaliation for an actual or perceived wrong done by their employer, to either them or some form of perceived unethical behavior (Collister, 2014). As an example, the hacktivist Bradly Manning stated that his reasons for 'leaking' information to WikiLeaks were in response to his perceived unethical behavior of the United States Government in the wars in Iraq and Afghanistan (Sangarasivam, 2013).

An external attack, or external hack, is conducted by someone outside the organization, who uses the internet or other external communications channel to gain access to the internal servers of the organization (Dutt, Ahn, & Gonzalez, 2013). Since the attacks on the local area network come mostly from the organization's attachment to the internet, external attacks on networks are often called cyber-attacks (Dutt et.al. 2013). External hackers generally cause more damage than internal hackers (Holtfreter & Harrington, 2014). In Holtfreter and Harrington's 2014 article, they identified that the average external hack compromised 663,261 records (Holtfreter & Harrington, 2014). In comparison, they found that the average internal hack compromised only 2,119 records (Holtfreter & Harrington, 2014). External hackers are often cited as carrying our cyber-attacks for personal profit, peer recognition, general curiosity, personal conviction (often called hacktivism), or a belief that all information on the world wide web should be free and open to everyone (Young & Zhang, 2007).

As an example, Target is a major online and ground-based retailer in the United States. In 2013, the company was plagued by two major security issues that damaged its reputation as a trusted retailer, cost the company millions in sales and credit monitoring fees, and brought to the forefront the highly inadequate security of online and electronic payments (PCI Security Standards Council, 2014). Targets' first issue stems from a failure to properly address and mitigate vendor security (PCI Security Standards Council, 2014). The first breach resulted from a heating, ventilation, and air conditioning (HVAC) contractor leaving a port open on its firewall that provided hackers a direct link into Target's PCI, version 2, hardened network. PCI version 2, the Payment Card Industry standard for electronic payment processing, addressed vendor security but did not adequately address network security. Therefore, Target followed the same methodology as most other organizations and provided only a hardened segment to their network infrastructure, instead of a separate hardened network or a fully secured and hardened primary network (PCI Security Standards Council, 2014). As a result, the HVAC contractor, who did not have access to the segmented network, had access to the primary network, and, once inside, the criminals were able to penetrate the hardened segment from inside where barriers were lower (PCI Security Standards Council, 2014). This allowed hackers to steal all of the identity information of customers before the outbound network traffic volume increase was detected (PCI Security Standards Council, 2014). Target's second issue resulted from a zero-day attack on the point of sale devices (POS) that allowed for unencrypted card data to be sent to a resident database outside the firewall for criminal retrieval at a later date, when traffic levels were already high and would be less detectable (PCI Security Standards Council, 2014). Zero-day attacks are exploitations that take advantage of security vulnerabilities in either hardware or software code that allows for attack execution prior to the vulnerability becoming known or having remediation, usually a software patch, available for deployment by an intended victim. Both of these issues were outside the direct control of Target, but, since Target failed to provide adequate vendor assessment and oversight, it is responsible for the damage, and in the public's view, only the name Target is associated with the breach, even though Target itself was not actually breached, the vendors were breached.

There are various types of attacks on networks. They include eavesdropping, identity spoofing, denial of service attacks, distributed denial of service attacks, and sniffer attacks.

Attacks such as eavesdropping, which is often called snooping, involve interception of network traffic. Identity spoofing is the process of an attacker assuming, or fooling the network into believing, the IP address they have presented to the network is a valid IP address, thus gaining access to the system. Of the types of attacks presented above, denial of service and distributed denial of service attacks are among the most common and most dangerous. The main goal in a denial of service attack is to deny, disrupt, or slow down network services to legitimate users (Spyridopoulos et al., 2013).

To accomplish this goal, the attacker attempts to flood the server with requests to verify as many network credentials as possible (Chhabra, Gupta, & Almomani., 2013). This ties up as many system resources as possible to slow down the systems or crash the systems (Chhabra et al., 2013; Spyridopoulos et al., 2013). A distributed denial of service attack is the same as a denial of service attack, but, instead of the attacker directly flooding the server with credential requests, the attacker uses a control program to perform attacks simultaneously from several different machines (Chhabra et al., 2013). Because of their distributed nature, this form of attack is particularly effective and difficult to trace back to the attacker (Chhabra et al., 2013).

Hackers generally follow a four-step process when attacking a network (Holtfreter & Harrington, 2014). To carry out an attack, a hacker starts with reconnaissance and enumeration. The goal of the reconnaissance phase is to gather as much information as possible about the intended target (Holtfreter & Harrington, 2014). The enumeration phase is where network scanning or war dialing happens (Holtfreter & Harrington, 2014). Scanning seeks to identify network service and open-port vulnerabilities that can be exploited (Holtfreter & Harrington, 2014). The reconnaissance and enumeration step can often employ social engineering attack strategies to further gain information about the targeted system. The second step, intrusion and advanced attack, is when the attacker has gained the ability to penetrate the network by exploiting the vulnerabilities detected in step one (Holtfreter & Harrington, 2014). Step three of a network scanning attack generally is the insertion of malware (Holtfreter & Harrington, 2014). The insertion of malware gives the attacker the ability to have ongoing remote control over the network systems and provides them with the ability to execute code within the network (Holtfreter & Harrington, 2014). Step four is generally the clean-up phase of the attack (Holtfreter & Harrington, 2014). In this step, the goal is to erase any traces of the attack, either manually or automatically, or deploy destructive viruses or worms to conceal their attack (Holtfreter & Harrington, 2014).

The next common form of attack is an intrusion. The word intrusion describes the intent of an attack. The main purpose is to get into the system. Intrusion attacks can be manual or automated (Manivannan & Sathiyamoorthy, 2013). They are deliberate and unauthorized attempts to access or manipulate information or their associated systems (Manivannan & Sathiyamoorthy, 2013). The objective of this type of attack is to subvert the information systems' defenses to gain access (Corona, Giacinto, & Roli, 2013). This type of attack is generally used by criminal organizations and nation-states (Corona et al., 2013). The goal is usually to exploit system security vulnerabilities without being detected by the system being attacked (Corona et al., 2013). This attempt to conceal the attacker’s presence is so they can continue to exploit and control the systems for their on-going and continued advantage (Corona et al., 2013). In most cases, intrusion attacks are used to gain access to systems to steal information, such as "breaking in" to a research and development firm to steal designs and other intellectual property on new products (Corona et al., 2013).

Intrusion attacks can be broken down into four main categories of attack. They are probing, denial of service, R2L attacks, and U2R attacks (Manivannan & Sathiyamoorthy, 2013). Probing attacks seek to gain access to the target system through a known vulnerability or weakness (Manivannan & Sathiyamoorthy, 2013). Denial of service attacks, as discussed before, are attacks that are intended to deny services to authorized or legitimate users. R2L attacks are by unauthorized users from remote locations (Manivannan & Sathiyamoorthy, 2013). U2R attacks are attacks by unauthorized users so that they may gain local root access privileges (Manivannan & Sathiyamoorthy, 2013).

Hackers generally accomplish defeating system security by either evasion or overstimulation (Corona et al., 2013). Evasion is the process of injecting patterns that do not match any known signatures in the intrusion defense system (Corona et al., 2013). It seeks to evade detection by masking itself as an unknown entity, much like a spy who might conceal their identity by posing as a waiter in a hotel. Overstimulation is the process of generating event patterns that match one or more signatures, but they do not present any real threat to the monitored system (Corona et al., 2013). This is an attack based on basic deception and diversion. It seeks to divert the attention of security services away from the real attack. In military terms, it would be considered a 'false flag operation'. One of the real dangers in intrusion attacks is that current infrastructures are inefficient against these kinds of powerful attacks (Manivannan & Sathiyamoorthy, 2013). Intrusion attacks mainly differ from network attacks in their end goal. Intrusion attacks are generally designed to be covert and seek to gain information, while general network attacks primarily seek to disrupt services. This type of attack is particularly useful to criminal organizations and both private and nation-state intelligence services in gathering information for profit or political purposes.

Social-engineering attacks are a particularly interesting form of attack. This type of attack is defined in a new context, but it is really similar to the deceptive practices used by ‘white collar’ criminals, often called ‘confidence men’, for generations. The main difference is that technology is employed, at least partially, to carry out the con (Conteh & Schmick, 2016). A social-engineering attack differs from other forms of attack because it is not purely technical (Conteh & Schmick, 2016). It has a human psychological component and securing against social-engineering attacks is predominately based on human defense skills (Conteh & Schmick, 2016). While other forms of attack have limitations, social-engineering attacks are limitless, in that the attacker gets its information from the victim through deception (Conteh & Schmick, 2016; Krombholz, Hobel, Huber, & Weippl, 2015). This method of attack involves gaining information or access to systems or locations by building a trust relationship with the targeted person (Krombholz, Hobel, Huber, & Weippl, 2015).

In a social-engineering attack, the perpetrator gathers as much information as possible about the target by attacking the weakest link in the security chain, the human being (Krombholz, Hobel, Huber, & Weippl, 2015). Social-engineering attacks occur in two forms. The first is human based. Human-based attacks include piggybacking, tailgating, telephone cheats and dumpster diving (Conteh & Schmick, 2016; Krombholz, Hobel, Huber, & Weippl, 2015). In these types of attacks, the attacker poses as someone that the victim can trust. Piggybacking is when an attacker uses an authorized person to gain access to a secured location, such as posing as a co-worker who left their access card at home or a family member coming to visit a worker (Conteh & Schmick, 2016). Tailgating is when the attacker uses like uniforms or communication skills to gain unauthorized access (Conteh & Schmick, 2016). As an example, a person poses as part of the janitorial staff and gains access to secured areas by wearing the same uniform as the authorized workers. Telephone cheating is another common tactic. The telephone cheat will call an unsuspecting victim, and pose as an authority figure, to gain access credentials, such as someone from IT, who needs to use your credential to access your secured network drive to clean up a problem (Conteh & Schmick, 2016). Dumpster diving, or going through an organizations trash is another common way for an attacker to gain information (Krombholz, Hobel, Huber, & Weippl, 2015). Employees that are unconscious about the information they discard often throw away little pieces of information that an attacker can use to gain unauthorized access. This approach is very appealing to attackers since trash can be searched, and it is not illegal for someone to go through trash left in an outside unsecured dumpster or at a landfill that they have been granted access to (Krombholz, Hobel, Huber, & Weippl, 2015).

The second type of social-engineering attack is computer based. It includes the use of fake mail, phishing, and pop-up windows (Conteh & Schmick, 2016). Fake mail is a series of useless emails that install malicious items on the victim's system to gain access (Conteh & Schmick, 2016). Phishing is a fraud that uses email addresses that resemble trusted locations and logos to get people to provide their access credential (Conteh & Schmick, 2016). This fraud uses the trust people have in companies, such as their email provider, to get the victim to send information such as user ids and passwords to the attacker. The attacker then uses this information to gain unauthorized access to the secured resource. As an example, a victim receives an email purportedly from their bank telling them that their account has been compromised and that they need to follow a link to log into the system to change their password. In reality, they are actually giving their user name and password to the hacker. Pop-up window attacks are another from a computer-based social-engineering attack. In this attack, the victim's machine gets a pop-up window that entices them to click on the pop-up and enter a user name and password (Conteh & Schmick, 2016). The attacker just has to sit back and wait for the information to come to them. Social-engineering attacks are particularly insidious. The attacker gains as much information as possible about the victim to gain their trust, and then they use that information to hurt the person or the organization (Krombholz, Hobel, Huber, & Weippl, 2015). It is based on the manipulation of the victim's mind (Krombholz, Hobel, Huber, & Weippl, 2015). Many times, the victim might not even know that they have been compromised. It is easy to tell when a good has been stolen, but it is hard to tell if information has been stolen since the information is usually still there (Krombholz, Hobel, Huber, & Weippl, 2015). This form of attack is particularly successful when organizations have unclear policies and staff that are undertrained in defending against this type of attack.

Cyber-attack is the fourth form of common attack employed by hackers. Cyber-attack can employ different methods of attack, including many of the forms mentioned above, but differs from the other forms of attack in one basic premise. Cyber-attacks are an attempt to damage or destroy a computer network. They do not seek the traditional gains as sought by the other forms of attack. Their aim is to destroy the actual system. An example of this type of attack was the Stuxnet attack that targeted the industrial control systems of the Iranian nuclear program (Leong, 2013). Cyber-attacks usually target a specific system and with the proliferation of malware variants, targeted cyber-attacks are becoming harder to detect and are causing more damage (Leong, 2013). Cyber-attacks can be more difficult to detect because both malicious and non-malicious events are occurring (Dutt et al., 2013,). The attacker is introducing threats to the environment, while authorized users are continuing to utilize the system (Dutt et al., 2013). In addition, attackers that are more patient tend to inject threats towards the end of a sequence (Dutt et al., 2013). This also makes them more difficult to identify. For these reasons, cyber-attacks are very dangerous and can be very devastating.

An attacker is generally identified as a person or computer trying to gain access to the internal network services, or information, of an organization or individual (Dutt et al., 2013). While all of the methods of attack evaluated above are effective individually, combining attack methods can produce greater success for the attacker, and are harder to defend. In security, the weakest link in any information system are people (Krombholz, Hobel, Huber, & Weippl, 2015). Combining social-engineering attacks with denial-of-service attacks can not only slow down or crash network services; it can undermine peoples' confidence in their own safety and trust in organizations. If people do not have confidence in the organization, they might be less likely to trust the organization; thus, undermining the foundation of the institution under attack (Collister, 2014; Holtfreter & Harrington, 2014). Intrusion attacks, combined with social-engineering attacks, can make the intrusion attack much more successful. Gaining the knowledge of insiders can make it easier to cover up the attacker's presence and make it easier for the attacker to exploit security vulnerabilities they were able to elicit from the unsuspecting inside authorized user. A destructive cyber-attack will always be more efficient if insider information is obtained by first exploiting the techniques from a social-engineering attack. It is easy to go on and on regarding combinations of attack, but in summary, any form of attack can have a synergistic effect from another form of attack if variations and mutations of the attack methodologies are carefully plotted out to maximize the exploitation of victims.

A blended attack is a combination of multiple types of attack at the same time, or within short succession. They can blend electronic attacks with other electronic attacks (i.e. two or more types of malware or a Trojan attack and a DDoS attack in succession), an electronic attack with a physical attack (i.e. a DDoS attack or hack on your security systems to allow someone unauthorized access to your facilities) or an electronic attack with a human attack (i.e. combining a DDoS attack with a social-engineering attack so that someone claiming to be from IT can get confidential information, such as passwords, from unsuspecting staff) (Heckman, Stech, Schmoker, & Thomas, 2015). Blended attacks pose a greater threat to an organization because coordinated multi-approach attacks have a synergistic effect. Any attack is threatening on its own, but the effects of a blended attack combined and compounded with each other places the system, and the organization's response to the attack under more pressure. The main threat of a blended attack is its purpose, which is to overwhelm the organization's ability to respond, thus allowing the attacker(s) the ability to carry out their end goal. As an example, on December 8, 2010, MasterCard, and others, were attacked by a coordinated, bundled, multi-layers DDoS attack (Priyanka & Davis, 2015). This attack, dubbed Operation Payback, carried out by the hacktivist group Anonymous, was a retribution attack for stopping the processing of payments to WikiLeaks (*United States of America v. Dennis Owen Collins, et-al*). The attack used standard DDoS botnets coupled with the deployment of Low Orbit Ion Cannon attacks to disable the payment processor (Priyanka & Davis, 2015). This coordinated Low-Orbit-Ion-Cannon (LOIC) attack was designed to flood the MasterCard websites with huge amounts of irrelevant TCP and UDP traffic to make their systems resources unavailable to legitimate users (Sauter, 2013; *United States of America v. Dennis Owen Collins, et-al*). As a result, MasterCard's website was knocked offline for several hours and its SecureCode payment verification system was slowed and temporarily disrupted (*United States of America v. Dennis Owen Collins, et-al*).

Blended attacks often include a diversionary attack to conceal what they are really after. This is often called a false flag operation. An emerging form of blended hacker attack is to combine a DoS or DDoS attack with information exfiltration (Sauter, 2013). The purpose of this attack is not disruption, but information theft (Sauter, 2013). This allows hackers to divert the attention of information security staff away from the information they are trying to co-opt and allow them to take the information without being noticed.

Offensive Cyber Security and the Concept of Mutually Assured Disruption

In the evolving world of information-security, the concept of active, or offensive, cybersecurity is gaining attention (Neal & Ilsever, 2016). Active Cyber Defense, or Offensive Cyber-Security, is the concept of using hacker tools, such as hack-backs, malware deployment, denial of service, or distributed denial of service attacks, social engineering, and ransomware against the hackers that attack an organization (Neal & Ilsever, 2016). In relation to this concept, one must understand who is hacking their system, in order to 'hack-back' the hackers, especially when you consider the legal, ethical, and moral dilemmas that can be associated with offensive cyber actions (Harrington, 2014).

This understanding of behaviors will become even more important as artificial security intelligence, behavioral analysis, and threat intelligence sharing grow out of their infancy in cyber-security and become a security driving force (Craig, Shackelford & Hiller, 2015). This concept is critical to understanding the changing relationship between hackers and the hacked. If security professionals 'hack-back' the hackers that have attacked them, this supposes that attribution can be adequately established, they themselves become hackers (Craig, Shackelford & Hiller, 2015). This moves us towards the cold-war doctrine of Mutually Assured Destruction, or as coined by Geers in 2010, Mutually Assured Disruption.

Deterrence is a way to reduce cybersecurity threats, such as hacking. Deterrence theory was a concept developed during the cold war between the United State and the former Soviet

Union (Geers, 2010). It was used in relation to each sides' ability to launch a first strike with nuclear weapons and also provide nations with a second retaliatory strike capability that which would ensure the destruction of everyone on the planet (Geers, 2010). This was commonly known as Mutually Assured Destruction (Geers, 2010). This theory, in relation to cybersecurity, has two basic strategies. They are cyber-attack deterrence, by denial, and cyber-attack deterrence, by punishment (Geers, 2010). The strategy of deterrence by denial is predicated in concepts of prevention, which, as stated above, will not eliminate attack. It is designed to reduce the number of attacks and manage the attacks to minimize loss. The second strategy of deterrence is punishment. While this can work well when dealing with cyber- attack from nation-states, it is not very effective against rogue elements, individuals, or criminal organizations that are easily able to hide in the vast anonymity of cyberspace (Geers, 2010). Nations can retaliate easily against other nations, but finding an individual or a group of individuals is more difficult and acquiring proof is difficult and often times, impossible (Geers, 2010). For deterrence theory to be effective, cyber defenses have to become more aggressive. Punishment, including mutually assured disruption, would have to become an integral part of cybersecurity response plans. One would have to have the capacity to "turn off" the perpetrator's ability to continue their illegal acts. This can only be done at the governmental level, so cyber defense has to be a national effort, not just an effort undertaken by a few corporations. This is not to say that deterrence is not a valuable tool. Without deterrence, there would be total anarchy in cyberspace. What it means is that none of the current tools developed can do it all. There is not a magic bullet. Many different tools must be combined to reduce the threats to cybersecurity, and many tools will still need to be developed as technology develops.

Standard Defensive Technologies

Defending against hacker attack requires numerous defensive layers (Bissell, 2013, Collister, 2014). There are a number of tools to defend networks from attack. Since most network attacks will have an increase in network traffic to and from the server, many defense strategies focus on monitoring and analyzing network traffic (Bissell, 2013). Other forms of defense build on signature-based recognition systems to defeat malicious attacks. Unfortunately, the proliferation of attack tools, and the increased organization of hacker and hacktivist groups have left security professionals constantly playing catch-up (Bissell, 2013, Collister, 2014). The computer-security field is working diligently to identify server and client-side vulnerabilities, create defensive software signatures, and patch problem areas, but hacker/hacktivist groups and criminal organizations are also conducting research and developing new tools, that allow them to circumvent network defenses (Leong, 2013).

Access control is the first layer of defense in information systems from all outsiders, including hackers. Access control is the process of granting access to resources the user needs while protecting resources from unnecessary and unauthorized access (Hasani & Modiri, 2013). The most commonly used and widely accepted form of initial access control is a password (Cheswick, 2013; Hong & Reed, 2013). Password-based access-control methods are inexpensive, easy to set-up, and are currently the accepted standard in basic access control (Cheswick, 2013; Hong & Reed, 2013). Even though passwords are the most commonly used initial access control method, they have many issues and risks (Honog & Reed, 2013). In an attempt to resolve these issues and vulnerabilities, new access methods are gaining attention. Methods such as radio-frequency identification (RFID) access cards, biometrics, and visual passwords are newer access control systems that improve security (Kumar & Srinivasan, 2013).

When properly implemented, these new methods can reduce the burden on users (Kumar & Srinivasan, 2013). In addition to the access method, attention must also be given to the encryption methods employed in the system. The encryption process, cryptography standards, and associated concerns must also be addressed by information-security professionals (Uduthalapally & Zhou, 2016).

The strongest access policies and procedures in the world will do nothing to secure systems from hackers if information or access credentials can be read through open and clear channels. Encryption is critical to verifying the validity of a message sender and in ensuring the confidentiality and integrity of data ("United State Internal Revenue Service," 2013; Uduthalapally & Zhou, 2016). Encryption, which is used in cryptography, is the process of changing the plain text into cipher text so that unintended receivers of the message cannot read the original text (Uduthalapally & Zhou, 2016). The process uses a secret key so that only intended receivers of the message can read the message (Uduthalapally & Zhou, 2016).

There are three main types of encryption. They are hashing, symmetric cryptography, and asymmetric cryptography. Hashes are created by using fixed length algorithms that are unique to a specific message; therefore, it is easier to tell if the message has been tampered with (Boneh, Corrigan-Gibbs, & Schechter 2016). Symmetric cryptography employs an algorithm that uses the same key for encryption and decryption (Rihan, Khalid, & Osman, 2015). This method requires both the sender and receiver to agree on the key prior to communication being established (Rihan et al., 2015). The third type of encryption, asymmetrical cryptography, employs a method where the encryption key and the decryption key are different (Teodorescu, Lita, Cioc, & Visan 2015). All of these forms of encryption are effective. The main difference between hashing encryption and the other two forms of encryption is that once hashing encryption has been started, it cannot be deciphered. This means that a hacker cannot decrypt an intercepted message. With symmetric encryption algorithms, the encryption and decryption keys are the same and must remain secret because anyone who has the key can read the message (Rihan et al., 2015; Teodorescu et al., 2015). If the key fails to remain secret, it will be ineffective at preventing unauthorized access. An asymmetrical encryption algorithm uses an encryption key to encrypt the data and a different key to decrypt the data (Teodorescu et al., 2015). The public key is generally used to encrypt the data (Teodorescu et al., 2015). The private key is used to decrypt data and is generally kept secret by the user (Teodorescu et al., 2015). This method is generally more secure than symmetrical encryption since a single key does not have to be kept secret by an entire group.

Encryption is the strongest method currently available to prevent unauthorized access to private information (NIST, 2016). Many hacker groups will use sites, like WikiLeaks, or just dump information on targets, in order to embarrass them (Sangarasivam, 2013). Unless they are given the keys, encryption prevents someone from getting access to this information.

Firewalls are a primary tool in defending networks from hackers and can be either hardware based or software based. They have evolved from basic packet filter detectors to application layer firewalls (Naik & Jenkins, 2016). Basically, a firewall provides a barrier between the internal network and outside TCP/IP communication traffic and determines what traffic is allowed or denied. Its main purpose is to control communication between the network and external traffic. They are designed to keep unauthorized people and traffic out and keep internal people from abusing the company's internet access through policy enforcement. Network-based firewalls provide perimeter protection. Host-based firewalls provide protection on individual computers.

Firewalls are best at defending against outside intruders and have many advantages (Bissell, 2013). Once turned on, firewalls run continuously and provide constant protection. They can be configured to allow specific traffic and to deny certain types of traffic (Leong, 2013). This is called filtering. They can monitor internet and network traffic and log that traffic. Firewalls can block random probing and are cost-effective (Bissell, 2013). Some firewalls can block viruses, worms, and Trojans; although, additional software is needed to detect and prevent malware (Leong, 2013).

Firewalls have distinct disadvantages against a hacker attack. Firewalls cannot protect against attacks that do not go through the firewall or are conducted through a tunneled opening in the firewall (Leong, 2013). Examples of this include attacks sent through email or attacks that actuate when a user clicks on a website or internet pop-up that has malware. This is because once a user has established a connection to the malicious site, a two-way connection, or tunnel is, opened. Firewalls examine every packet of communication that goes through them (Kamiya et.al, 2015). This can cause congestion and slow network performance and internet speeds. Improperly configured connections can provide a false sense of security, allow malicious attackers access to a system, or deny resource access to authorized users (Leong, 2013). Firewalls are only a piece of the security puzzle. One must have additional software to provide good protection against malware, such as viruses, worms, and Trojans.

Intrusion-detection systems are used in conjunction with firewalls to monitor, administer, and log network traffic (Ambusaidi, He, Nanda, & Tan, 2016). There are two types of intrusion detection systems (IDS). Network-based IDS are deployed so that all network traffic is sent through the IDS device or a copy of the network traffic is sent to the IDS for analysis and patterns related to attack (Ambusaidi, He, Nanda, & Tan, 2016). Host-based IDS is usually deployed on critical systems to perform file-integrity monitoring (Ambusaidi, He, Nanda, & Tan, 2016). The overall purpose of all IDS systems is to protect against attempts to violate the network's defense systems (Corona, Giacinto, & Roli, 2013). They check for suspicious activity and notify the network administrator of potential attacks for further investigation (Manivannan & Sathiyamoorthy, 2013).

Intrusion-prevention systems are more advanced versions of intrusion-detection systems. Intrusion-prevention systems can block and drop network traffic that is suspicious (Ambusaidi, He, Nanda, & Tan, 2016). If the timing-to-event ratio is correct, it is very successful at identifying and preventing port-scanning attacks. It is also very effective at analyzing network traffic for anomalous network behavior. IDS have both advantages and disadvantages in protecting systems from hackers. Advantages include the ability to log and alert network administrators in real-time to potentially threatening traffic, they can force the router to terminate malicious traffic, and they can serve as a deterrent to hackers due to IDS' ability to constantly monitor the system and quickly respond to threats (Corona, Giacinto, & Roli, 2013). Disadvantages include a tendency for false positives, especially in intrusion-prevention systems, difficulty in managing the enormous log file sizes, configuration management issues can lead to missed events, and intrusion-preventions systems are expensive to deploy and manage (Corona, Giacinto, & Roli, 2013).

Log files are an important tool in network defense. Log files track what is happening on the system and allow system administrators to view and investigate events. The main advantage of log files is their ability to track everything that is happening in the system. When used in conjunction with security-information and event-management software, they can provide invaluable information on system issues, system breaches, and system performance (Kamiya et.al, 2015). The main disadvantage of log files is their sheer size. Files can be very long and cumbersome to navigate, which is why they are often overlooked (Kamiya et.al, 2015).

Antivirus and anti-spyware is critical to network defense. It is critical to stopping virus, worm, Trojan, and spyware programs. Mainstream antivirus and anti-spyware software work on signature patterns that scan a file to detect malicious code (Shukla, Singh, Shukla, & Tripathi, 2014). Advantages include the fast and accurate detection of events with a relatively low rate of false alarms, they are low cost and easy to maintain, and unless disabled, will continuously check incoming code (Shukla et al., 2014). As with all defensive measures, antivirus and anti-spyware have several disadvantages. The primary disadvantage of this measure is the constant need to update virus and spyware signature files. Systems will not recognize what they do not know; therefore, these types of defenses will not defend against malicious code that is not in the signature file (Shukla et al., 2014).

Penetration testing is the process of having internal or external staff hack the system to find vulnerabilities and evaluate incident responses (Dawson & McDonald. 2016). It goes beyond normal system auditing by actually exploiting the discovered system vulnerabilities (Dawson & McDonald. 2016). Tests can include everything from hacking attacks to physical security attacks (Dawson & McDonald. 2016). The main advantage of penetration-testing is that it discovers and exploits real system vulnerabilities and tests the actual incident response (Dawson & McDonald. 2016). The main disadvantages include the possibility that if system administrators are aware of the test, they can patch the systems ahead of time and if there are no limits on the test, penetrators could actually disrupt or destroy the system, thus slowing or stopping the organization's ability to conduct business (Dawson & McDonald. 2016).

Information-security professionals have additional nontechnical tools at their disposal. These tools include policy and procedure development, including incident-response plans and procedures, risk assessment, and staff security awareness training. These tools might be the most important tools in the security arsenal, since the human factor is the weakest link in the security chain.

The effectiveness of established security measures is a twofold issue. Effectiveness in relation to known threats can range from high to low. This is dependent on the individual or organization's perception of risk (PCI Security Standards Council, 2014). Organizations that aggressively seek a defensive posture are better able to respond to or defend against threats (Leong, 2013). This is one possible explanation for the shift from military cyber targets to civilian or personal targets, which are often more vulnerable due to resource limitation and skill shortages (Leong, 2013). Effectiveness against unknown threats is difficult and almost impossible to defend (Corona, Giacinto, & Roli, 2013). Zero-day attacks, large scale DDOS attacks, and the ever-changing variants of attacks make cyber defense difficult and sometimes impossible (Corona et al., 2013). It is difficult to defend against an unknown attack. As an example, intrusion-prevention systems (IPS) are very capable of defending against known crypto attacks and stopping the encryption before the encryption key is returned to the sending source, but when unknown variants are introduced to a system, the key will circumvent the IPS and the cryptovirus encryption will occur. At best, current defensive strategies are limited in effectiveness (Corona et al, 2013). Offensive strategies are also limited in their effectiveness due to the difficulty in labeling the attack source (Neal & Ilsever, 2016). Without being able to positively identify the attack source, a miss-targeted counter strike could escalate into a full-blown conflict (Neal & Ilsever, 2016).

Criminology and the Hacker

Criminology is the study of criminal behavior, at both the individual and societal levels (Dollar, 2014). Hacker activities are defined by most countries as criminal behavior, due to the exploitive nature of the action (Wood, 2015; Xiang, 2013). Within this area of study, there are a number of positions ranging from individual choice to outside social influences affecting the individual's propensity to engage in socially defined criminal behavior (Rege, 2014). The classical approach to criminology most closely aligns with the general-deterrence theory in relation to hackers and the predominate way society attempts to deal with individuals engaging in hacker behaviors.

The classical school of thought is based on four main tenets. First, individuals have free will (Dollar, 2014). Second, people seek to avoid pain and seek activities that provide pleasure (Dollar,2014). Third, punishment must be severe enough to outweigh the benefit of committing the crime (Dollar, 2014). Fourth, the swifter and more certain the punishment, the more successful and effective the punishment will be at deterring criminal behavior (Young & Zhang, 2007). Where this school of thought fails in relation to deterring hacker behavior is at the basic core of its third and fourth tenets. The internet is anonymous; therefore, the chance of getting caught and punished is slim (Rege, 2012). If there is no or little fear of apprehension, then the benefit outweighs the punishment.

Oher criminological schools of thought, such as the positivist position and the Chicago school, seek to explain criminal behavior as either internal or external factors outside of the person's control, or that the breakdown in society drives criminality (Dollar, 2014; McCarthy, 2015). While these schools of thought address potential causes of deviant behavior, they do not fully embrace the factors of free choice, social interactionism, or the cross-economic strata found within the hacker community (Dollar, 2014; Nwalozie, 2015; Rege, 2014).

Subcultural theory, in relation to criminology, builds on the Chicago school, and strain theory in an effort to focus on Sutherland's idea of differential association within small cultural groups (Nwalozie, 2015). Within this theory, small subsets, such as the hacktivist subculture, break away from mainstream social norms and from their own values and meanings (Sutherland, 1947; Nwalozie, 2015). This school of thought follows much of the research on hacker behavior, and with new-social-movement theory in relation to group interaction, in that group acceptance a primary goal (Fuast, 2013; Nwalozie, 2015). When the norms of the group are deviant, then the members will conform to those norms (Faust, 2013; Nwalozie, 2015).

General Deterrence Theory

General deterrence theory, common in the field of criminology, requires attention due to the categorization of many hacker activities as criminal. The theory espouses that higher consequences, or penalties, reduce, or deter, illegal actions (Young & Zhang, 2007). General-deterrence theory models are currently the most common way governments address the phenomena of hacking (Lederman, 2015; Turner, 2013; *United States of America v. Dennis Owen Collins, et-al*, 2014; Xiang, 2013). Governments, under this model, impose long sentences on individuals they are able to catch, hoping to deter others from engaging in the same behavior (Xiang, 2013; Young & Zhang, 2007). This theory only addresses individuals caught and only hopes that the punitive actions will deter others (Collister, 2014; Young & Zhang, 2007). General-deterrence theory does not seek to understand or account for motivations and presupposes that harsh punishment will deter criminal behavior. As an example, WikiLeaks published leaked United States Department of State cables and emails (Murphy, 2011). After the leak, the United States government pressured payment processors to stop accepting Wiki Leaks transactions (Murphy, 2011). Payment processors complied, which resulted in a hacker attack that shut down PayPal, MasterCard, Visa, and others as retaliation for what the hacktivist group, Anonymous, viewed as an attack on the "openness and freedom of the internet" (Murphy, 2011).

Under this theory, the hackers would have not attacked the payment processor for fear of the steep punishments for breaking into the networks of these merchants. Instead, more people worldwide participated in this attack than in any other hacktivist attack in history (Murphy, 2011). Additionally, studies have shown that hackers are more motivated by social factors, less inhibited to participate due to the anonymity of the internet, and are not fearful of being caught or prosecuted (Murphy, 2011; Xiang, 2013; Young & Zhang, 2007).

Conflict Theory

Conflict theory argues that people are moved to action to improve their economic condition or to right the political injustices they perceive within society and that control of the population will control society (Marx & Engels, 1883). As applied to hackers, conflict-theory is used to better understand the actions of individuals and determine methods to assert control of specific populations (Collister, 2014, Marx & Engels, 1883). Groups, such as hacktivists, use conflict, or differences, to elicit emotional responses and to engage others in action, controlling the 'message' and influencing outcomes (Marx & Engels, 1883).

Game and Decision Theory

Game-theory emphasizes the strategic decision- making process in relation to human actions and places a strong emphasis on the development of matrices and models of behavior to determine people's actions and inactions (Young & Levenson, 2014). In relation to hacker behavior, game-theory would argue that the analysis of intelligence and determining risks would dominate the decision to engage in hacker behaviors. Decision-theory is a broader and more general category than game theory and emphasizes the identification of rational choices by labeling values, uncertainties, and other variables to reach conclusions that will provide the greatest positive consequence to actions, and the least negative consequence to actions (Schuessler, 2014; Young & Levenson, 2014). As applied hacker behavior, decision-theory is utilized to identify variables and reach conclusions related to external and internal events to apply appropriate mitigation strategies. Decision-theory would emphasize that rational choice is a primary motivator for engaging in hacker behavior.

Stage Theory

Stage-theory, in relation to information systems, dates back to 1969 (Schuessler, 2014). It is characterized by the development, or maturity of an information systems department through evolutionary stages (Schuessler, 2014). As organizations mature, they are identified in one of four stages of maturity based on the characteristics they exhibit (Schuessler, 2014). The four stages are initiation, contagion, control, and integration (Schuessler, 2014). This becomes applicable to information security and risk management in that it provides a theory for understanding how mature an organization is in these areas and provides a theoretical framework for how an organization can continue to grow and improve. In relation to hacker behavior, stage-theory could explain the evolution of hacker growth into more organized, but loosely affiliated, efforts, such as those demonstrated by the hacktivist group Anonymous.

Social Bond Theory

Social-bond theory, as posited by Travis Hershi, states that people who have weak ties to society are more likely to commit deviant acts (Hershi, 1969; Kendall, 2006; Young & Zhang, 2007). There are four main parts to this theory. They are attachment, commitment, involvement, and belief (Hershi, 1969; Kendall, 2006; Young & Zhang, 2007). Attachment refers to a person's connections with others or lack of connections with others, that will positively or negatively affect deviant behavior (Hershi, 1969; Kendall, 2006; Young & Zhang, 2007). Commitment concerns the amount of time, effort, and expense that a person invests in societally deemed appropriate actions (Hershi, 1969; Kendall, 2006; Young & Zhang, 2007). Involvement attempts to gauge a person's propensity to commit a deviant act, based on the time and effort they put into engaging in conventional activities (Young & Zhang, 2007). Last is belief. With this dimension of social-bond theory, the acceptance of societal rules is the basis for an individual’s propensity to act in a societally acceptable way (Young & Zhang, 2007). This theory addresses individual behavior attributes, which is part of the new social movement theory.

Social Learning Theory

In social learning theory, individuals learn behaviors from others by observing their behaviors and the consequences of those behaviors (Fuist, 2013; Kendall, 2006; McGregor, 2014; Young & Zhang, 2007). This theory states that people who are in regular contact with those whom society has labeled deviant will most likely adopt deviant traits and behaviors of those individuals, and begin to act in deviant ways (McGregor, 2014; Young & Zhang, 2007). This theory places an emphasis on herd-mentality and discards the concept that individuals have free will (McGregor, 2014). It also places a distinct value on individuals learning from other individuals and ignores societal or cultural influences on people (Fuist, 2013).

Economic Threats

Both developed and developing nations depend on the Internet and other electronic communications to rapidly move data, manage data, control systems, and manage commerce (Leong, 2013; ITIL [ITIL], 2014; PCI Security Standards Council, 2014). Banks, hospitals, educational/research institutions, power-generating facilities, ports, transportation systems, water-treatment facilities, and consumer- purchasing operations are all high value economic and infrastructure targets to hackers (Leong, 2013; PCI Security Standards Council, 2014; FEMA, personal communication, October 1, 2014). A successful hacker attack on these types of facilities can cause chaos in the marketplace, and bring essential services to a standstill, crippling the economy, and sending a nation-state into an economic recession or depression (Leong, 2013; PCI Security Standards Council, 2014).

In 2007, a propertied Russian-based hacking group with ties to the Russian government attacked Estonia's information network, causing severe disruption and extended outages in communication networks, banks, and other services (Kirsch, 2012; Leong, 2013; PCI Security Standards Council, 2014). This hacktivist attack was in response to perceived negative actions taken by the Estonian government towards the Russian government (Krisch, 2012). Panic and riots erupted, leaving one person dead, over 150 injured, and an economic loss estimation to corporations, the government of Estonia, and individuals in the tens of billions of dollars (Krisch, 2012; PCI Security Standards Council, 2014). This example demonstrates that interconnected infrastructures can be disabled by hackers/hacktivists when successfully attacked, and can cause severe devastation to the economies of nation-states and have deleterious effects on individuals.

Summary

Even with the significant advances in defensive information-security technologies and government-enacted criminal penalties, illegal hacking continues to rise (Collister, 2014; Prislan, 2016). As a result, billions of dollars continue to be spent on protective and recovery measures (FBI, 2016; Fortinet, 2017, Internet World Stats, 2017). Additionally, governments continue to rely on general deterrence as the primary method for curbing illegal computer hacking (Hui, et-al, 2017; Lederman, 2015; Scheuerman, 2016; Turner, 2013; *United States of America v. Dennis Owen*

Collins, et-al, 2014; Xiang, 2013). This reliance on deterrence has proven to be only marginally effective, due, in part, to the lack of examining the behavioral factors that influence an individual's decision to engage in illegal computer hacking (Madarie, 2017; Udris, 2016). There is a great deal of conflict in the literature around both the causes of and solutions to illegal computer hacking (Collister, 2014, Hui, et-al, 2017, Maderie, 2017, Scheuerman, 2016). To develop greater perspective, this literature examination sought to seek understanding of the problem, illegal computer hacking, by examining theories of social and new social movement, criminality, deterrence in general, as well as the current and historical methods for dealing with this problem, and the ethical dilemmas related to hacking

The chapter began with a discussion describing the conceptual framework for this study. This replication study examined the self-reported engagement in illegal hacking by individuals from the constructs of general-deterrence theory, social-bond theory, and social-learning theory, as utilized in Young and Zhang (2007). Young and Zhang (2007) attempted to link general-deterrence, social-bonding, and social-learning theory constructs with factors that encourage and deter an individual from engaging in illegal computer hacking (Young & Zhang, 2007). Conceptually, this study assessed whether: 1) the general deterrence theory independent variables of punishment severity and punishment certainty; 2) the social bonding theory independent variables of attachment to other socially conforming individuals, commitment to actions deemed acceptable by society, involvement a person has with activities deemed acceptable by society, belief (the degree to which an individual accepts the rules of society); and 3) the social learning theory independent variable of interaction with other hackers encourage or discourage individuals to engage in self-reported illegal hacking, the dependent variable.

The search revealed considerable conflict between the theories related to movement and action. Early cultural, economic, and political theorists, such as Karl Marx and Friedrich Engels, argued that people moved to action to improve their economic condition or correct the political injustices they perceived in society (Buechler, 1995; Marx & Engels, 1883). This conflict approach to social movement is directly in contrast with new social-movement theory motivators, which are a conglomeration of several theories that include general-deterrence theory, social-bond theory, and social-learning theory. These new social movement theory tenants argue that the actions of individuals, in this case hackers, in society through individual or group identity and social connectivity (Udris, 2016), lifestyle, and cultural development (Buschler, 1995; Collister, 2014), as well as through economic and political factors (Collister, 2014; Kendall, 2006) are more likely to move people to action. This modernist view, as theorized by Buschler (1995) and Kendall (2006), casts actions as less dependent on personal economics, such as hacking for financial gain (Hui et al, 2017), or political condition, as theorized by Marx and Engels (1883), and more on an individual's search for self-fulfillment (Collister, 2014), attachment with others (Udris, 2016), intellectual challenge, or a general dislike for the intended target (Madarie, 2017). Criminologists also have argued there are a number of reasons, ranging from individual choice to outside social influences, affecting the individual's propensity to engage in socially defined criminal behavior (Rege, 2014; Udris, 2016). Others explain criminal behavior as either internal or external factors outside of the person's control or that the breakdown in society drives criminality (Dollar, 2014; McCarthy, 2015). Furthermore, theories such as social bond and social learning view criminality as a consequence of the environment the criminal, in this case, the hacker, is a part (Hershi, 1969, Kendall, 2006; McGregor, 2014). Furthermore, there is a great deal of difference related to the deterrence effect with hackers (Hui, et-al, 2017; Lederman, 2015; Scheuerman, 2016). While law and governments have responded to the illegal hacker by raising the perceived costs, such as fines and lengthy terms of incarceration (*United States of America v. Dennis Owen Collins, et-al*, 2014; Xiang, 2013), the Internet itself is an anonymous global community without traditional boundaries' leaving laws only partially successful at curbing behavior (Collister, 2014; Lederman, 2015).

This search also revealed a great deal of information related to how countries and organizations respond to illegal hacking behavior. Some have argued that the underlying moral and ethical dilemmas faced in information technology have plagued society since the time of Aristotle (Kaptein, 2017). Access to information and new technologies that enable nefarious, corrupt, or criminal exploitation of individuals and organizations have grown exponentially over the past 30 years (Cao, 2015; Rechtman, 2017). Citizens of the world now demand information technology professionals address these issues at the corporate and government institutional levels (European Union General Data Protection Regulations, 2017; Prislan, 2016). With all of the information that is available through technological means, it is imperative that business executives, government officials, educators, and ordinary individuals must consider how they interact with technology and what they do with the almost instantaneous multitudes of information available to them (Avci, 2017; Chatterjee et al, 2015).

Hackers, including hacktivists, using techniques such as social engineering, prey on the fear and lack of understanding or awareness related to information security (Dahbur, Bashabsheh, & Bashabsheh, 2017). Hacker behavior, such as denial of service attacks and social engineering, instills fear in victims, which, in turn, can offer new opportunities to those engaged in this behavior (Dahbur et al., 2017; Pike, 2013). This limited fear leads to attempts to build countermeasures and defenses to counter the illegal hacker threat. Additionally, the currently most accepted ways of countering hacker threats, such as defensive technologies (Suroto, 2017) and punishment (Collister, 2014; Xiang, 2013; Young & Zhang, 2007) are not effective.

Defense-driven strategy, primarily through awareness training, applications, and appliances, focus on prevention or responds to an attack (Holtfreter & Harrington, 2014; Maan & Sharma, 2015; Neal & Ilsever, 2016). These current technologies and strategies do not seek to apply individual behavioral reasons for the attack, beyond potential user patterns and the characteristics of the attack after occurrence (Collister, 2014; Suroto, 2017; Young & Zhang, 2007). They focus strictly on developing better methods for defending systems (Marechal, 2013; Prislan, 2016). While it is important to defend systems, not understanding behavior and individual motivations leave defenders with only a partial understanding of the threat environment and how best to counter that threat (Collister, 2014; Lederman, 2015; Wood, 2015; Young & Zhang, 2007).

Overall, the literature provides a great deal of conflict around motivations to hack and demonstrates the conflicts that exist on how to understand defenses and provide for effective system defense. As this field begins to grow and emerge, greater understanding will follow, but the exponential rates of technology growth leave security professional in a constant race to keep up. This is why more non-technical views, such as motivation and behavioral based deterrents to hacking are critical to the development of improved information security defenses.

Where the concepts of traditional theories fail, in relation to hackers, is that they do not address the modern civil society (Avci, 2017; Collister, 2014). They fail to consider the youth-culture movement or cultural development based on lifestyles and values that are not politically, militarily, or economically motivated (Avci, 2017; Buechler, 1995; Fuist, 2013). While the literature does adequately look at political and economic motivators for hacker activities, it falls short in understanding the motivations for why a person becomes a hacker, beyond political or financial gain (Holt, et-al, 2017; Nwalozie, 2015).

Chapter 3: Research Method

Ideally, there should be proactive disincentives that prevent people from becoming computer hackers (Hui et al, 2017). However, the general problem is that illegal computer breaches increased in the United States by 78% between 2013 and 2016 (ITRC, 2017). A possible cause of the increase in illegal hacking could be the limited understanding of exactly what factors encourage or discourage hacker behavior; factors such as 1) legal deterrence; 2) social/peer bonds; 3) personal attachment to people generally; 4) interactions with other hackers; 5) intellectual challenge; 6) revenge/retaliation; or 7) financial incentives (Chatterjee et al, 2015; Young and Zhang, 2007). The purpose of this quantitative non-experimental replication study was to relate the independent variables of punishment severity, punishment certainty, attachment to other socially conforming individuals, commitment to actions deemed acceptable by society, involvement a person has with activities deemed acceptable by society, belief (the degree to which an individual accepts the rules of society), and interactions with other hackers to the dependent variable of self-reported engagement in illegal hacking for individuals that identify as hackers online, as found within DefCon user groups, LulzSec Facebook page, the Anonymous YouTube feed, and through an open Facebook page developed for this survey.

RQ1. What is the relationship between punishment severity and reported engagement in illegal hacking?

RQ2. What is the relationship between punishment certainty and reported engagement in illegal hacking?

RQ3. What is the relationship between attachment to other socially conforming individuals and reported illegal hacking activities?

RQ4. What is the relationship between commitment to actions deemed acceptable by society and reported illegal hacking activities?

RQ5. What relationship exists between the involvement a person has with activities deemed acceptable by society and reported illegal hacking activities?

RQ6. What relationship exists between belief, which is the degree to which an individual accepts the rules of society, and reported illegal hacking activities?

RQ7. What relationship exists between interaction with other hackers and reported illegal hacking activities?

This chapter outlines the research methods and design of this quantitative non-experimental replication study. The population and sample size are defined; the survey instrument is discussed; variables are operationally defined; and the data processing, collection, and analysis are detailed. Finally, research assumptions, limitations, delimitations, and ethical considerations are addressed.

Research Methodology and Design

This study sought to gain insight into the larger population of the hacker culture. A quantitative non-experimental replication study provides an avenue to gain such knowledge (Cozby & Bates, 2012). This study used an online survey with appropriate statistical tests conducted to draw conclusions that are generalizable to the larger population.

A quantitative study facilitates results that can be generalized to a greater population (Cozby & Bates, 2012). Quantitative studies allow researchers to ascertain attitudes, opinions, and belief through the collection and analysis of data numerically (Park & Park, 2016). Then, take that data and find patterns or inconstancies (Park & Park, 2016). The ability to generalize findings to a larger population accomplishes the overall goal of this study to increase the understanding of motivational factors to become a hacker. A qualitative research design, such as a case study, is designed to discover information and address a specific instance or circumstance (Park & Park, 2016). Since the intent of qualitative research is to gain a deeper understanding of a specific instance or circumstance, it is not able to provide results that can be generalized to the same degree of rigor as a quantitative study; therefore, it would not meet the intended purpose of this study (Park & Park, 2016).

Replication studies provide many benefits to the research community. Replication studies can bring faulty or fraudulent results to light (Duvendack, Palmer-Jones, & Reed, 2017). Inversely, replication studies can confirm the finding, expand the understanding of findings, and can place finding in a current world context (Duvendack, Palmer-Jones, & Reed, 2017). To address the research questions, a quantitative non-experimental replication study design was employed. This study seeks to gain insight into behavior. The phenomena were assessed through an online survey in an uncontrolled environment to collect data on factors that influence behavior. This study did not seek to manipulate behavior; therefore, no treatment requiring a controlled environment is injected into the study.

The online survey utilized Qualtrics and included links to complete the survey posted in discussion forums geared to hackers. These forums include the DefCon user group forums for the national, international, and area chapters. In addition, a Facebook, Twitter, and YouTube feeds were developed with links to the survey, and link requests or comment posted with links to the survey were submitted to Anonymous, LulzSec, and other hacker groups Facebook and YouTube feeds.

Since there are no membership lists for hackers, self-identification was the primary method for gaining study participants. Self-identification, or self-selection, is an accepted form of gaining survey participants and can potentially increase survey participation online since the Internet provides a measure of anonymity not offered by in-person surveying (McInroy, 2016). Self-identification could lead to sampling bias, and limits the control the research has over the sample population (Khazaal, van Singer, Chatton, Achab, Zullino, Rothen, Thorens, 2014); however, reaching illegal computer hackers on the internet is the only practical way to find study participants.

The disclosure statement provided to every individual that agrees to complete a survey ensures the participant is aware of the purpose of the study, that only non-identifying information was collected, that their participation was voluntary, and that their responses are anonymous (CITI Program Collaborative Institutional Training Initiative at the University of Miami website, 2012). This study replicated the survey questions developed and validated by Young and Zhang (2007) for their study on enablers and detractors to engage in illegal computer hacking. The demographic questions help classify and categorize respondents.

Population and Sample

The general population for this study was individuals self-identified as criminal hackers, who carry out their activities through technological means. This population must meet basic general technology requirements, including resources available, such as a computer and internet connection, and at least low level technical skills that allow them to at a minimum watch online demonstrations of hacking techniques, or utilize either paid or free ‘resource kits’ that can be deployed against a target (Collistor, 2014; Pike, 2013). Through this definition, the population for this study could have come from anywhere in the world, and from anyone having access to the basic requirements and anytime.

With such a broad potential population, it was necessary to define the distinct populations for this study. This population meets the basic characteristics and qualifiers to participate in the study by having an internet connection and the ability to utilize that connection. The population size is refined and targeted through the placement of solicitations to participate in the survey on various hacker and hacktivist online forums. This includes websites, postings on known hacker/hacktivist social-media sites, and posting links to the survey on social media sites, including Facebook and Twitter. This population meets the basic characteristics and qualifiers due to their presence on hacker/hacktivist-related forums and their self-selection to participate in a survey on the topic of hacking.

The actual estimates of the size of this population are impossible to determine since the identities of individuals that participate in hacking activities are concealed by the internet (Collister, 2014), but the recent online activity of websites, such as Anonymous' Facebook page, have had hundreds of thousands of views. Additionally, Hyung-Jin Woo (2003) completed an online dissertation study on the relationship between psychological variables and hacking activities that included 1,385 hackers, from 30 countries. Furthermore, Holt, Kilger, Chiang, & Yang (2017) study exploring the correlates of individual willingness to engage in ideologically motivated cyber-attacks received online survey responses of 802 individuals.

To further distinguish the population, the sample included individuals who chose to participate in the online survey. Since there is no membership list of hackers or hacktivists, and since participation in hacker and hacktivist activities can be done by groups or individuals, the sample was defined as follows. The online survey population was not limited by location, and come from a sample of self-selected individuals, ages 18-65, who opted to take the survey from a link or requests posted on known hacker or hacktivist website and a Facebook and Twitter page. All participants met this definition.

Sample size is the primary way used in studies to assure that adequate power is available to detect outcomes, thus avoiding Type II errors and allowing for a study that can be generalized to a greater population (Cozby & Bates, 2012; Houser, 2007; Trochim & Donnelly, 2008). The 80% power-level is the minimally acceptable level (Houser, 2007). The standard for obtaining the desired power of 80% is the rationale for selecting the beta to alpha ration (Faul, Erdfelder, Lang, & Buchner, 2007; Mayr, Erdfelder, Buchner, & Faul, 2007). Additionally, the .05 alpha level is the typical standard set for eliminating Type I errors (Bennett, Briggs, & Triola, 2014; Jackson, 2012; Mayr et al., 2007; Trochim & Donnelly, 2008). To reduce Type I and Type II error probabilities, an initial calculation determined that a total sample size of 578 would be required to yield significant results for the online study groups (see Appendix B).

Materials/Instruments

The online survey gathered either nominal or interval data through questions that are closedeended or Likert-type scale. This allowed for the quantification of the results, and comparison between the independent variables and the dependent variables, as well as the gathering of non-identifying demographic data. In this study, the independent variables of 1)punishment severity; 2) punishment certainty; 3) attachment to other socially conforming individuals; 4) commitment to actions deemed acceptable by society; 5) involvement a person has with activities deemed acceptable by society; 6) belief (the degree to which an individual accepts the rules of society); and 7) interactions with other hackers to the dependent variable of self-reported engagement in illegal hacking. Study variables assessment used a Likert scale with values ranging from one to five. Demographic data, which is nominal in scale, included gender, age, income bracket, and education level.

Young and Zhang addressed survey content validity by conducting a literature review in which they identified, selected, and developed the appropriate phrasing for questions to measure the constructs (Young & Zhang, 2007). They followed this by activity by presenting the survey questions to a panel of subject-matter-experts to determine if the items were necessary to operationalize the survey constructs (Young & Zhang, 2007). As a final step, they interviewed two scholars familiar with criminology research and received their input on the constructs, measurement domains, and the appropriateness of the measures.

As an additional content validity step, this researcher contacted a sociology and criminology research methods professor and asked him to review the survey instrument. He reviewed the survey instrument as well as Young and Zhang's approach to content validity and issued the opinion that they had followed acceptable standards for the development of the instrument. Next, to assess the construct validity and reliability of this survey instrument, a principle-components-factor analysis, with a varimax rotation, was used, in conjunction with a reliability analysis with Cronbach's Alpha. For this analysis, the constructs of punishment severity, punishment certainty, attachment, commitment, involvement, and belief account for 80.56% of the total variance, which is above the 70% lower threshold identified by de Winter and Dodou (2016). Furthermore, Cronbach's Alpha is a statistical test used to determine the internal consistency of questions to gauge the reliability of the survey (Bonett & Wright, 2015). The generally accepted level of significance for this test is about a 0.7 lower limit (Bonett & Wright, 2015). All constructs for this analysis exceeded this level, and are described in greater detail in Chapter 4.

Operational Definition of Variables

The dependent variable for this study is self-reported engagement in illegal hacking. It is operationally defined as the likelihood that the independent variables in this study would motivate a person to participate in hacker behaviors. For this study, *hacker behaviors*, or engagement, including taking actions that would criminally access systems for gain through technological means. To measure the nominal dependent variable of self-reported engagement in illegal hacking, participants in a hacking activity that is considered outside the bounds of United States law. The question is presented in a "yes" or "no" format.

The independent variables, all of which are interval in nature, for this study are punishment severity, punishment certainty, attachment to other socially conforming individuals, commitment to actions deemed acceptable by society, involvement a person has with activities deemed acceptable by society, belief (the degree to which an individual accepts the rules of society), and interactions with other hackers. For this study:

Punishment severity. Punishment severity is the belief that if caught illegally hacking, the punishment would significantly disrupt one's life. It is an interval variable that is rated on a Likert scale of 1 (strongly disagree) to 5 (strongly agree).

Punishment certainty. Punishment certainty is the belief that someone who illegally hacks will get caught. It is an interval variable that is rated on a Likert scale of 1 (strongly disagree) to 5 (strongly agree).

Attachment. Attachment is the attachment a person feels to older and assumedly less criminal adults. It is an interval variable that is rated on a Likert scale of 1 (strongly disagree) to 5 (strongly agree).

Commitment. Commitment is the belief a person has that hard work has or will yield a better position in life. It is an interval variable that is rated on a Likert scale of 1 (strongly disagree) to 5 (strongly agree).

Involvement. Involvement is the individual's work or social connections to non-criminal activities in life. It is an interval variable that is rated on a Likert scale of 1 (strongly disagree) to 5 (strongly agree).

Belief. Belief is the degree to which an individual feels that the rules and norms of society are fair and that people should obey laws. It is an interval variable that is rated on a Likert scale of 1 (strongly disagree) to 5 (strongly agree).

Interaction with hackers. Interaction with hackers is the connection an individual has to others who illegally hack systems. It is an interval variable that is rated on a Likert scale of 1 (strongly disagree) to 5 (strongly agree).

As stated above, independent variables were measured through a Likert-based survey instrument with values from 1 (strongly disagree) to 5 (strongly agree), in which the higher value placed on the question scale will translate into a stronger motivation to engage in the dependent variable behavior. Scores for each of the independent variables were calculated to ascertain if any independent variable appears to have a stronger link to the dependent variable of self-reported engagement in illegal hacking. The scores were then classified on a scale of 1 to 5, where 1 is a low-risk of engaging in illegal hacking and 5 is high-risk. For overall propensity to engage in illegal hacking, scores below 2 are categorized as low, scores between 2 and 4 are categorized as medium-risk, and scores 4 and above are categorized as high-risk.

Additionally, nominal and ordinal demographic information, such as gender (nominal), age (ordinal), and marital status (nominal) are collected to add context to the results. This scoring is based on category selection, such as male/female, age range, or married/divorced/single. This data was summarized for the populations based on the category selections.

Study Procedures

Data was collected through an online survey utilizes Qualtrics. The survey was set up as a link from an open Facebook page and remained open through the entire data collection period, and until a sufficient number of usable responses were collected to satisfy the population and sample size requirements. To solicit potential study participants, posts and links to the survey were placed in forums geared to hackers. These forums, including the DefCon user group forums for the national, international, and area chapters. In addition, a Facebook, Twitter, and YouTube feeds were developed with links to the survey and link requests or comment posts with links to the survey will be submitted to Anonymous, LulzSec, and other hacker groups Facebook and YouTube feeds.

Data Collection and Analysis

In this study, the dependent variable is the self-reported engagement in illegal hacking, and the independent variables are: 1) punishment severity; 2) punishment certainty; 3) attachment to other socially conforming individuals; 4) commitment to actions deemed acceptable by society; 5) involvement a person has with activities deemed acceptable by society; 6) belief (the degree to which an individual accepts the rules of society); and 7) interactions with other hackers. Dependent variable assessment is conducted using a nominal scale yes/no answer. Independent variable assessment is conducted using a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Demographic data, which is nominal or ordinal in scale, were collected and included gender, age range, ethnicity, and marital status.

SPSS version 22, Statistical Package for Social Sciences, was used to encode results and appropriate statistical tests will be conducted. These tests include, but are not limited to, Chi-squares, cross-tabulations, and regression-analysis to help determine if any relationships existed between or among the variables. Data was analyzed to report on the descriptive characteristics (percentages) of study participants.

Sample size is the primary way used in studies to assure that adequate power is available to detect outcomes, thus avoiding Type II errors, and allowing for a study to be generalizable to a greater population (Cozby & Bates, 2012; Houser, 2007; Trochim & Donnelly, 2008). The 80% power level is the minimally acceptable level (Houser, 2007). The standard for obtaining the desired power of 80% is the rationale for the selecting the beta to alpha ration (Faul, Erdfelder, Lang, & Buchner, 2007; Mayr, Erdfelder, Buchner, & Faul, 2007). Additionally, the .05 alpha level is the typical standard set for eliminating Type I errors (Bennett, Briggs, & Triola, 2014; Jackson, 2012; Mayr et al., 2007; Trochim & Donnelly, 2008).

Assumptions

The hacker population is a diverse and difficult group to identify. It is unlike traditional activist groups, with membership lists or members that attend demonstrations. This population participates in activities from the general anonymity of any location with an internet connection. Thus, this study assumes that anyone who participates in this study is a self-described hacker. Hacking is also generally identified by governments as deviant behavior and often illegal; therefore, any participant in this study would also be assumed to be a member of a deviant and potentially illegal sub-culture. This study also assumes that participants in hacker activities are not bound or tied to locations or term lengths of participation. This is due to the low barriers of entry or exit to participating in hacker activities, which are an internet-enabled device, an internet connection, and a personal desire to act. It is further assumed that participants do not require any special skills or technical capabilities, due to the high availability of resources and tools to conduct hacker activities available on the internet.

The survey participants are self-identified, and it is assumed they answered the surveys truthfully. No identifying information was tracked regarding the surveys, and confidentiality and anonymity will be guaranteed to study participants. Furthermore, no questions were asked regarding specific hacking activities that participants have engaged in, only the general question of whether they believe that they have participated in a hacking activity that is outside the bounds of United States law. These steps should mitigate the issues of honesty in responses, by offering participants a level of assurance that their participation will not link them to specific illegal activities, that no tracking was conducted on an individual biases, and questions did not seek direct details on hacking participation.

Limitations

The sample was drawn based on a convenience procedure. This is due to the inability to identify a large enough sample for this population. Since no official membership lists or definitive source exists to identify a population, self-selection of study participants through online sites linked to hacker or hacktivist groups is the most viable method for reaching this population. This does present several potential study limits, including biased results and potential for the misrepresentation of the data, especially in relation to the general population (Cozby, 2012; Houser, 2007; Jackson, 2012). Biased results can occur due to limiting participation solicitations to known hacker/hacktivist sites (Jackson, 2012). Self-selection could lead to bias since individuals who choose to participate are willing to come forward to answer the study survey. To limit this, the survey was available to everyone interested in participating. The survey was open until adequate results were obtained. Misrepresentation and incomplete conclusions can also occur with this sampling method (Cozby, 2012; Jackson, 2012).

The study results are limited to the self-selected respondents; thus, the potential for misrepresentation and incomplete conclusions must be considered. An additional study limiter relates to the potential that a single individual could provide multiple responses. While IP address limiting is a possibility, the ability to mask an IP address or using IP hiding services, such as TOR or other Virtual Private Network (VPN) provider, make it impractical to attempt to limit the acceptance by IP address. What this means is that more than one person could be assigned the same IP address when they follow the link to complete the survey by the VPN provider they are using to access the internet. Since this population has to be skilled at masking their online identities to avoid prosecution, this study limitation must be accepted.

Delimitations

There are a number of delimitations for this study. This study's purpose is to gain insight into motivation factors, not specific causes for hacker participation or techniques used to conduct hacker activities. Therefore, no examination was conducted related to specific hacker actions discussed and only a literature review of hacker techniques is discussed for the purpose of clarification related to the types of activities that are conducted, not the specifics for the choice of hacker techniques used. This means that this study was not focused on hacker targets, what event or events triggered their hacker behavior, or hacker technologies.

Additionally, delimitations related to the population were chosen due to the availability of study participants. Due to a lack of membership lists or binding associations, the population selection had to occur where the most likely participants could be found. This means that online forums, where this activity occurs, were the best venues for discovering individuals to participate. The online population allows for the participation of diverse members of the hacker culture from around the globe, without the limitation of geography. Since hacking must be conducted through technological means, the online community, meaning anyone who possesses the ability to be online, provides the best venue to reach this community.

Ethical Assurances

IRB approval was sought and obtained prior to the collection of any data. Both technical-ethical concerns and special-population concerns must be addressed in this study. Since this study is based on activities that can be considered outside the bounds of legality, special precautions to ensure the rights and protections of the participants must also be addressed.

Throughout this study, bias was considered. Bias can prejudice or guide a study and must always be guarded against. Due to the nature of this study, there are risks to participants and the organizations/institutions the researchers are affiliated with, so full discloser of those risks must be made. Study participants are skilled at techniques that can be turned against both individuals and organizations that can cause harm to participants, researchers, affiliated organizations, and innocent organizationally or individually associated individuals that are not a part of the study. Potential harms included reputations, access to confidential or personal information of myself or others, including student populations, and cause financial or other harms to associated individuals. The types of study participants could include members of groups, such as Anonymous, known for causing electronic harm, and potential criminals who could view participation as an opportunity to conduct social-engineering towards gaining access to potential credentials that would allow for large system compromise.

Over-stated results could lead readers to the impression that this information means more than it does. There is a risk that this study could lead to criminal prosecution, if responses were tracked to individuals, and could lead to the participant being labeled or considered a legal offender. Due to this concern, and data handling concerns associated with assessing through an online survey, all research activities will be conducted on hardware encrypted media and on secured encrypted devices that are ‘air-gapped’ from the internet while analysis is conducted. This should meet ethical standards to protect the data and the institutions I am affiliated with.

In addition, hacking, in and of itself, often has legal implications, so questions must be designed in a way as to not allow for specific incidents to be discussed regarding actual hacker activities. The study sought to understand motivations to engage in hacker activities; therefore, questions did not ask about specific instances of criminal behavior and informed consent documents clearly articulate that the research is attempting to ascertain information regarding what motivates the study participants and not any information regarding specific hacker activities. The survey instrument did not contain identifying information. Informed consent information appeared at the beginning of the online survey.

Due to the anonymity of the internet and the self-selection of survey participants, it is possible that respondents will not answer the question about participation in illegal hacking activities. Since no identifying information will be ascertained, there will be only a minimal risk of harm to respondents, minimizing the risk in a lack of responses. In addition, the form had a checkbox at the top where they can check that they received, and were able to read, the informed consent document, reviewed it, and voluntarily agree to participate in the survey. Since the survey was openly available on the internet, everyone who comes into contact with the survey site will be asked to participate and subjects are not known to the researcher. All survey participants must be between the ages of 18 and 65. For this survey, participants had to indicate that they are over the age of 18, or their results will not be included. Since no data regarding criminality or identify information is kept on study participants a Certificate of Confidentiality was not necessary.

Summary

This research into hacking sought to quantitatively confirm findings from Young and Zhang's 2007 study on illegal hacking behaviors and gain insight into the deterrents and motivators for engaging in illegal hacking activities through the internet. This venue allowed for a larger survey setting and will confirm, or refute, the 2007 findings with a potentially larger population size, and allow respondents to reply in the actual environment, online, that they use to hack. Most research in this area focuses on the illegal hacking activities, illegal hacking sanctions, and defenses to hack-attack, and not the behavioral motivators or detractors to becoming a hacker (Chatterjee et al 2015; Collistor, 2014; Fuist, 2013; Tomblin & Jenion, 2016) and does not take into account other factors that encourage or deter individuals from engaging in illegal hacking activities, such as punishment severity or certainty, social bonds, commitment, attachment, and involvement; therefore, this study seeks to gain a deeper understanding of the phenomenon based on the actual perceptions of the hackers into their motives as they understand them.

The survey instrument allowed for data-collection processes to calculate standard statistical tests to determine if there are any correlations or significance between the study constructs and to draw conclusions, based on the research, that can be generalized to the population of hackers at large. This allowed for inference to the general population and additions to theory related to the motivations for individuals to become illegal computer hackers. A quantitative study was chosen so that results can be generalized to a greater population, since qualitative research, such as a case study is more apt to apply understanding to a particular circumstance or event and easily provide valid results to the general population.

The general population for this study must meet basic general technology requirements including resources available, such as a computer and internet connection, and at least low-level technical skills that allow them to, at a minimum, watch online demonstrations of hacking techniques, or utilize either paid or free ‘resource kits’ that can be deployed against a target (Collistor, 2014; Pike, 2013, Xiang, 2013). Due to a lack of membership lists or binding associations, the population selection had to occur where the most likely participants could be found, in an online internet-based environment. The online population allows for the participation of diverse members of the hacker culture from around the globe, without the limitation of geography.

Chapter 4: Findings

The purpose of this replication study is to relate the independent variables: 1)punishment severity; 2) punishment certainty; 3) attachment to other socially conforming individuals; 4) commitment to actions deemed acceptable by society; 5) involvement a person has with activities deemed acceptable by society; 6) belief (the degree to which an individual accepts the rules of society); and 7) interactions with other hackers to the dependent variable (self-reported engagement in illegal hacking for individuals that identify as hackers). Data are collected through an online survey distributed through online posts requesting participation through various forums. Facebook, Twitter, and YouTube sites for DefCon, Anonymous, and LulzSec were contacted and asked to post a link. In addition, dedicated Facebook and Twitter accounts were created with anonymous links to the survey.

Five-hundred-eighty-six surveys were collected through Qualtircs. Collected data was then transferred in SPSS, version 22, and evaluated for inconsistencies or incompleteness. Of the surveys collected, one did not affirm consent to participate in the research, one indicated consent but did not complete any other questions, and five selected the option not to consent. All seven of these responses were eliminated from the final data set, leaving a useable data set of 579 surveys for N=579. Within the useable data set, four surveys were missing age, 13 surveys did not have a gender-identifier selected, and 14 did not answer the question regarding marital status. Two surveys were missing responses to two questions, and two surveys were missing responses to one question. This chapter will present an examination of the validity and reliability of the study data, followed by an evaluation, and a summary of the results and findings.

Validity and Reliability of the Data

Sample size is the primary way used in studies to assure that adequate power is available to detect outcomes, thus avoiding Type II errors and allowing for a study to be generalized to a greater population (Cozby & Bates, 2012; Houser, 2007; Trochim & Donnelly, 2008). The 80% power level is the minimally acceptable level (Houser, 2007). The standard for obtaining the desired power of 80% is the rationale for the selecting the beta to alpha ratio (Faul, Erdfelder, Lang, & Buchner, 2007; Mayr, Erdfelder, Buchner, & Faul, 2007). Additionally, the .05 alpha level is the typical standard set for eliminating Type I errors (Bennett, Briggs, & Triola, 2014; Jackson, 2012; Mayr et al., 2007; Trochim & Donnelly, 2008). To reduce Type I and Type II error probabilities, a G score calculation determined that a total sample size of 578 would be required to yield significant results for the online study group (see Appendix B). This study obtained 579 results; thus, providing satisfactory assurances for Type I and Type II errors minimization.

A Kaiser-Meyer-Olkin (KMO) measure of sample adequacy with Bartlett's test of sphericity was conducted. Kaiser-Meyer-Olkin values closer to one, and Bartlett's test of sphericity significance values less than 0.05 indicate a factor analysis might be useful (Field 2009, 2013). Kaiser-Meyer-Olkin values above 0.5 are considered the minimum level of acceptability to yield consistent factors (Field, 2009; Field, 2013). A Kaiser-Meyer-Olkin analysis resulted in a value of .878, which exceeds the minimum threshold for factor analysis sample size sufficiency. Additionally, Bartlett's test of sphericity, which tests if your correlation matrix is an identity matrix, yielded a significance level 0.0. This result further confirms the adequacy of the sample size and the potential usefulness of a factor analysis with the data.

Construct validity and reliability. Construct validity is about inference and the degree to which that inference can be operationalized, measured, or translated into the theoretical construct of your research (Trochim & Donnelly, 2008). Construct validity is similar to external validity, in that it seeks to generalize, but is different, in that it seeks to generalize the measures to the theoretical constructs of the study (Trochim & Donnelly, 2008). Reliability differs from validity in that reliability is concerned with stability and consistency of the measurement tool (Jackson, 2012).

To assess the construct validity and reliability of this survey instrument, a principle-components-factor analysis, with a varimax rotation, was used, in conjunction with a reliability analysis with Cronbach's Alpha. A principal component analysis assumes that there are no unique variances and that the total variance is equal to the common variance (de Winter & Dodou, 2016). This analysis seeks to explain the total variance of all components. For components to be selected for further analysis they should generally explain at least 70% and 80% of the total variance (de Winter & Dodou, 2016).

For this analysis, the constructs of punishment severity, punishment certainty, attachment, commitment, involvement, and belief account for 80.56% of the total variance. Varimax rotation is employed when the correlation between components is unnecessary, or not important, so that load factors can be maximized (Kaiser, 1958). The research questions for this study assume that the factors are independent of each other; therefore, the varimax rotation is employed to maximized load factors. A potential impact on the interpretation of findings centers on the exclusion of the construct of inclusion. Young and Zhang (2007) eliminated this construct due to the cross-loading of factors. In this study, there was no cross-loading of factors detected.

Cronbach's Alpha is a statistical test used to determine the internal consistency of questions to gauge the reliability of the survey (Bonett & Wright, 2015). This test assumes unidimensionality, or that the question is only measuring one variable (Cronbach, 1951). All questions to assess independent constructs are based on a Likert scale and are therefore unidimensional. The generally accepted reliability alpha lower limit using the Cronbach analysis is 0.7 (Bonett & Wright, 2015). A lower alpha can indicate that there are not enough questions to assess that variable on the test, or that the questions to assess the variable are poorly interrelated (Cronbach, 1951). Cronbach's Alpha for the independent variable construct of interaction with other hackers was below the 0.7 lower limit; therefore, it did not meet the assumption of adequate questions or proper interrelatedness of the questions to assess the variable.

This differs from Young and Zhang's (2007) finding, in which the construct of interaction with others alpha was above the 0.7 lower limit and included in the logistic regression model. This could also have an impact on the interpretation of findings, due to this factors exclusion from the regression testing. All of the other independent variables, punishment severity and certainty, commitment, attachment, involvement, and belief all had Cronbach's Alphas higher than the 0.7 lower limit. The factor analysis also provides insight related to the reduction in variance. Table 1 demonstrates, from left to right, that the construct variance decreased. Severity accounted for more than 43% of the variance, with the next highest variance being slightly less than 11%. In total, the combined constructs of severity, certainty, belief, attachment, and commitment accounted for 80% of the variance. The results of the factor analysis are shown in Table 1.

Table 1

Factor Analysis, Mean, and Standard Deviation

	SE	CE	BE	AT	CO	IN
Severity1	0.898					
Severity2	0.642					
Severity3	0.903					
Certainty1		0.763				
Certainty2		0.873				
Certainty3		0.904				
Belief1			0.884			
Belief2			0.828			
Belief3			0.916			
Attachment1				0.957		
Attachment2				0.962		
Commitment1					0.933	
Commitment2					0.963	
Commitment3					0.911	
Involvement1						0.927
Involvement2						0.914
Cronbach's alpha	0.753	0.796	0.846	0.912	0.928	0.814
% of variance explained	43.049	10.605	9.118	7.808	5.526	4.449
Mean	3.560	1.865	2.866	2.185	2.919	2.585
Standard Deviation	0.804	0.711	0.987	1.004	1.126	1.138

Note: SE = Severity; CE = Certainty; BE = Belief, AT = Attachment; CO = Commitment; and IN = Involvement.

Evaluating validity and reliability. To ensure the credibility of the data, a comparison of the factor-analysis results between Young and Zhang's (2007) study and this study was completed. Table 2 indicates that a comparison between the individual-factor scores is generally proximate in the values for most individual factors. Furthermore, Young and Zhang (2007) found that the factor analysis explained approximately 72.72 % of the variance. A confirmatory factor analysis for this study indicates that 80.56% of the variance is explained by the factors. This total variance indicates that the factors extracted from this study align with the factors extracted in the Young and Zhang (2007) study. The results of this comparison shown in Table 3.

Table 2

Factor Analysis Comparison

	Young and Zhang (2007)	Current Study
Severity1	0.939	0.898
Severity2	0.912	0.642
Severity3	0.674	0.903
Certainty1	0.696	0.763
Certainty2	0.805	0.873
Certainty3	0.919	0.904
Belief1	0.808	0.884
Belief2	0.696	0.828
Belief3	0.411	0.916
Attachment1	0.824	0.957
Attachment2	0.777	0.962
Commitment1	0.873	0.933
Commitment2	0.896	0.963
Commitment3	0.888	0.911
Involvement1	0.853	0.927
Involvement2	0.812	0.914

Table 3

Comparison in the Percentage of Variance Explained

	Severity	Certainty	Belief	Attachment	Commitment	Involvement
Young and Zhang (2007)	8.943	12.040	6.196	6.224	32.653	6.668
Current Study	43.049	10.605	9.118	7.808	5.526	4.449

Additional assumptions. In addition to the assumptions discussed above, there are a number of assumptions related to the applied statistical tests that could impact the results. Logistic regression does not make many of the same key assumptions that are made in general or linear regression (Hilbe, 2016). In logistic regression testing, the dependent and independent variables do not require a linear relationship; however, independent variables must have a linear relationship to the log odds (Hilbe, 2016). Additionally, normal distribution and homoscedasticity are not required (Hilbe, 2016). Next, the dependent variable must be binary, in this case, it is a “yes” or “no”, and the variable is not measured by an interval, ration, or ordinal scale (Hilbe, 2016). For a binary logistic regression, the observations should not come from repeated measurements, and data matching should not occur (Hilbe, 2016). Furthermore, independent variables should have little to no multicollinearity, and if any correlation between the independent variables exists, the correlation should be low (Hilbe, 2016). A final assumption for logistic regression is a larger sample size. Each independent variable should have a minimum of 10 cases for the least frequent outcome (Hilbe, 2016). To assure this assumption is fulfilled, a review of the independent variable fields was conducted and there were no observed counts for the Likert scale responses under 10.

Results

A profile of respondents is listed in Table 2. Of the respondents, 469 were under age 30. This represents 82% of the respondents, of which 58% were between the ages of twenty-one and twenty-nine, and 42% were between eighteen and twenty. Of the 566 respondents who reported gender, 460 (81%) were male and 106 (19%) were female. Of the 565 responding to marital status, 408 (72%) reported that they were single. Four-hundred-thirty-six respondents (75%) reported that they engaged in some form of illegal computer hacking within the previous 12 months. Three-hundred-ninety-four respondents (68%) reported that they belonged to some type of hacking organization. Finally, 108 respondents (19%) indicated that they have been caught hacking in the past.

A Chi-square analysis was conducted on gender and individuals that hacked in the past year. Gender did not have a significant relationship, yielding a p-value of .148. Chi-square analysis was also conducted on gender and hacker organization membership, with no significant relationship discovered. Chi-square showed a significant relationship between marital status and participation in hacking in the past year (p<0.01). Among the 428 individuals that hacked in the last year, 337 were single. Furthermore, a Chi-square shows a significant relationship between marital status and hacker organization membership (p<0.05). Of the 385 respondents that reported being members of a hacking organization, 288 were single. Finally, Chi-square was conducted on age, gender, and marital status in relation to participants caught hacking. No significant relationships were found in these three analyses.

Table 4

Profile of Respondents

Age Range	N	%
18-20	198	34%
21-29	271	47%
30-39	69	12%
40-49	27	5%
50-59	7	1%
60-65	3	<1%
Missing	4	<1%
Gender		
Male	460	80%
Female	106	18%
Missing	13	2%
Marital Status		
Single	408	71%
Married	97	17%
Divorced	53	9%
Widowed	7	1%
Missing	14	2%
Number of respondents who hacked illegally in the last year	436	80%
Number of respondents who belonged to a hacking organization	394	68%
Number of respondents who have been caught hacking illegally	108	19%

The dependent variable for all research questions is binary, so binary logistic regression was used to test the hypotheses. In addition, the dependent variable is binary and the sample size was large enough for logistic regression. Generally, to have an adequate sample size for logistic regression, the sample should have a minimum of 10 cases of the least-frequent outcome for each independent variable (Bennett & Triola, 2014). The independent variable of punishment severity, punishment certainty, attachment to other socially conforming individuals, commitment to actions deemed acceptable by society, involvement with activities deemed acceptable by society, and the degree to which an individual accepts the rules of society met this condition. The third assumption of logistic regression is that the variables are independent of each other and not correlated with each other too highly (Bennett & Triola, 2014).

The omnibus tests of model coefficients yielded a model significance of 0.000, which is less than the significant p-value of 0.05. The Hosmer and Lemeshow test, which requires a significance greater than 0.05, had a significance level of 0.542. The overall model fit indicated a predictive level of 85% for this regression model and is higher than the null predictive model of 76.8%. The Wald statistic is used for significance testing and provided estimated coefficients for the hypotheses test for each research question, and the odds ratio was calculated.

Research question 1. What is the relationship between punishment severity and self-reported engagement in illegal hacking?

H1$_0$. Punishment severity is negatively related to self-reported engagement in illegal hacking.

H1$_a$. Punishment severity is positively related to self-reported engagement in illegal hacking.

$H1_n$. There is no relationship between punishment severity and self-reported engagement in illegal hacking

In contrast to the hypothesis, the binary logistic regression for this research question indicates that there is a positive relationship between punishment severity and the self-reported engagement in illegal hacking activity. While a positive relationship exists, the relationship is not statistically significant ($p<0.05$). The results are shown in Table 5.

Table 5

Regression Results for Punishment Severity

	Statistic
Parameter Estimate	0.098
Wald Chi-square	0.179
Odd Ratio	1.104
P-value	0.672

Research question 2. What is the relationship between punishment certainty and self-reported engagement in illegal hacking?

$H2_0$. Punishment certainty is negatively related to self-reported engagement in illegal hacking.

$H2_a$. Punishment certainty is positively related to self-reported engagement in illegal hacking.

$H2_n$. There is no relationship between punishment certainty and self-reported engagement in illegal hacking.

The binary logistic regression for this research question indicates that there is a positive relationship between punishment certainty and the self-reported engagement in illegal hacking. This relationship is significant ($p<0.05$). The regression results are shown in Table 6.

Table 6

Regression Results for Punishment Certainty

	Statistic
Parameter Estimate	0.772
Wald Chi-square	13.983
Odd Ratio	2.164
P-value	0.000

Research question 3. What is the relationship between attachment to other socially conforming individuals and self-reported engagement in illegal hacking?

H3$_0$. Attachment to other socially conforming individuals is negatively related to self-reported engagement in illegal hacking.

H3$_a$. Attachment to other socially conforming individuals is positively related to self-reported engagement in illegal hacking.

H3$_n$. There is no relationship between attachment to other socially conforming individuals and self-reported engagement in illegal hacking.

The binary logistic regression for this research question indicates that there is a negative relationship between attachment and self-reported engagement in illegal hacking activity. While a negative relationship exists, the relationship is not statistically significant ($p<0.05$). The results are shown in Table 7.

Table 7

Regression Results for Attachment

	Statistic
Parameter Estimate	-0.181
Wald Chi-square	1.614
Odd Ratio	0.834
P-value	.204

Research question 4. What is the relationship between commitment to actions deemed acceptable by society and self-reported engagement in illegal hacking?

H4$_0$. Commitment to actions deemed acceptable by society is negatively related to self-reported engagement in illegal hacking.

H4$_a$. Commitment to actions deemed acceptable by society is positively related to self-reported engagement in illegal hacking.

H4$_n$. There is no relationship between commitment to actions deemed acceptable by society and self-reported engagement in illegal hacking.

The binary logistic regression for this research question indicates a positive relationship between commitment to actions deemed acceptable by society and the self-reported engagement in illegal hacking. This relationship is significant ($p<0.05$). The regression results are shown in Table 8.

Table 8

Regression results for commitment

	Statistic
Parameter Estimate	0.900
Wald Chi-square	18.432
Odd Ratio	2.460
P-value	0.000

Research question 5. What relationship exists between the involvement a person has with activities deemed acceptable by society and self-reported engagement in illegal hacking?

H5$_0$. The involvement a person has with activities deemed acceptable by society is negatively related to self-reported engagement in illegal hacking.

H5$_a$. The involvement a person has with activities deemed acceptable by society is positively related to self-reported engagement in illegal hacking.

H5$_n$. There is no relationship between the involvement a person has with activities deemed acceptable by society and self-reported engagement in illegal hacking.

The binary logistic regression for this research question indicates that there is a positive relationship between involvement in actions deemed acceptable by society and the self-reported engagement in illegal hacking. This relationship is borderline significant due to a p-value of 0.05. A one-tail test of significance was conducted and resulted in a p-value of <0.05, confirming inclusion as a significant result. The regression results are shown in Table 9.

Table 9

Regression results for involvement

	Statistic
Parameter Estimate	0.442
Wald Chi-square	7.723
Odd Ratio	1.556
P-value (two-tailed)	0.005
P-value (one-tailed)	0.000

Research question 6. What relationship exists between belief, the degree to which an individual accepts the rules of society, and self-reported engagement in illegal hacking?

H6$_0$. Belief, the degree to which an individual accepts the rules of society, is negatively related to self-reported engagement in illegal hacking.

H6$_a$. Belief, the degree to which an individual accepts the rules of society, is positively related to self-reported engagement in illegal hacking.

H6$_n$. There is no relationship between belief, the degree to which an individual accepts the rules of society, and self-reported engagement in illegal hacking.

The binary logistic regression for this research question indicates that there is a positive relationship between the construct of belief and the self-reported engagement in illegal hacking. This relationship is significant ($p<0.05$). The regression results are shown in Table 10.

Table 10

Regression results for belief

	Statistic
Parameter Estimate	0.796
Wald Chi-square	15.453
Odd Ratio	2.217
P-value	0.000

Evaluation of the Findings

The findings of this survey differ from the results obtained by Young and Zhang in 2007. In their study, the construct of interaction was found to be significant; in this study, it was not significant. Young and Zhang (2007) identified a significant positive relationship to the construct of punishment severity. This study indicated a positive relationship, but that relationship was not statistically significant. Both studies found a negative relationship to attachment and engagement in illegal hacking; however, neither study found that relationship to be significant. The constructs of punishment certainty, commitment, involvement, and belief were found to have significant positive relationships to an individual’s propensity to engage in illegal hacking activities. This differs from the Young and Zhang (2007) study, in which they supported the conclusion of a negative relationship between punishment certainty, commitment, and belief.   Refer to Table 11 for a summary of the hypothesis tests.

Table 11

Analysis of hypotheses

Hypothesis	Results
H1$_0$. Punishment severity is negatively related to self-reported engagement in illegal hacking.	Reject
H1$_a$. Punishment severity is positively related to self-reported engagement in illegal hacking.	Reject
H1$_n$. There is no relationship between punishment severity and self-reported engagement in illegal hacking.	Supported
H2$_0$. Punishment certainty is negatively related to self-reported engagement in illegal hacking.	Reject
H2$_a$. Punishment certainty is positively related to self-reported engagement in illegal hacking.	Supported
H2$_n$. There is no relationship between punishment certainty and self-reported engagement in illegal hacking.	Reject
H3$_0$. Attachment to other socially conforming individuals is negatively related to self-reported engagement in illegal hacking.	Reject
H3$_a$. Attachment to other socially conforming individuals is positively related to self-reported engagement in illegal hacking.	Reject
H3$_n$. There is no relationship between attachment to other socially conforming individuals and r self-reported engagement in illegal hacking.	Supported
H4$_0$. Commitment to actions deemed acceptable by society is negatively related to self-reported engagement in illegal hacking.	Reject
H4$_a$. Commitment to actions deemed acceptable by society is positively related to self-reported engagement in illegal hacking.	Supported
H4$_n$. There is no relationship between commitment to actions deemed acceptable by society and self-reported engagement in illegal hacking	Reject
H5$_0$. The involvement a person has with activities deemed acceptable by society is negatively related to self-reported engagement in illegal hacking	Reject
H5$_a$. The involvement a person has with activities deemed acceptable by society is positively related to self-reported engagement in illegal hacking.	Supported
H5$_n$. There is no relationship between the involvement a person has with activities deemed acceptable by society and self-reported engagement in illegal hacking.	Reject
H6$_0$. Belief, the degree to which an individual accepts the rules of society, is negatively related to self-reported engagement in illegal hacking	Reject
H6$_a$. Belief, the degree to which an individual accepts the rules of society, is positively related to self-reported engagement in illegal hacking.	Supported
H6$_n$. There is no relationship between belief, the degree to which an individual accepts the rules of society, and self-reported engagement in illegal hacking.	Reject

General deterrence theory, or the use of penalties and punishment, have been relied upon by some governments to curb illegal hacking activities (Hui, Kim, & Wang, 2017). This study, through hypothesis 1 and 2, assesses the impact punishment severity and certainty have on an individual's engagement in illegal hacking. In relationship to punishment severity, this study did not find a statistically significant relationship between the construct and engagement in illegal hacking. This study did find anecdotal support for Young and Zhang's (2007) assertion that a positive relationship exists between punishment severity and engaging in illegal hacking; however, this claim cannot be supported by this research since the findings were not statistically significant.

Punishment certainty can be supported by this research but differs from the 2007 study. Young and Zhang demonstrated support for a negative relationship indicating that the tendency to participate in illegal hacking decreases as the chance of being caught increases (Young & Zhang, 2007). This study refutes this claim and supports the inverse. This study's results indicate that a positive relationship exists between punishment certainty and illegal hacking engagement, and indicates the likelihood of participation in illegal hacking activities increases as the chance of being caught increases. While this finding may sound counter-intuitive, some studies indicate that people are less inhibited to participate in online activities due to the anonymity of the internet (Xiang, 2013). Furthermore, technological advances, such as Virtual Private Networks, make it easier to hide the true location of an individual, so being caught illegally hacking and being arrested or prosecuted are substantially different from the past (Rege, 2012).

Additionally, the finding for social-bond theory constructs of commitment, involvement, and belief also differ from Young and Zhang (2007). It was hypothesized that commitment to actions and involvement in activities deemed socially acceptable, as well as acceptance of societal rules, would be related negatively to engagement in illegal computer hacking; therefore, the higher degree to which a person reportedly subscribes to socially accepted behaviors, the less they would engage in illegal computer hacking. This study found the inverse. Positive relationships were found between commitment to action deemed socially acceptable, involvement in activities deemed socially acceptable, and belief or the acceptance of society's rules to reported engagement in illegal hacking activities.

Summary

The purpose of this quantitative replication study was to determine if relationships existed between the dependent variable of engagement in illegal computer hacking and the independent variables of punishment severity, punishment certainty, attachment, belief, commitment, interaction, and involvement. Data were collected through an online survey and 579 viable responses were collected. To assess the survey instrument's validity, a principal components factor analysis with varamax rotation and Cronbach analysis was conducted and demonstrated sufficient survey instrument validity, except for the construct of interaction. This construct's Cronbach alpha was below the .7 standard acceptability rate.

A profile of study participants was developed from the 579 responses. The majority of respondents, 82%, were under the age of 30. Additionally, 19% of the respondents were female, and 72% reported being single. Furthermore, 68% of the respondents reported belonging to some type of hacking group. Finally, 75% of the respondents reported that they had engaged in some form of illegal computer hacking within the last year, and 19% indicated that they had been caught, in some way and at some point in their lives, illegally hacking. While a Chi-square analysis shows a significant relationship between marital status and hacker membership organization, there is no statistical significance between gender and reported engagement in illegal computer hacking.

Binary logistic regression was conducted on the remaining constructs. The test of model fitness indicated an 85% model fit; thus, the remaining constructs held a high degree of predictability for engagement in illegal hacking activities. The findings of this study differ greatly from the findings of Young and Zhang's (2007) study. The constructs of punishment certainty, commitment, involvement, and belief were found to have significant positive relationships to an individual's propensity to engage in illegal hacking activities. This differs from Young and Zhang (2007); they supported the conclusion of a negative relationship between punishment certainty, commitment, and belief.

This study did not find a significant relationship to punishment severity and the propensity to engage in illegal computer hacking. The study did find a counter-intuitive relationship between punishment certainty and illegal hacking engagement. This relationship indicates that the greater the certainty level for being caught, the greater the chance a person will engage in illegal hacker behaviors. The social-bond theory constructs of commitment, involvement, and belief also differ from Young and Zhang (2007). Positive relationships were found between commitment to action deemed socially acceptable, involvement in activities deemed socially acceptable, and belief or acceptance of society's rules to reported engagement in illegal hacking activities. This also counter-intuitively indicates that as increases in social connectivity occur, increases in illegal hacking engagement also occur.

Chapter 5: Implications, Recommendations, and Conclusions

Between 2013 and 2016, illegal computer-hacking breaches increased by 78%. If this trend continues, illegal computer-hacking breaches will increase between 12% and 40% per year (IRTC, 2017), continuing to cost billions of dollars (FBI, 2016). Most research into illegal hacking focuses on activities, sanctions, and defenses to hack attacks, and not on the behavioral motivators or detractors to becoming a hacker (Chatterjee et al 2015; Collistor, 2014; Fuist, 2013; Tomblin and Jenion, 2016). The research that exists also demonstrates continuing disagreement on the degree to which hacking behaviors influence, or correlate with, economic incentives and deterrence certainties (Hui et al., 2017), or socio-cultural motivators (Madarie, 2017; Udris, 2016).

The purpose of this quantitative, non-experimental, replication study of self-identified hackers is to determine the relationship of the independent variables of 1) punishment severity; 2) punishment certainty; 3) attachment to other socially conforming individuals; 4) commitment to actions deemed acceptable by society; 5) involvement a person has with activities deemed acceptable by society; 6) belief (the degree to which an individual accepts the rules of society); and 7) interactions with other hackers to the dependent variable of self-reported engagement in illegal hacking. This research, administered via an online survey, seeks to quantitatively confirm or refute findings from Young and Zhang's 2007 study on illegal hacking behaviors, and gain insight into the deterrents and motivators for engaging in illegal-hacking activities. An online survey format was selected to gain insight from a larger population of the hacker culture, and participant selection was conducted through known online hacker and hacktivist internet sites. Young and Zhang (2007) completed their survey, face-to-face, with about 122 individuals at a hacker conference; this online survey was able to gain results from 579 self-identified hackers.

Since there are no membership lists for hackers, self-identification is the primary method for soliciting study participants. Self-identification, or self-selection, is an accepted form of gaining survey participants, and can potentially increase survey participation online since the internet provides a measure of anonymity not offered by in-person surveying (McInroy, 2016); however, it could also lead to sampling bias, and it limits the control the research has over the sample population (Khazaal, van Singer, Chatton, Achab, Zullino, Rothen, Thorens, 2014). These limits include biased results due to self-selection and the location of (convenience sampling) participant recruiting, limited control of the honesty of study participants, which is assumed in this research, and the potential for incomplete responses.

A total of 579 usable questionnaires were obtained prior to survey deactivation. To assess the validity and reliability of the survey instrument, a principle-component factor analysis, and a Cronbach's Alpha analysis were conducted (Table 1), which resulted in all factors exhibiting acceptable levels of validity and reliability, except the factor of interaction with other hackers. This factor was removed from the logistic regression model. A profile of respondents (Table 2) was developed with Chi-square calculations to test for significant relationships between/among demographic characteristics.

Since the dependent variable, self-reported engagement in illegal hacking is binary, a binary logistic regression was used to test the hypotheses. Model fitness testing indicated a predictive level of 85%, with the interaction independent variable removed, due to the Cronbach's Alpha results. The logistic regression analysis found punishment certainty, commitment, involvement, and belief have significant positive relationships to an individual's propensity to engage in illegal hacking activities. This study did not find a significant positive or negative relationship between punishment severity and the propensity to engage in illegal computer hacking.

The remainder of this chapter focuses on the implications of this study's findings, recommendations for practice in the field of information security, recommendations for future research, and overall conclusions drawn from this study.

Implications

The results of this study have implications that can positively inform change at the individual, organizational, and societal level. Understanding motivations for actions enable pro-active decision-making related to risk reduction, threat analysis, attribution, and response (Shamsi, Zeadally, Sheikh, & Flowers, 2016). This section focuses on how the study answered the research questions, the fitness of the survey to answer those questions, and the factors that could have affected the outcomes.

RQ1/hypothesis. *What is the relationship between punishment severity and self-reported engagement in illegal hacking*? The purpose of this question was to determine if punishment severity influenced the likelihood that an individual would engage in illegal hacking behaviors. The survey statements, 1) if you were caught hacking illegally, your life would be severely disrupted; 2) the punishment for being caught hacking illegally is severe; and 3) if you were caught hacking illegally, it would have a detrimental effect on your future, were designed to test the hypothesis that punishment severity is negatively related to engagement in illegal hacking.

Pearson correlations indicated that the three variables were individually good predictors of punishment severity, meaning that if severity increased the engagement in illegal hacking would decrease. The binary logistic regression indicates that there is a positive relationship between punishment severity and the self-reported engagement in illegal hacking activity, meaning that as severity increased engagement in illegal hacking also increased. This result refutes the hypothesis that punishment severity has a negative or deterrent effect on an individual's propensity to refrain from illegal hacking behavior. While a positive relationship exists, the relationship is not statistically significant ($p<0.05$). This suggests, anecdotally, that the general deterrence model could have the effect of deterring individuals from engaging in illegal hacking behaviors (Lederman, 2015; *United States of America v. Dennis Owen Collins, et-al*, 2014), but this study cannot support claims that the general deterrence model, which advocates higher punishments and fines (Hui, Kim, & Wang, 2017), deters illegal hacking engagement. Young and Zhang (2007) found that increased severity of punishment did not lead to decreasing reports of illegal hacking behaviors.

RQ2/hypothesis. *What is the relationship between punishment certainty and self-reported engagement in illegal hacking?* The goal of this question was to determine if a perceived likelihood of being caught decreased the likelihood a person would engage in illegal hacking. The survey statements, 1) people who hack illegally will be caught eventually; 2) if other people were to hack illegally, on average, the chances they would be caught are small; and 3) if you were to hack illegally, on average, the chances you would be caught are small, were designed to test the hypothesis that punishment certainty is negatively, or inversely related to engagement in illegal hacking.

Pearson correlations indicated that the three variables were individually good predictors of punishment certainty. The binary logistic regression indicates that there is a statistically significant, positive relationship between punishment certainty and the self-reported engagement in illegal hacking activity. Young and Zhang (2007) found a negative relationship between punishment certainty and the likelihood to engage in illegal hacking activities, meaning that as the perception of being caught increased, the participation in illegal hacking activates decreased. The positive relationship discovered in this study indicates the opposite. This study indicates that, as the perceived likelihood of being caught increases, engagement in illegal hacking increases. This finding is counter to the classic tenets of criminology and general deterrence theory, which argue that increased chances of being caught deter illegal behaviors since people will rationally weigh risk and reward to avoid punishment (Dollar, 2014).

RQ3/hypothesis. *Attachment to other socially conforming individuals is negatively related to self-reported engagement in illegal hacking.* The intent of this question is to determine if attachment to others, in particular, older individuals, reduces the likelihood an individual will engage in illegal hacking behaviors. The survey statements, 1) I often talk to older adults about my future; and 2) I often talk to older adults about my thoughts and feelings were designed to test the hypothesis that attachment is negatively related to engagement in illegal hacking.

Pearson correlations indicated that the two variables were, individually, good predictors of attachment. The binary logistic regression indicates that there is no relationship between attachment to socially conforming older adults and the self-reported engagement in illegal hacking activity. Social-bond theory, as posited by Travis Hershi, states that people who have weak ties to society are more likely to commit deviant acts (Hershi, 1969; Kendall, 2006; Young & Zhang, 2007). Young and Zhang's (2007) findings differ from Hershi in that attachment to socially conforming older adults does not appear to affect participation in illegal hacking. This study does not find a negative, or alternately a positive relationship between attachment to socially conforming individuals and engagement in illegal hacking activities, and appears to confirm Young and Zhang's (2007) study that attachment and participation in illegal hacking do not appear to be linked. The implications of this finding tend to indicate that attachment to older adults does not play a role in predicting if an individual will hack illegally.

RQ4/hypothesis. *Commitment to actions deemed acceptable by society is negatively related to self-reported engagement in illegal hacking.* This question is to determine if commitment to actions deemed acceptable by society reduces the likelihood that a person will engage in illegal hacking activities. The survey statements, 1) I worked hard to get where I am now, 2) I work hard to get myself into a better position in the future, and 3) between school and/or my job, I work very hard, were designed to test the hypothesis that commitment is negatively related to engagement in illegal hacking.

Pearson correlations indicated that the three variables were, individually, good predictors of commitment. The binary logistic regression indicates that there is a positive relationship between commitment to socially conforming norms and the self-reported engagement in illegal hacking activity. Young and Zhang (2007) found a negative, or inverse, relationship, meaning that the greater commitment to societally accepted norms, the less likely an individual will participate in illegal actions and jeopardize their current or future positions in life. The implications of this study's findings contradict of Young and Zhang's (2007) study.

This study found a positive relationship between commitment and illegal hacking. As people (who work, or have worked hard to get where they are) felt more connected to conventional societal norms, they are more likely to engage in illegal hacking. This is a drastic shift from conventional theory on commitment. Commitment concerns the amount of time, effort, and expense that a person invests in societally deemed, appropriate actions (Hershi, 1969; Kendall, 2006; Young & Zhang, 2007). One possible explanation for this is the shift in the socio-economic status of hackers (Leederman, 2015). Leederman (2015) found that hackers, specifically hacktivist, increasingly come from families that are more affluent and report deeper ties to their communities. Another explanation, discussed by Leederman (2015) and Collister (2014) could be the rationale for the hacking. Hacktivism, a form of hacking, is a more widely used form of social activism and expression than in the past (Collister, 2014) and is conducted by individuals from many different backgrounds (Leederman, 2015). Respondents were solicited from websites for known hacker and hacktivist groups. Young and Zhang (2007) were limited to DefCon only. This survey also sought responses from both Anonymous and LulzSec online community members, known hacktivist sites. These respondents could be more willing to engage, due to a social cause or perceived social-justice issue (Collister, 2014).

RQ5/hypothesis. *The involvement a person has with activities deemed acceptable by society is negatively related to self-reported engagement in illegal hacking*. Involvement attempts to gauge a person's propensity to commit a deviant act, based on the time and effort they put into engaging in conventional activities and differs from commitment that gauges current position and future aspirations (Young & Zhang, 2007). Young and Zhang (2007) hypothesize that as involvement increases, engagement in illegal hacking decreases, using the statements, 1) I spend too much time at my job to do anything else, and 2) I spend too much time participating in social activities to do anything else.

Pearson correlations indicated that the two variables were individually good predictors of commitment. The binary logistic regression indicates that there is a positive relationship between involvement and self-reported engagement in illegal hacking activity. This follows the conventional social bond theory as posited by Hershi (1969). This positive relationship indicates that as time devoted to engaging in conventional activities increased, so did participation in illegal hacking activities. This is counter to what both Young and Zhang (2007) and Hershi

(1969) posited. A possible cause for this difference could include the proliferation of the internet. As online access has become more available, the number of internet users has increased, and the social characteristics of individuals online have increased (Prislan, 2016). A second potential factor to explain the discrepancy could include the nature of hacking itself. Hacking used to be more difficult and technical. Now hacking is ‘out of the shadows;’ and tools and techniques are easily available online (Krombholz et al., 2015). Another possible cause for the difference in results could be the change in how individuals interact. Digital natives view online interaction as a social activity (Prislan, 2016). This view could explain the positive relationship because study participants might have viewed online hacking as a social activity. Furthermore, an additional reason for the discrepancy could be based on the emergence of hacktivism. Hacktivism is the use of electronic means to bring about social or societal change through the manipulation of systems or data (Collister, 2014). Respondents might consider hacking justified and rationalize it as a socially constructive form of social justice regardless of legality. Anonymous, and other hacktivist groups, often undertake operations against targets based on actions they perceive to be unethical by the ‘offending’ party (Collister, 2014). In addition, research also points to the popularity of ‘information dump sites’, such as WikiLeaks, as a force for social change, based on the perceived unethical behavior of nations, organizations, and others in society (Cammaerts, 2014).

RQ6/hypothesis. *Belief, the degree to which an individual accepts the rules of society, is negatively related to self-reported engagement in illegal hacking.* Belief is a social-bond theory concept that seeks to gauge the acceptance of societal rules as a basis for an individual’s propensity to act in a societally acceptable way (Hershi, 1969; Young and Zhang, 2007). The theory assumes that a common set of values exists in society and that all individuals view those values as important (Hershi, 1969). The goal of this question is to determine if reduced reporting on accepting societal rules increased participation in illegal hacking. The survey questions of 1) society is better off having people follow the laws of the land; 2) society, in general, has fair and supportive norms; and 3) I am better off following the rules of society, were designed to test the hypothesis that belief is negatively related to engagement in illegal hacking.

Pearson correlations indicated that the three variables were individually good predictors of belief. The binary logistic regression indicates that there is a positive relationship between belief in social norms and self-reported engagement in illegal hacking activity. This finding indicates that as individuals' acceptance of societal norms increased, so did their participation in illegal hacking. The implications of this finding are counter to Hershi (1969), as well as Young and Zhang's (2007) finding, and suggest that individuals recognize and accept perceived societal norms, but continue to hack illegally. A possible cause for the difference could include a central criticism of social-bond theory in that societal norms or rules can be viewed more or less important by any individual (Fuist, 2013; Husu, 2013, Turner, 2013). Individuals view society, their place in society, and the norms or rules of society from their personal perspective; meaning that people place individual value judgments on what is important to them (Hershi, 1969). Since this survey population was broader than a single conference event, and participants were recruited from hacktivist organizations that support social causes, the respondents might feel that the use of hacking is justified in order to bring about social change (Collister, 2014).

Recommendations for Practice

The research findings presented contribute to understanding why people engage in and refrain from illegal hacking. It is clear from the findings that there has been a shift from the male-dominated hacker stereotype (Tanczer, 2016). Of the 566 respondents reporting gender, 460 (81%) were male and 106 (19%) were female. The 19% female response rate is in stark contrast to the 1% received by Young and Zhang (2007). Furthermore, Chi-Square tests indicated that there is not a statistical difference (p>0.05) that men hack more than women. This change indicates that the information-security field should expand its profile of the typical hacker to include women as a potential adversary.

As the chances of being caught hacking increases, so do the instances of illegal hacking have profound impacts on the field of information security. This finding indicates that current deterrents to hacking are not reducing people's willingness to engage in illegal computer hacking. This would indicate that current sanctions and detection capabilities are not strong enough to curb illegal hacking. With 75% of all survey respondents stating that they have hacked illegally within the last year, the risks of getting caught do not appear to outweigh the rewards that come from illegal hacking. This would suggest that the field of information-security practice should continue to examine and modify protection, punishment, and reward-deterrence strategies, in search of alternative or enhanced ways to curb illegal computer hacking.

With a significance of less than 0.05 (p<0.05), attachment to older individuals does not appear to have a deterring effect on illegal hacking. In the field of criminology, it is commonly accepted that attachments with conforming, older adults leads to reduced criminality (Hershi, 1996; Kendall, 2006). However, this finding indicates that the development of older/younger individual relationships, such as seen in mentoring programs, would do little to curb the problem of illegal hacking.

The factors of commitment, involvement, and belief all showed significant positive relationships to engaging in illegal hacking behavior. These findings also have a profound impact on the practice of information security. The findings show that as individuals subscribe more to societal norms, they increase their illegal hacking propensity. This leaves the field of practice looking beyond the traditional stereotype of a hacker or criminal hacker, to determine who is hacking and what they are attempting to accomplish.

Recommendations for Future Research

This study brings to light several areas that would benefit from continued investigation. Since the results of this replication study differ from the original, further replication could provide a clearer picture of the nature of the relationships between the research questions and factors that deter, or encourage, illegal computer hacking. Compared to the current study, the original study was over a decade ago, with one-fourth the number of respondents. This could explain some of the variances. Certainly, over a decade, the (sub) culture of hacking has changed significantly in terms of techniques and technologies, values, motivations, and rationales to engage in illegal hacking behaviors. Since the current study received four times the number of responses, it presumably represents the culture and changes to that culture more thoroughly than the original study, and discrepant findings, a decade apart, justify and warrant a third and fourth replication.

Future research could extend this study in many ways. Expanding the survey to a larger, international participant base could allow for more generalization to the hacker population. Both studies focused on hackers in the United States, but hacking is a borderless endeavor. Additionally, a demographic-based analysis of the data could help build a clearer profile of the modern "typical hacker," if one exists. In-depth analysis of gender, age, marital status, and additional factors, such as race or ethnicity, could shed light on who is hacking illegally.

Furthermore, expanding the study could determine an individual's primary motivation to hack, such as social cause, challenge, establishing one's reputation within the hacking culture, social justice, financial gain, or boredom, enhancing our understanding of the modern hacker. Finally, in relation to motivation, further study of hacking target groups might be able to identify trends and potential profiles associated with target types, such as corporations, nonprofits, religious institutions, government agencies (foreign and domestic), the military (foreign and domestic), financial institutions, or educational institutions.

Conclusion

Despite significant advances in defensive information-security technologies and government-enacted criminal penalties, hackers continue to misappropriate information, damage computer networks, deface websites, or deny authorized users access to online services (Collister, 2014; Prislan, 2016). While some argue that the underlying moral and ethical dilemmas faced in information technology have plagued society since the time of Aristotle (Kaptein, 2017), access to information and new technologies that enable nefarious, corrupt, or criminal exploitation of individuals and organizations have grown exponentially over the past 30 years (Rechtman, 2017). Citizens of the world now demand that information-technology professionals address these issues at the corporate and government institutional levels (Prislan, 2016) which requires a better understanding of the behavioral characteristics of hackers. The purpose of this quantitative, non-experimental replication study was to relate the variables of punishment severity and certainty, attachment, commitment, involvement, and belief to the variable of self-reported engagement in illegal hacking; enabling a clearer understanding of 'who' a modern hacker is.

The constructs of punishment certainty, commitment, involvement, and belief were found to have significant positive relationships to an individual's propensity to engage in illegal hacking activities. This is counter-intuitive to previous study findings and to both general deterrence theory and social bond theory. Some of the key takeaways from this study include that as the certainty of punishment increases and the individual’s acceptance of societal norms increases, their engagement in illegal hacking increases. The implications for how society must deal with current hackers is profound. These finding clearly demonstrate that deterring hacking attacks through technical means or punishment are ineffective. Further key takeaways include a shift in the gender of hackers. Analysis showed a substantial increase in the female hacker population, and that there is not a statistical difference ($p>0.05$) between men and women engaging in hacker behaviors. The implications from this find illustrate that the male-dominated stereotype of a hacker is no longer the norm.

In conclusion, when all of these findings are examined, the picture of who becomes a hacker is very different from the profile developed by Young and Zhang (2007). It is no longer a deviant behavior conducted by malcontent individuals or small groups of men hiding in basements. It includes both men and women who subscribe to generally conceived societal norms. This picture could be your next-door neighbor, your co-worker, or any other ‘typical” person you see on the street, or at your local coffee shop.

These results further indicate that general-deterrence theory and social-bond theory have limited, if any, application in reducing engagement in illegal computer hacking. This is very different from other studies of criminality that have shown increased punishment or social connectedness generally reduce illegal behavior (Dollar, 2014; Hershi, 1969). That, in turn, suggests that a pre-requisite for developing effective deterrence is the construction of suitable and explanatory theoretical paradigms. Prevention and deterrence that is not theoretically based and driven are serendipitously effective (hit and miss); therefore, continued research will ferret out the components of new theoretical modeling.

References

Accenture and HFS Research, Ltd., (2016). The state of cybersecurity and digital trust. Retrieved from https://www.accenture.com

Akers, R.L., Krohn, M.D., Lanza-Kaduce, L., & Radosevich, M. (1979). Social learning and deviant behavior: A specific test of a general theory. *American Sociological Review*, 44(4), 636-655. Retrieved from http:// eds.b.ebschost.com.libproxy.lib.ilstu.edu

Altuhhov, O., Matulevičius, R., & Ahmed, N. (2013). An Extension of Business Process Model and Notation for Security Risk Management. *International Journal of Information System Modeling and Design (IJISMD)*, 4(4), 93-113. doi:10.4018/ijismd.2013100105

Ambusaidi, M.A., He, X., Nanda P., & Tan, Z., (2016) "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm," in *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986-2998, Oct. 1 2016. doi: 10.1109/TC.2016.2519914

Armsden, G.C. & Greenberg, M.T. (1987). The inventory of parent and peer attachment: Individual differences and their relationship to psychological well-being in adolescence. *Journal of Youth and Adolescence* 16 (5). 427-454. https://doi.org/10.1007/BF02202939

Avci, E. *International Journal of Ethics Education* (2017) 2: 3. https://doi.org/10.1007/s40889-016-0027-6

Beccaria, C. d. (1775). *An essay on crimes and punishments,*. Printed for F. Newbery.

Becker, H. (1960). Notes on the Concept of Commitment, *American Journal of Sociology,* 66(1), 32-40. Retrieved from http://eds.b.ebschosgt.com.libproxy.lib.ilstu.edy

Bennett, J., Briggs, W. L., & Triola, M. F. (2014). *Statistical reasoning for everyday life* (4th ed). Boston, MA: Pearson.

Bhuyan M. H., Kashyap H. J.,. Bhattacharyya D. K, Kalita J. K. (2014). Detecting distributed denial of service attacks: Methods, tools and future directions. *The Computer Journal*, 57(4), 537–556. https://doi.org/10.1093/comjnl/bxt031

Boneh D., Corrigan-Gibbs H., Schechter S. (2016) Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks. In: Cheon J., Takagi T. (eds) Advances in Cryptology – ASIACRYPT 2016. ASIACRYPT 2016. Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-662-53887-6_8

Bonett, D.G, & Wright T.A. (2015). Cronbach’s alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior*, 36, 3-15. doi: 10.1002/job.1960

Buechler, S. M. (1995), New Social Movement Theories. *Sociological Quarterly*, 36: 441–464. doi:10.1111/j.1533-8525.1995.tb00447.x

Cao, G. H. (2015). Comparison of china-US engineering ethics educations in sino-western philosophies of technology. *Science and Engineering Ethics, 21*(6), 1609-1635. http://dx.doi.org.proxy1.ncu.edu/10.1007/s11948-014-9611-3

CITI Program Collaborative Institutional Training Initiative at the University of Miami website. (2012). Retrieved from: https://www.citiprogram.org/

Chatterjee, S, Sarker, S., & Valacich, J. (2015). The behavior roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, 31 (4), 49-87. https://10.1080/07421222.2014.1001257

Chhabra, M., Gupta, B., & Almomani, A. (2013, July). A novel solution to handle ddos attack in manet. *Journal of Information Security*, *4*(3), 165-179. http://dx.doi.org/10.4236/jis.2013.43019

Collister, S. (20*14*, November). Abstract hacktivism as a model for postanarchist organizing. *Ephemera: Theory & Politics in Organizations*, 14(4), 765-779. Retrieved from www.eds.b.ebschost.com

Computer Fraud and Abuse Act of 1984, 18 U.S.C § 1030 (1986).

Computer Misuse Act of 1990, 18 (1990)

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31-38. doi:10.19101/IJACR.2016.623006

Cozby, P. C., & Bates, S. C. (2012). *Methods in behavioral research* (11th ed.). New York, NY: McGraw-Hill.

Craig, A., Shackelford, S., & Hiller, J. (2015). Proactive cybersecurity: A comparative industry and regulatory analysis. *American Business Law Journal*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573787##

Cronbach LJ (1951). "Coefficient alpha and the internal structure of tests". *Psychometrika*. 16 (3): 297–334. doi:10.1007/bf0231055

Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. *International Management Review, 13*(1), 37-58,101-102. Retrieved from http://libproxy.lib.ilstu.edu/

Davis, S. (2014). Responsible technology. *The Serial Librarian*, 67, 12-20. http://10.1080/0361526x.2014.915607

Dawson J., & McDonald, J.T. (2016). Improving penetration testing methodologies for security-based risk assessment," *2016 Cybersecurity Symposium (CYBERSEC)*, Coeur d'Alene, ID, 2016, pp. 51-58. doi: 10.1109/CYBERSEC.2016.016

de Winter, Joost C. F., Dodou, D. (2016) Common factor analysis versus principal component analysis: A comparison of loadings by means of simulations. *Communications in Statistics - Simulation and Computation*, 45(1), 299-321. doi: 10.1080/03610918.2013.862274

Durkheim, É., & Wilson, E. K. (1981). The Realm of sociology as a science. *Social Forces*, 59(4), 1054-1072. Retrieved from http://eds.b.ebschost.com

Dutt, V., Ahn, Y., Gonzalez, C., (2013). Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, 55(3), 605-618. doi:10.1177/001872081246045

Duvendack, M., Palmer-Jones, R., & Reed, W. R. (2017). What Is Meant by 'Replication' and Why Does It Encounter Resistance in Economics. *American Economic Review*, *107*(5), 46-51. doi:10.1257/aer.p20171031

European Union (EU-GDPR). (2017). *General Data Protection Regulation*. Retrieved from https://www.iapp.org

Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop? *Crime Science*, *7*(1), 1–4. https://doi.org/10.1186/s40163-018-0082-8

Federal Bureau of Investigations. (2006). *Internet Crime Report*. Retrieved from https://www.ic3.gov/media/annualreports.aspx

Federal Bureau of Investigations. (2016). *Internet Crime Report*. Retrieved from https://www.ic3.gov/media/annualreports.aspx

Faul, F., Erdfelder, E., Lang, A., & Buchner, A. (2007, May). G power: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175-191. Retrieved from http://search.proquest.com.proxy1.ncu.edu/docview/204305161/138F82745CE2C6F1DF6/5?accountid=28180

Field, A. (2009). *Discovering statistics using SPSS* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Los Angeles, CA: Sage Publications.

Fitri, N. (2011, April). Democracy discourse through the internet communication: Understanding the hacktivism for the global change. *Online Journal of Communication and Media Technology*, *1*(2). Retrieved from http://www.ojcmt.net/articles/12/121.pdf

Fortinet. (2017). Threat landscape report. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/threat-reports

Fuist, T. N. (2013, July 12). Culture within sites, culture as a resource, and culture as wider context: A typology of how culture works in social movement theory. *Sociology Compass*, 1044-1052. Retrieved from http://eds.b.ebschost.com

Gordon, R.J. (2017). DDoS attack simulation to validate the effectiveness of common and emerging threats. *Journal of Information Warfare* 16(1), 49-63. Retrieved from https://www.jinfowar.com/journal-issue/volume-16-issue-1

Grasmick, H. & Bryjack, G. (1980). The deterrent effect of perceived severity of punishment. *Social Forces* 59(2), 471-491. Retrieved from www.eds.b.ebschost.com

Hafner, K. & Markoff, J. (1995). Cyberpunks: Outlaws and hackers on the computer frontier. Toronto: Simon and Schuster.

Hampson, N. (2012, Spring). Hacktivism: A new breed of protest in a networked world. *Boston College International & Comparative Law Review*, *35*(2), 511-542. Retrieved from www.eds.b.ebschost.com

Harrington, S. (n.d.) Cyber security active defense: Playing with fire or sound risk management. *Richmond Journal of Law and Technology*, 20 (4), 1-41. Retrieved from http://jolt.richmond.edu/jolt-archive/v20i4/article12.pdf

Heckman, K. E., Stech, F. J., Schmoker, B. S., & Thomas, R. K. (2015). Denial and Deception in Cyber Defense. *COMPUTER -IEEE COMPUTER SOCIETY-*, (4). 36. Retrieved from www.eds.b.ebschohost.com

Hirschi, T. (1969). *Causes of delinquency*. Berkeley: University of California Press.

Holt, T., Freilich, J., & Chermak, S. (2017). Exploring the subculture of ideological motivated cyber-attackers. Journal of Contemporary Criminal Justice, 33 (3), 212-233. https://10.1177/1043986217699100

Houser, J. (2007, March). How many are enough? Statistical power analysis and sample size estimation in clinical research. *Journal of Clinical Research Best Practices*, *3*(3). Retrieved from http://firstclinical.com/journal/2007/0703_Power.pdf

Hui, K., Kim, S, Wang, Q., (2017) Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *MIS Quarterly*, 41(2), 297-523. Retrieved from www.eds.b.ebschost.com

Husu, H. (2013). Bourdieu and social movements: Considering identity movements in terms of field, capital, and habitus. *Social Movement Studies*, *12*(3), 264-279. http://dx.doi.org/10.1080/14742837.2012.704174

Identity Theft Resource Center. (2017). IRTC breach statistics 2005-2016. Retrieved from http://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf

Internet World Stats. (2017) IWS internet usage statistics. Retrieved from https://www.internetworldstats.com/

Jackson, S. L. (2012). *Research methods and statistics: A critical thinking approach* (4th ed.). Belmont, CA: Wadsworth.

Jamal, A., Ferdoos, A., Zaman, M., & Hussain, M. (2015). Cyber-Ethics and the Perceptions of Internet Users: A Case Study of University Students of Islamabad. *Pakistan Journal of Information Management & Libraries*, *16*8-20. Retrieved from http://libproxy.lib.ilstu.edu/login?url=https://search.ebscohost.com/

Kaiser, H. (1958). The varimax criterion for analytic rotation in factor analysis. *Psychometrika*, 23 (3). doi:10.1007/BF02289233

Kaptein, M. (2017). The battle for business ethics: A struggle theory. *Journal of Business Ethics, 144*(2), 343-361. http://dx.doi.org.proxy1.ncu.edu/10.1007/s10551-015-2780-4

Kaptein, M. (2017). When organizations are too good: Applying aristotle's doctrine of the mean to the corporate ethical virtues model. *Business Ethics, 26*(3), 300-311. http://dx.doi.org.proxy1.ncu.edu/10.1111/beer.12147

Kamiya K., Aoki K., NakataK., SatoT., Kurakami H., & TanikawaM., (2015). The method of detecting malware-infected hosts analyzing firewall and proxy logs. *2015 10th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT)*, Colombo 22-24. doi: 10.1109/APSITT.2015.7217113

Kendall, D. E. (2006). *Sociology in our times: the essentials* (5th ed.). Belmont, CA: Thompson/Wadswoth.

Khazaal, Y., van Singer, M., Chatton, A., Achab, S., Zullino, D., Rothen, S., Thorens, G. (2014). Does Self-Selection Affect Samples' Representativeness in Online Surveys? An Investigation in Online Video Game Research. *Journal of Medical Internet Research*, *16*(7), e164. http://doi.org/10.2196/jmir.2759

Krips, H. (2012, March-May). New social movements, populism and the politics of the lifeworld. *Cultural Studies*, *26*(2-3), 242-259. http://dx.doi.org/10.1080/09502386.2011.636197

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22(Special Issue on Security of Information and Networks), 113-122. doi:10.1016/j.jisa.2014.09.005

Lederman, S. (2015, April). Councils and revolutions: Participatory democracy in anarchist thought and the new social movement. *Science & Society*, *79*(2), 243-263. Retrieved from http://eds.b.ebschost.com

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. *Crime, Law & Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Levy, S. (1984). *Hackers: heroes of the computer revolution*. Garden City, N.Y. Anchor Press/Doubleday, 1984.

Maan, P., & Sharma, M. (2015). Fuzzy improved decision tree approach for outlier detection in SMS. *International Journal of Computer Applications*, 119 (16), 6-10. Retrieved from https://pdfs.semanticscholar.org

Madarie, R. (2017). Hacker's motivations: testing Schwart's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology*, 11 (1), 78-97. http://10.5281/zenodo.495773

Macrae, A. (2013). Identifying threats in real time. *Network Security*, *2013*(11), 5-8. doi:10.1016/S1353-4858(13)70119-3

Marx, K., & Engles, F. (1883). *Das Kapital*.

Mayr, S., Erdfelder, E., Buchner, A., & Faul, F. (2007). A short tutorial of gpower. *Tutorials in Quantitative Methods for Psychology*, *3*(2), 51-59. Retrieved from http://www.tqmp.org/Content/vol03-2/p051/p051.pdf

McGregor, C. (2014). From social movement learning to sociomaterial movement learning? Addressing the possibilities and limits of new materialism. *Studies in the Education of Adults*, *46*(2), 211-227. Retrieved from www.eds.b.ebschost.com

McInroy, L. B. (2016). Pitfalls, Potentials, and Ethics of Online Survey Research: LGBTQ and Other Marginalized and Hard-to-Access Youths. *Social Work Research*, *40*(2), 83-93. doi:10.1093/swr/svw005

Murphy, S. (2011, September 10). Summer of Lulz: how hacktivists have exposed the sorry state of internet security. *New Scientist*, *211*, 46-49. http://dx.doi.org/10.1016/S0262-4079(11)62228-8

Neal, P., & Ilsever, J. (2016). Protecting information: Active cyber defense for the business entity: A prerequisite corporate policy. *Academy of Strategic Management Journal*, *15*(2), 15-35. Retrieved from http://libproxy.lib.ilstu.edu/login?url=https://search.proquest.com

Naik, N., & Jenkins, P. (2016) "Enhancing Windows Firewall Security Using Fuzzy Reasoning," *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, Auckland, 2016, pp. 263-269. doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.64

Nolan, C. (2017). The Edward Snowden Case and the Morality of Secrecy. *Catholic Social Science Review*, *22*291-310. Retrieved from http://libproxy.lib.ilstu.edu/login?url=https://search.ebscohost.com

North, M. M., Richardson, R., & North, S. M. (2017). Information security and ethics awareness: A concise comparative investigation. *Calitatea, 18*(160), 141-149. Retrieved from http://libproxy.lib.ilstu.edu/login?url=https://search.proquest.com/

Park, J., & Park, M. (2016). Qualitative versus Quantitative Research Methods: Discovery or Justification. *Journal Of Marketing Thought*, *3*(1), 1-7. doi:10.15577/jmt.2016.03.01.1

Preetha, G., Kiruthika Devi, B.J., & Mercy Shalinie, S. (2014) Autonomous agent for ddos attack detection and defense in an experimental testbed. *International Journal of Fuzzy Systems*, 16(4), 520-528. Retrieved from https://pdfs.semanticscholar.org/

Prislan, K. (2016). Efficiency of corporate security in managing information threats: An overview of the current situation. *Journal of Justice and Security*, (2) 128-147. Retrieved from www.eds.b.ebschost.com

Priyanka D. M. (2015). A review of recent peer-to-peer botnet detection techniques. *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, 2015, 1312-1317. doi: 10.1109/ECS.2015.7124797

Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107-56 (2001)

Pike, R. E. (2013). The ethics of teaching ethical hacking. *Journal of International Technology & Information Management*, 67-75. Retrieved from http://eds.b.ebscohost.com

Rechtman, Y. (2017). Shifting the risk of cybercrime. *The CPA Journal*. Retrieved from www.eds.b.ebschost.com

Rihan, D., Khalid, A., Osman, S.E., (2015) A performance comparison of encryption algorithms aes and des. *International Journal of Engineering Research and Technology*, 4(12), 151-154. Retrieved from https://www.researchgate.net

Scheuerman, W. (2016). Digital disobedience and the law. *New Political Science*, 38 (3), 299-314. http://dx.doi.org/10.1080/07393148.2016.1189027

Shukla, J., Singh, G., Shukla, P., & Tripathi, A. (2014). Modeling and analysis of the effects of antivirus software on an infected computer network. *Applied Mathematics & Computation*, 22711-18. doi:10.1016/j.amc.2013.10.091

Spyridopoulos, T., Karanikas, G., Tryfonas, T., & Oikonomou, G. (2013). A game theoretic defense framework against dos/ddos cyber attacks. *Computers & Security*, 38, 39-50. doi:10.1016/j.cose.2013.03.014

Sutherland, E. H. (1947). Principles of Criminology. 4th ed. Philadelphia: Lippincott.

Suroto, S. (2017) A review of defense against slow HTTP attack. *International Journal on Informatics Visualization*, 1(4), 127-134. http://dx.doi.org/10.30630/joiv.1.4.51

Taylor, P. A. (2005). From hackers to hacktivists: Speed bumps on the global superhighway. *New Media & Society*, *7*(5), 625-646. http://dx.doi.org/10.1177/1461444805056009

Teodorescu, R.M. Lita, I., Cioc, I.B, & Visan, D.A. (2015). Virtual instrumentation application for symmetrical and asymmetrical text encryption/decryption studying, *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI),* Bucharest, 2015, P-23-P-26.doi: 10.1109/ECAI.2015.7301245

Tomblin, J & Jenion, G (2016). Sentencing 'Anonymous': exacerbating the civil divide between online citizens and government. *Police Practice and research*, 17 (6), 507-519. http://dx.doi.org/10.180/15614263.2016.1205983

Tanczer, L. M. (2016). Hacktivism and the male-only stereotype. *New Media & Society*, *18*(8), 1599– 1615. https://doi.org/10.1177/1461444814567983

Trochim, W. M., & Donnelly, J. P. (2008). *Research methods knowledge base* (3rd ed.). Mason, OH: Atomic Dog.

Turner, E. (2013). New movements, digital revolution, and social movement theory. *Peace Review: A Journal of Social Justice*, *25*, 376-383. http://dx.doi.org/10.1080/10402659.2013.816562

Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *International Journal of Cyber Criminology*, 10(2). 127-146. Retrieved from www.eds.b.ebschost.com

Uduthalapally P. & Zhou B., "Improvement of ETSFS algorithm for secure database," *2016 4th International Symposium on Digital Forensic and Security (ISDFS)*, Little Rock, AR, 2016, pp. 63-67. doi: 10.1109/ISDFS.2016.7473519

United States of America v. Dennis Owen Collins, et-al, (2014) 1:13-cr00383-LO http://ia601002.us.archive.org/0/items/gov.uscourts.vaed.299616/gov.uscourts.vaed.299616.1.0.pdf.

Wakunuma, K., & Stahl, B. (2014). Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues. *Information Systems Frontiers*, *16*(3), 383-397. doi:10.1007/s10796-014-9490-9

Wellisz, C. (2016, September). The dark side of technology. *Finance & Development* Retrieved from www.eds.b.ebschost.com

Wolff, J. (2016). Perverse effects in defense of computer systems: When less is more. *Journal of Management Information Systems*, 33 (2), 597-620. http://10.1080/07421222.2016.1205934

Xiang, L. (2013, Fall). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology*, *27*(1), 301-330. Retrieved from http://eds.a.ebscohost.com.proxy1.ncu.edu/

Xu, Z., Hu, Q., Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, 56(4), 64-74. doi: 10.1145/2436256.246272

Young, R., & Zhang, L. (2007). Illegal computer hacking: An assessment of factors that encourage and deter the behavior. *Journal of Information Privacy & Security*, *3*(4), 33-52. Retrieved from http://learners.ncu.edu/

Appendix A: Survey

Factors Encouraging and Deterring Illegal Computer Hacking: Replicating and Extending Young and Zhang's Treatise on Illegal Computer Hacking Survey	
Demographic	
Age	18-20 21-29 30-39 40-49 50-59 60-65
Gender	Female Male
Marital Status	Single Married Divorced Widowed
Income	Less than $25,000 per year $25,001 - $50,000 per year $50,001 - $75,000 per year $75,000 - $100,000 per year Over $100,000 per year
Education Level	Less than High School High School Diploma (or Equivalent) Some College Bachelor's Degree Master's Degree Beyond Master's Degree
Punishment Severity	
If you were caught hacking illegally, your life would be severely disrupted	Strongly Disagree Strongly Agree 1 5
The punishment for being caught hacking illegally is sever	Strongly Disagree Strongly Agree 1 5
If you are caught hacking illegally, it would have a detrimental effect on your future	Strongly Disagree Strongly Agree 1 5
Punishment Certainty	
People who hack illegally will be caught eventually	Strongly Disagree Strongly Agree 1 5

If other people were to hack illegally, on average, this chances they would be caught is small (Reverse coded)	Strongly Agree Strongly Disagree 1 5
If you were to hack illegally, on average, the chances you would be caught is small (Revers coded)	Strongly Agree Strongly Disagree 1 5
Attachment	
I often talk with older adults about my future	Strongly Disagree Strongly Agree 1 5
I often talk with older adults about my thoughts and feelings	Strongly Disagree Strongly Agree 1 5
Commitment	
I work hard to get where I am right now	Strongly Disagree Strongly Agree 1 5
I work hard to put myself in a better position in the future	Strongly Disagree Strongly Agree 1 5
Between school and/or my job, I work very hard	Strongly Disagree Strongly Agree 1 5
Involvement	
I spend too much time at my job to do anything else	Strongly Disagree Strongly Agree 1 5
I spend too much time participating in social activities to do anything else	Strongly Disagree Strongly Agree 1 5
Belief	
Society is better off, having people follow the laws of the land	Strongly Disagree Strongly Agree 1 5
Society, in general, have fair and supportive norms	Strongly Disagree Strongly Agree 1 5
I am better off following the rules of society	Strongly Disagree Strongly Agree 1 5
Interaction with others	
I have witnessed other people hacking illegally	Strongly Disagree Strongly Agree 1 5
I have seen friends of mine hacking illegally	Strongly Disagree Strongly Agree 1 5

I hear my friends talk about hacking sometimes	Strongly Disagree Strongly Agree 1 5
Other	
Have you ever participated in a hacking activity that would be considered outside the bounds of that allowed by the court system in the last year	Yes No
Do you belong to a hacking organization	Yes No
Have you ever been caught hacking	Yes No

Appendix B: Population Estimates G Power Analysis test - Logistic regression

```
Options:      Enumeration method, Wald-
test  Analysis:      A priori: Compute
required sample size
  Input:      Tail(s)                          =  One
              Odds ratio                       =  1.3
              Pr(Y=1|X=1) H0                   =  0.2
              α err prob                       =  0.05
              Power (1-β err prob)             =  0.80
              R² other X                       =  0
              X distribution                   =  Normal
              X parm μ                         =  0
              X parm σ                         =  1
  Output:     Noncentrality parameter λ        =  6.189963
              Critical χ²                      =  2.705543
              Df                               =  1
              Total sample size                =  578
              Actual power                     =  0.800434
```

Appendix C: Survey Approval Letter

From: Lixuan Zhang [mailto:lixuan.zhang@gmail.com]
Sent: Friday, September 8, 2017 3:07 PM
To: Crouse, Kevin <ktcrous@ilstu.edu>
Cc: andinodr27@yahoo.com
Subject: Re: Your 2007 study of illegal hacking behavior

Kevin,

I am fine with you using the survey for your dissertation. Good luck with your dissertation.

Regards,
Lixuan