11-8-2019

The Cybercrime Triangle

Sinchul Back
sinchul.back@scranton.edu

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

THE CYBERCRIME TRIANGLE:

AN EMPIRICAL ASSESSMENT OF OFFENDER, VICTIM, AND PLACE

A dissertation submitted in partial fulfillment of

the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

INTERNATIONAL CRIME AND JUSTICE

by

Sinchul Back

2020

To: Dean John F. Stack, Jr.
Steven J Green School of International and Public Affairs

This dissertation, written by Sinchul Back, and entitled The Cybercrime Triangle: An Empirical Assessment of Offender, Victim, and Place, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

_____
Ryan Charles Meldrum

_____
Stephen Pires

_____
Alexander Perez Pons

_____
Kyung-shick Choi

_____
Rob T. Guerette, Major Professor

Date of Defense: November 8, 2019

The dissertation of Sinchul Back is approved.

_____
Dean John F. Stack, Jr.
Steven J Green School of International and Public Affairs

_____
Andrés G. Gil
Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2020

DEDICATION

This dissertation is dedicated to my father, Seungkap Back, my mother, Chayeon Kim, my mother-in-law, Jaesun Jung, my wife, Hyobin Sung, and my son, Doosan Ryan Back. All of you have walked on this journey side by side with me and dreamed with me.

ACKNOWLEDGMENTS

To my dissertation committee members, Dr. Rob T. Guerette, Dr. Ryan Charles Meldrum, Dr. Stephen Pires, Dr. Alexander Perez, and Dr. Kyungshick Choi, you have remained with me through this academic journey and have shaped my intellectual development. Thank you for the support, encouragement, and continuous substantive feedback. To my chair, Rob T. Guerette, you have encouraged me, celebrated with me, and most importantly challenged me to consistently do better, for that I am forever grateful.

To all of the faculty and staff in the Department of Criminology and Criminal Justice, you have each impacted my doctoral journey by providing immense support throughout this process. This has truly been a pleasurable experience and I thank you.

I am thankful for the many organizations, scholars, and practitioners that have helped facilitate my dissertation research along the way. First, to the Florida International University Graduate Assistantship, I am thankful for the monetary support, the emotional support, and the professional development opportunities. Second, I thank the Division of Information Technology at FIU for the data from the phishing campaign and cybersecurity awareness program which helped me obtain meaningful insight into topics that I am passionate about.

To Dr. Kyungshick Choi, my master's program professor and one of my excellent mentors, thank you for exposing me to social science research, encouraging me to pursue a Ph.D., believing in my potential, and always looking far beyond what I could only imagine. You will always be my mentor. The experience you provided me with during my time engaging in research projects at the Center for Cybercrime Investigation and Cybersecurity Center at Boston University shaped my dissertation research and continues

to be a fond memory. Thank you for allowing me to learn from you and continuing to serve as one of my mentors.

I am especially thankful for Dr. Lisa Stolzenberg, Dr. Carleen Vincent, and Dr. Chang. During a time when the practice and culture of teaching in the college setting has been intensely scrutinized at FIU, it could have been easy for you to close your doors to me as an educator. Rather, you chose to open your doors even wider. Thank you to the entire department for the countless hours that you all spent with me during meetings, interviews, ride-a-longs and more, which allowed me to conduct this research.

To all of the fellow graduate students (both inside and outside of my department) that have become my dearest friends along the way. You have uplifted me, motivated me, laughed with me, traveled with me, exposed me to new cultures and broadened my perspective. In five short years, we have created memories that I will cherish for a lifetime.

To my father, Seungkap Back, my mother, Chayeon Kim, my mother-in-law, Jaesun Jung, and my wife, Hyobin Sung, the love, guidance, patience, encouragement, and experiences that you have provided to and for me have truly made me a better person, a better scholar, and a better educator. Words fall short in expressing my sentiments of gratitude. To my son, Doosan Ryan Back, you continue to show me what a heart of kindness and generosity looks like. Thank you for always believing in me and inspiring me to do this work. To my relatives and friends, you have embodied what it means to persevere. Thank you for so generously passing that along to me.

ABSTRACT OF THE DISSERTATION

THE CYBERCRIME TRIANGLE:

AN EMPIRICAL ASSESSMENT OF OFFENDER, VICTIM, AND PLACE

By

SINCHUL BACK

Florida International University, 2020

Miami, Florida

Professor Rob T. Guerette, Major Professor

Information technology can increase the convergence of three dimensions of the crime triangle due to the spatial and temporal confluence in the virtual world. In other words, its advancement can lead to facilitating criminals with more chances to commit a crime against suitable targets living in different real-world time zones without temporal and spatial borders. However, within this mechanism, cybercrime can be discouraged if the offender is properly handled, the target/victim is well guarded, or the place is effectively managed (Wilcox & Cullen, 2018, p. 134). In fact, Madensen and Eck (2013) assert that only one effective controller is enough to prevent a crime. Given this condition of the crime triangle, it must be noted that each of these components (the offender, the target, and the place) or controllers (i.e., handler, guardian, and manager) can play a pivotal role in reducing cybercrime.

To date, scholars and professionals have analyzed the phenomenon of cybercrime and developed cybercrime prevention strategies relying predominantly on cybercrime

victimization (suitable targets) but have yet to utilize the broader framework of the crime triangle commonly used in the analysis and prevention of crime. More specifically, the dimensions of cybercrime offenders, places, or controllers have been absent in prior scientific research and in guiding the establishment and examination of cybercrime prevention strategies. Given this gap, much remains to be known as to how these conceptual entities operate in the virtual realm and whether they share similarities with what we know about other crimes in the physical world. Thus, the purpose of this study is to extend the application of the "Crime Triangle," a derivative of Routine Activity Theory, to crime events in the digital realm to provide scholars, practitioners, and policy makers a more complete lens to improve understanding and prevention of cybercrime incidents. In other words, this dissertation will endeavor to devise a comprehensive framework for our society to use to form cybersecurity policies to implement a secure and stable digital environment that supports continued economic growth as well as national security.

The findings of this study suggest that both criminological and technical perspectives are crucial in comprehending cybercrime incidents. This dissertation attempts to independently explore these three components in order to portray the characteristics of cybercriminals, cybercrime victims, and place management. Specifically, this study first explores the characteristics of cybercriminals via a criminal profiling method primarily using court criminal record documents (indictments/complaints) provided by the FIU law library website. Second, the associations between cybercrime victims, digital capable guardianship, perceived risks of cybercrime, and online activity are examined using Eurobarometer survey data. Third, the associations between place management activities and cybercrime prevention are examined using "Phishing Campaign" and "Cybersecurity

Awareness Training Program" data derived from FIU's Division of Information Technology.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION: CYBERCRIME

The Internet and information technology systems have dramatically changed the way individuals communicate, interact, and conduct business around the globe. Computer and information systems play a pivotal role in government and industry sectors as well as individuals' lives. As such, many benefits have been derived from such technological evolutions. However, such technological advancements have also provided cybercriminals great opportunities with efficient tools to exploit online users. In other words, cybercriminals are abusing these opportunities to use illicit means to achieve their criminal goals. At the same time, these criminal activities inspire fear in online users and lead to a lack of trust in the security and safety of information technology and e-commerce (Taylor, Fritsch, Liederbach, Saylor, & Tafoya, 2019). Furthermore, the Information Age has unleashed numerous challenges and obstacles for law enforcement officials to effectively enforce and prosecute cybercrime. This is because cutting-edge technologies can assist cybercriminals in reducing their risk of detection and apprehension by law enforcement.

The Department of Justice asserts that cybercrime is one of the most serious national security threats facing the United States in recent years (Scams and Safety, 2016). Moreover, the U.S. government implements cybersecurity policies against cyber threats (e.g., cyberattacks, cyber espionage, intellectual theft, and phishing, etc.) as one of their top priorities. In fact, cybercrime poses a threat to national security and the nation's economic well-being as well as individual online users' properties. For example, due to Chinese hackers in 2013, China obtained vast amounts of intellectual information, in particular sensitive information regarding the new US stealth jet, and the F-35 Lightning

jet (Grabosky, 2015). In another example, a Connecticut man was charged with stealing bitcoins in an online phishing scheme (Scams and Safety, 2016). The defendant posted fake links to online marketplaces on dark web forums. These fake links directed online users to a fake login page that looked like legitimate login pages. When online users tried to log in, he stole their usernames and passwords, which were utilized to steal the bitcoins. The point in highlighting these two cases is that crime in cyberspace can pose grave threats to the greater society.

In fact, the 2018 FBI's Internet Crime Complaint Center (IC3) Report (Internet Crime Complaint Center, 2018) indicates that a total of 351,936 Internet crime incident reports were received from cybercrime victims in the United States with reported financial losses exceeding $2.7 billion. The Center for Strategic and International Studies (Lewis, 2006, 2018) estimated that cyber threats (cyberattack, internet fraud, intellectual espionage, cybercrime, and cyberterrorism) cost approximately 1 percent of the Gross Domestic Product (GDP) in the United States, with a loss of $600 billion per year. Also, these cyber threats create opportunity costs such as service and employment disruptions and the additional cost of securing networks, insurance, and recovery from cyber threats (Lewis, 2006, 2018). Consequently, cyber threats, directly and indirectly, hurt the economic well-being and national security of the United States.

Statement of the Problem

Technological advancement has fundamentally altered the paradigm of crime and criminal justice on a worldwide scale (Taylor et al., 2019). Information technology can increase the convergence of three dimensions (i.e., cyber offender, cybercrime victim, and cyberspace) of the crime triangle due to spatial and temporal confluence in the virtual world.

In other words, technology's advancement provides criminals with more chances to commit crimes against suitable targets living in different real-world time zones without temporal and spatial borders. However, within this context, cybercrime can be discouraged "if the cyber-adversary is handled, the target/victim is guarded, or the place is effectively managed" (Wilcox & Cullen, 2018, p. 134). Madensen and Eck (2013) assert that only one effective controller is enough to prevent a crime incident Given this condition of the crime triangle, it must be noted that each of these components (the offender, the target, and the place) or controllers (i.e., handler, guardian, and manager) can play a pivotal role in reducing cybercrime. In this sense, each component of the crime triangle should be thoroughly explored as a key factor in crime control strategies within the context of cybercrime.

Many scholars have attempted to understand and identify the causes of crime events and victimization in a physical environment using Cohen and Felson's (1979) routine activity theory (RAT). In an attempt to explain rising crime trends observed in metropolitan areas, the RAT approach was presented to identify the causal role that opportunity plays in crime (Felson, 1987). Cohen and Felson (1979) contended that crime occurs when there is a convergence in space and time of three elements: (1) a motivated offender, (2) a suitable target, and (3) the absence of a capable guardian against crime. Thus, crime can increase (or decrease) even when the number of potential offenders remains the same. In recent years, the RAT perspective has been applied to the explanation of cybercrimes including cyberstalking, cyber-harassment, cyberbullying, internet fraud, identity theft, hacking, and malware infection (see Morgan, Maguire, & Reiner, 2012). However, to date, while a growing body of research in criminology and crime science has

focused on cybercrime victimization, this literature provides little insights into the causal mechanisms that underlie cybercrime offense and cyber-place management (Pratt, Holtfreter, & Reisig, 2010).

In a broad sense, Clarke and Eck (2005) argue that traditional criminology attempts to improve understanding of the psychological and social forces that cause individuals to become criminals. Traditional criminology tries to account for why some individuals are more likely than others to commit criminal and deviant acts from the offender perspective (e.g., motivation). In contrast, crime science focuses on addressing how individual criminal propensity and environmental factors "facilitate, promote, or provoke, criminal events" (Cockbain & Laycock, 2017, p. 2; Junger, Laycock, Hartel, & Ratcliffe, 2012). Cockbain and Laycock (2017) explain that crime science's theoretical underpinning derives from opportunity theories of crime such as routine activity theory (Cohen & Felson, 1979), the rational choice theory (Clarke & Cornish, 1985), and crime pattern theory (Brantingham & Brantingham, 1981). Indeed, crime science can provide tentative answers to questions regarding how individual criminal propensity or environmental conditions affect a potential offender's decision to engage in crime.More specifically, crime science can account for how the changes of these conditions (e.g., cybersecurity settings, virtual environment) result in a reduction of cyber threats as a cybercrime prevention strategy through identifing and suppressing cybercriminal opportunity structure.

As a method of crime science, the crime triangle framework can clearly help address crime problems in our society (Cockbain & Laycock, 2017). For example, over the last few decades, crime science research has demonstrated that the problem analysis triangle (crime triangle) framework could be applied as a useful analytic method to help in

everyday police work (Scott, Eck, Knutson, & Goldstein, 2008). The crime triangle framework consists of the three sides representing the offender, the target, and place and is grounded in routine activity theory's dynamics (a motivated offender, a suitable target, and the absence of a capable guardian). Despite the significance of the application of the crime triangle to crime, there is no empirical study that applies this theoretical framework to establish effective cybercrime control strategies.

Purpose of the Study

To date, scholars have analyzed the phenomenon of cybercrime and have developed cybercrime prevention strategies mainly focusing on cybercrime victimization (suitable target) and have largely ignored the other aspects of the crime triangle (i.e., cybercrime offenders, places, or controllers). That is, the determinants of cybercrime offenders, places, or controllers have been less often applied in establishing cybercrime prevention strategies. Given this, the existing literature might be unable to reveal the exact causal factors of cybercrime. Consequently, the purpose of this study is to propose the application of the crime triangle framework to crime events in the digital realm to provide scholars, practitioners, and policy makers a crime science lens to better understand cybercrime events. As a result, this dissertation will endeavor to devise a comprehensive framework to form a more effective blueprint of cybercrime control and cybersecurity policies to better ensure a secure and stable digital environment that supports continued economic growth as well as national security.

The Significance of the Study

The present study may help in the development of an effective cybercrime prevention strategy. First, this study can provide a comprehensive perspective of a cybercrime event, which can be utilized as a starting point to design cybercrime prevention and detection strategies based on the crime triangle framework. The use of this framework can help identify the patterns of crimes. In particular, by illuminating the situations and the places that the cybercrimes occurred, and noting the techniques used to commit the cybercrimes (Baker & Wolfer, 2003).

Second, Hirschfield (2017) asserts that "the targeting of interventions is intrinsically linked to the 'mechanisms' considered to be responsible for generating crime" (p. 493). The present study is an early initiative of the evaluation research conducted by place management strategies on the targeting of cybercrime interventions to reduce cybercrime in the public sector (a public university). Specifically, the current study evaluates an intervention that attempts to boost the resilience of potential victims (e.g., through cybersecurity awareness training). The findings of this evaluation can provide new insights into the usefulness of crime prevention in the online domain and people's behaviors in response to cyber threats in virtual settings.

Third, the present study is significant because it addresses a gap in the criminological literature. The current research of RAT by Cohen and Felson (2016) focused only on suitable targets and the absence of capable guardians. Nevertheless, they examined whether changes in routine activities at the aggregate level would be positively related to reducing crime rates; however, Cohen and Felson did not provide any measure of perpetrator's situational conditions and opportunities (Madero-Hernandez & Fisher, 2012;

Wilcox, Land, & Hunt, 2003). In a related sense, previous tests of RAT did not focus on clarifying the sources of criminal situational factors and opportunity factors or illustrating why individuals vary in their propensity to commit crimes. Using the cybercriminal profiling approach, this study will be able to gain insights for individual differences in criminal inclinations.

Overview of Chapters

This dissertation will be organized as follows. Chapter 2 will review the literature on the topic examined in this study. Also, this chapter will explore the current trend in cybercrime over the past 18 years. A review of the literature illustrates the links between (1) environmental criminology, and (2) routine activity theory and the crime triangle framework to explicate crime events. A discussion of the theoretical background of routine activity theory and the crime triangle for cybercrime events will follow. The second chapter will conclude with identification of gaps in the research literature and the importance of the application of the crime triangle framework for cybercrime study.

Chapter 3 will explore the characteristics of cybercriminals via a criminal profiling method using criminal record documents (i.e., indictments/complaints) retrieved from the Law School library website at Florida International University (FIU). This study will use descriptive/regression models to provide answers to the questions of which, what, where, and how cybercrime offenders attack suitable targets in the United States. After conducting the cybercriminal profiling analysis, this study will delineate sociodemographic factors, situational factors, opportunity factors, attack severity, and damage type.

In Chapter 4, the associations between cybercrime victims, digital capable guardian, perceived risk of cybercrime, and online activity will be examined using Eurobarometer survey data. A cross-sectional research design is used to reveal the nature of cybercrime victimization. The findings of the correlation and regression analyses will be discussed; and then a discussion and conclusion, and limitations of the study will close this chapter.

In Chapter 5, the association between place management activities and cybercrime prevention will be examined using "Phishing Campaign" and "Cybersecurity Awareness Training Program" related data derived from FIU's information technology division. This phase will employ a quasi-experimental design. The data will be analyzed by t-test, Mann Whitney U-test, and logistic regression methods to evaluate the effectiveness of the phishing prevention training program at FIU. The results of the effectiveness of the cybercrime prevention program will then be presented. This chapter will end with a discussion of the findings, conclusions, and limitations of this study.

Chapter 6 will conclude the dissertation. This chapter will discuss the results of all three phases of the study. The aim is to ground the findings in the existing literature. The chapter will also include a discussion of policy implications for policy makers and practitioners in the United States and internationally. Specifically, this discussion will focus on how to enforce the strengths of the crime triangle framework in the digital realm to combat and deter sophisticated cybercriminals.

CHAPTER 2

LITERATURE REVIEW: CYBERCRIME AND THE CRIME TRIANGLE

This dissertation attempts to magnify the lens of the cybercrime triangle framework to contribute to the literature on cybercrime prevention. Three bodies of research are examined in this chapter. First, an overview of cybercrime is presented that describes the current issues, trends, and problems in the cybercrime literature so that it may help the audience have a better understanding of the cybercrime phenomenon. Second, this chapter focuses its attention on environmental criminology and crime analysis, as well as the historical roots of the environmental perspective. Third, previous research will be discussed regarding routine activity theory, the crime triangle framework, and cybercrimes. To that end, the goal of this chapter is to explain the applicability of the crime triangle framework to cybercrime research.

Cybercrime

In order to better understand cybercrime issues in the United States, this section provides definitions of criminal offenses in the digital space, classifications of cybercrime, and overall trends in cybercrime.

Defining the Terms. This section briefly discusses the definition of cybercrime, computer crime, hacking, internet fraud, intellectual espionage, and cyberterrorism. Cybercrime studies are an emerging field of research; therefore, there are still significant inconsistencies in defining these types of offenses. Thus, this section can contribute to filling a gap in the existing literature through providing the most common and solid definitions of the cybercrime types stated above. First, cybercrime is a “computer-assisted

crime," which involves computers in a supporting role in the commission of a crime, while computer crime is a "computer-focused crime," which is the direct result of computer technology, such as hacking (Albanese, 2011; Brenner, 2010; Choi, 2015; Computer Misuse Act 1990; Holt, Burruss, & Bossler, 2015). Second, hacking is defined as a deviant act that is "analogous to the crime of trespass; it engages in a violation of a use restriction on the property that is committed by someone who has no right to access the property" (Brenner, 2010, pp. 50-1). Third, cyberterrorism is defined as "the use of digital technology or computer-mediated communications to cause harm and force social change against a civilian population based on ideological or political beliefs" (Brenner, 2010; Britz, 2010; Foltz, 2004; Holt et al, 2015, p. 10; Pollitt, 1998). Fourth, the U.S. Department of Justice defines intellectual espionage (economic/industrial espionage) as an act that violates the value of intellectual property and trade secrets related to the economic well-being and national security under the Economic Espionage Act of 1998 (Economic Espionage, 2016). In this regard, many cybercriminologists assert that cybercrime primarily encompasses computer crime, hacking, internet fraud, cyberterrorism, and cyber espionage (Brenner, 2010; Choi, 2015; Holt et al., 2015). Thus, cybercrime will be utilized as an umbrella term, which includes the aforementioned concepts.

Classifications of Cybercrime. Cybercrime can be classified into four categories: (1) cyber-trespassing, (2) cyber-deception/theft, (3) cyber-pornography, and (4) cyber-violence (Choi, 2015; Wall, 2001, pp. 3-7):

- Cyber-trespassing is the act of accessing unauthorized property/facility or causing damage including hacking, cyberattack, defacement, or viruses.

- Cyber-deception/theft is defined as stealing money and property or personal information (e.g., credit card fraud, identity theft, online auction fraud, economic espionage).
- Cyber-pornography is an activity that breaches laws on obscenity and decency (e.g., child pornography, online sexual exploitation, possession/distribution of child pornography online).
- Cyber-violence is defined as the act of committing psychological harm or the intention to hurt others, thereby breaching laws concerning the protection of the person (e.g., hate speech, cyber terrorism, cyberstalking).

Overall Trends in Cybercrime. In parallel with the increased use of information technology by virtually every citizen, new cyber threats are emerging. For example, information technologies are currently utilized to perform many traditional criminal acts such as child pornography, financial crimes, espionage, sexual exploitation, stalking, identity theft, drug trafficking, organized crimes, and terrorist activities (Taylor et al., 2019). In this regard, the characteristics of cybercriminals are very diverse. Moreover, the exponential growth of information technology and digital infrastructure may provide cyber-perpetrators new methods (e.g., Windows/Mac/Android malware, malware distribution methods, scams) and create cybercriminal-friendly environments with black markets (e.g., dark web) and digital currencies (e.g., Bitcoin).

Given these complexities, it is important to review the overall trends in cybercrime in the digital realm. Thus, this section is intended to inform our general knowledge concerning the scope and prevalence of cybercrime in the United States using a literature

review of the FBI's Internet Crime Complaint Center (IC3) Annual reports from 2001-2018.

Table 1. 2018 Crime Types

By Victim Count			
Crime Type	**Victims**	**Crime Type**	**Victims**
Non-Payment/Non-Delivery	65,116	Other	10,826
Extortion	51,146	Lottery/Sweepstakes	7,146
Personal Data Breach	50,642	Misrepresentation	5,959
No Lead Value	36,936	Investment	3,693
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811
BEC/EAC	20,373	Corporate Data Breach	2,480
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799
Advanced Fee	16,362	Ransomware	1,493
Identity Theft	16,128	Crimes Against Children	1,394
Spoofing	15,569	Re-shipping	907
Overpayment	15,512	Civil Matter	768
Credit Card Fraud	15,210	Charity	493
Employment	14,979	Health Care Related	337
Tech Support	14,408	Gambling	181
Real Estate/Rental	11,300	Terrorism	120
Government Impersonation	10,978	Hacktivist	77

The FBI's IC3 provides the public with reported information of cybercrime victimization and offenses nationwide and worldwide. According to the FBI's most recent IC3 report (IC3, 2018), in 2018 there were 34 major types of cybercrime victimization reported by online users (see Table 1). As hot topics for 2018 the FBI's IC3 highlights the

top three cybercrime types with the highest reported financial loss as follows: Business Email Compromise (BEC)[1], Ransomware[2], and Extortion[3].

An annual number of Internet crime victimization/monetary loss from 2000-2018 reported to the FBI's IC3 is shown in Figure 1. In 2000, the total number of cybercrime incidents was 16,838. This number increased to 351,937 by 2018. Overall, the number of Internet crime incidents reported to the FBI's IC3 has gradually increased between 2000 and 2018. More specifically, Figure 1 indicates that the count of cybercrime victimization in the United States increased from 2001-2005 (16,838 to 231,493) and peaked in 2009 with 336,655 cybercrime victims. Since then it has remained relatively steady from 2010-2018 (from 303,809 to 351,937). Also, Figure 1 shows that the amount of monetary loss in the United States steadily went up from 2001 to 2008 (from $17.8 million to $264.6 million), and abruptly increased in 2009 (47.2% increase from 2008) with a loss of $559.7 million, and increased once again from 2010 to 2014 (from $559.7 million to $800 million), and finally peaked in 2018 with a monetary loss of $2.7 billion.

[1] "BEC" is a criminal act that targets businesses in collaboration with foreign suppliers and/or businesses regularly performing wire transfer payments in order to achieve monetary gain (IC3, 2018).

[2] "Ransomware" is committed by using a type of malicious software that prohibits authorized access to a computer system and data base until ransom is paid by crypto currency; extortion refers a criminal act that a cyber offender demands something of value from a victim by threatening physical or financial harm or data breach (IC3, 2018).

[3] "Extortion" is unlawful extraction of money or property through intimidation or undue exercise of authority (IC3, 2018).

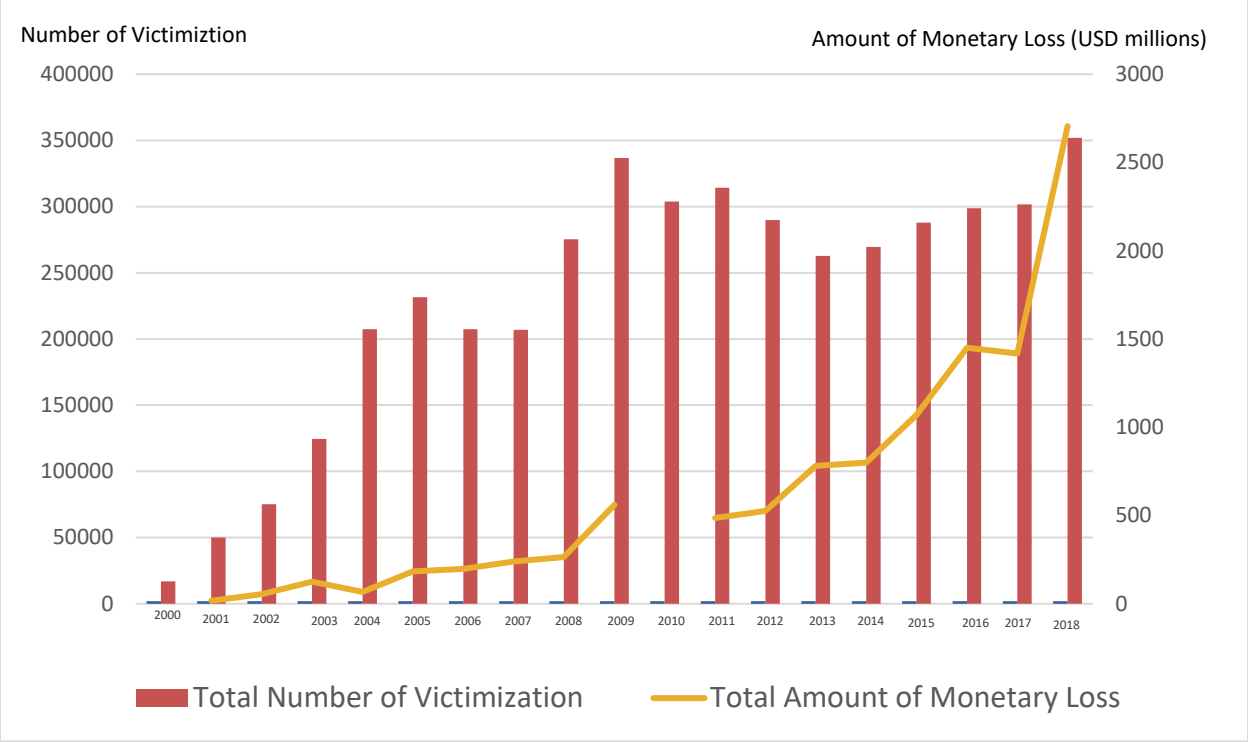


Figure 1. Cybercrime Victimization and Monetary Loss in the United States (2000 – 2018); Source. – Adapted from 2001 - 2018 Internet Crime Report (2018)

Having reviewed cybercrime victimization/monetary loss trends, attention can now be directed at the cybercrime typologies mostly utilized over the last 18 years. Cybercrimes have been committed in various forms (see Figure 2 and Note). Interestingly, Figure 2 indicates that auction fraud, non-delivery fraud, and Nigerian letter fraud were pervasively committed by perpetrators from 2001-2011. Since 2011, certain types of fraud (i.e., auction fraud[4], non-delivery fraud[5], Nigerian letter fraud[6], credit/debit card fraud, confidence fraud,

[4] "Auction fraud" is defined as "a fraudulent transaction or exchange that occurs in the context of an online auction site" (IC3, 2009).

[5] "Non-delivery fraud" can be defined as an incident in which customers purchase goods in online markets, but they never receive it (IC3, 2018).

[6] "Nigerian letter fraud" is defined as an act in which Nigerian criminals send an unsolicited email message, in which the criminals give the recipient guarantee to obtain a vast amount of money. At the same time, the criminals request the recipient to transmit "an advance fee or offer identity, credit card or bank account information" (IC3, 2007).

investment fraud, business fraud, check fraud, etc.: also see Note for definitions) decreased. Currently, blackmail/extortion/FBI scams, romance scams, auto auction fraud, real estate fraud, and ransomware scams mostly occurred in the United States followed by Canada, India, United Kingdom, Australia, France, Brazil, Mexico, China, Japan, and the Philippines. In short, this section indicates that the pattern of cybercrime typologies has been diverse and constantly fluctuating over the past 17 years. In this regard, it might have been influenced by information technology advancements and changes in social contexts (Taylor et al., 2019).

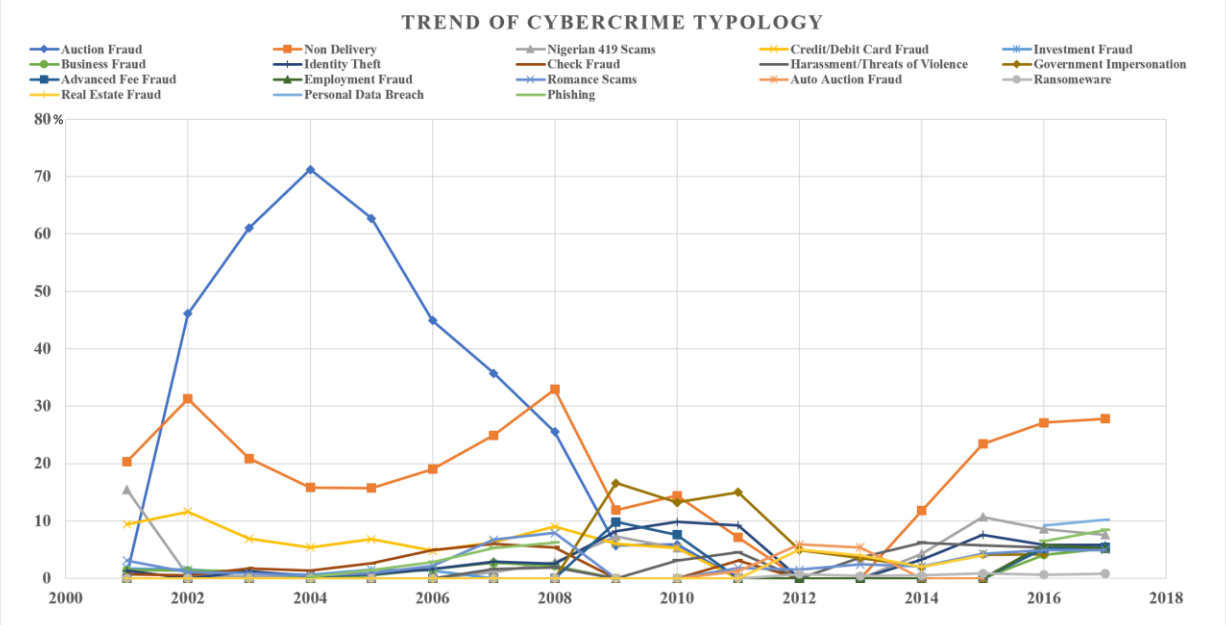


Figure 2. The Cybercrime Typology Trends; Source. – Adapted from 2001 - 2018 Internet Crime Report (2018); The numbers on the vertical axis indicate percent of total cybercrime victimization reported to the FBI's IC3 center.

To better justify the need for an advanced blueprint for responding and effectively controlling cybercrime, first, it is essential to understand the underlying theoretical mechanisms involved. The subsequent section introduces the main theoretical framework that leads to the development of the novel problem-solving strategy proposed in the dissertation. Specifically, I will discuss elements such as environmental criminology,

routine activities theory, and the original crime triangle. This review of literature helps prime the conceptualization of my novel cybercrime triangle framework that will better ensure a more secure digital environment.

Environmental Criminology and Crime Analysis

As environmental criminologists, Brantingham and Brantingham (1981) stated that criminal events can occur when offenders, victims or criminal targets, and laws converge in specific settings at certain temporal and spatial patterns. Also, they contended that the nature of the immediate environment facilitates criminal behavior. For example, the type of target, level of surveillance, and ease of access can affect the offender's choice of target. Furthermore, environmental criminology attempts to explain that criminogenic individuals are not only a major causal factor of crime events, but also criminogenic elements of certain places encourage potential perpetrators to engage in criminal activities (Wortley & Townsley, 2016). Environmental criminology also explains that criminal behavior and crime patterns are grounded in situational factors and the location of criminogenic environments. In other words, crime opportunities and other environmental characteristics shape criminal activities or deter crime in a given location. Given the situational and criminogenic environments, if crime analysts and practitioners can reveal certain crime patterns (e.g., offender activity spaces, movement patterns and temporal patterns), they will gain powerful investigative tools to control and prevent crime. For instance, crime patterns can be demonstrated visually using graphs, tables and maps in terms of their socio-demographic, temporal and spatial qualities through analyzing crime data and police reports (Wortley & Townsley, 2016). In a broad sense, it also can allow us to identify that a crime free environment sustainably reduces opportunity for the occurrence of cybercrime.

Along this line, Emig, Heck, and Kravitz (1980) asserted that crime analysis is employed to investigate pertinent information about crime patterns and crime trend correlations. From this perspective, crime analysts and practitioners are able to predict emerging crime problems, which initiates the development of crime prevention strategies. Thereafter, they can provide tactical advice to law enforcement on "criminal investigations, development of resources, planning, evaluation, and crime prevention" (Wortley & Townsley, 2016, p. 157). In the following sections, the historical roots of the environmental criminology perspective are reviewed in order to help readers comprehensively understand the cybercrime triangle framework.

The Historical Roots of Environmental Criminology

The initial idea of environmental criminology dates back to the 1960s. Elizabeth Wood (1961) grounded security guidelines with the use of vandal-proof materials and designs for facilities. Moreover, Wood (1961) and Jacobs (1961) found that design and surveillance for facilities were key factors for enhancing the security of a residence. In short, more 'eyes on the street' (surveillance) can potentially decrease criminal opportunities in a given location. In 1971, Ray Jeffery provided the concept of Crime Prevention Through Environmental Design (CPTED), which explained crime control through the design of physical environments (e.g., increasing surveillance on the street or natural access control by doors, fences, and shrubs) so that the rewards for criminal activities were reduced, while the risk increased. Newman (1973) then proposed the concept of defensible space, which explained a relationship between residential environments and crime. Newman explained that defensible space is considered as a crime-free area or territory where it is well managed by the owner or residents of that property.

Thus, he asserted that defensible space promotes the use of design to enhance the safety of a residence and reduce crime opportunities in that space.

In the wake of the development of environmental criminology, several crucial frameworks also arose to address specific conditions that manifest in both space and time. The first framework was routine activities theory (Cohen & Felson, 1979), which postulates three unique elements (motivated offender, suitable target, and absence of capable guardian) that could potentially facilitate criminal offending.[7] The second framework, crime pattern theory (Brantingham & Brantingham, 1981), helped explain why specific spatial and temporal artifacts conducted and inflated crime incidents. For example, certain places such as bus stops, train stations, and parks attract both potential offenders and victims in the same location, so these types of places can facilitate crime. The third framework was rational choice theory, which laid the groundwork for the criminal decision-making process (Clarke & Cornish, 1985). In this regard, criminals offend since crime offers the most effective instruments of achieving desired advantages such as money, material commodities, prestige, sexual gratification, and domination of victims (Cornish & Clarke, 2002; Gilmour, 2016). The last framework was Clarke's (1995) situational crime prevention theory, which posits that crime opportunities can be suppressed by increasing the risks of arrests, target hardening, and reducing the rewards of criminal behavior. Reyns (2010) asserted that if the virtual environment can be made less hospitable by cyber place managers (e.g., information technology officials) for crime, cybercrime incidents will decline. For example, through target hardening techniques like installing firewalls and

[7] The specific elements are discussed in the next section.

online security programs, cyber place managers can protect online environments against malware infection, Trojan Horse programs, and unauthorized access (hacking).

Before discussing crime triangle and cybercrime triangle frameworks, the following section will explain the concepts of RAT that underlie theoretical mechanisms of the cybercrime triangle proposed in this dissertation.

Routine Activity Theory

The initial idea of the crime triangle framework was expanded from Cohen and Felson's RAT. Thus, in this section, routine activity theory is explored to provide a fundamental backdrop for creating the new theoretical application of the cybercrime triangle framework. As discussed above, Cohen and Felson (1979) claimed that routine activities theory could explain why crimes occurred. Cohen and Felson's traditional routine activities theory consists of three major tenets: (a) motivated offenders, (b) suitable targets, and (c) the absence of capable guardianship (Cohen & Felson, 1979; Cohen, Felson, & Land, 1980; Felson, 1987; Kennedy & Forde, 1990; Massey, Krohn, & Bonati, 1989; Miethe, Stafford, & Long, 1987; Roncek & Maier, 1991; Sherman, Gartin, & Buerger, 1989). Routine activity theory explains that crime events occur when these three elements – a motivated offender, a suitable target, and the absence of a capable guardian – converge in time and space (Cohen and Felson, 1979; Felson, 2017). For instance, burglars may target their homes of choice, and these places are easily accessed in the absence of capable guardianship particularly during the daytime on a weekday (Tilley & Sidebottom, 2017) since changes to the activity of any one of these three elements can affect the likelihood of crime occurrence.

In the literature, a vast majority of the routine activities theoretical research has focused on the crime victimization since RAT has mainly been considered as a victimization theory rather than offending theory. However, the routine activities perspectives can be utilized to explain individual criminal behavior as well as victimization patterns. Since it clearly explains why certain criminals choose certain victims/targets and, furthermore, why certain victims are likely to be selected as attractive victims/targets at specific places and time (Chan, Heide, & Beauregard, 2011; Graney & Arrigo, 2002).

According to the routine activities approach, the first element of RAT is a motivated offender. Motivated offenders are defined as any individuals who might commit illegal offenses due to certain motivations (Clarke & Felson, 1993; Coster, Estes, & Mueller, 1999). Clarke and Felson (1993) and Clarke and Cornish (1985) contended that criminals can make a rational decision for the target selection process with which they attempt to maximize profit and minimize pain. The second element of RAT is a suitable target. Some scholars (e.g., Clarke & Felson, 1993; Cohen, Kluegel, & Land, 1981; De Coster, Estes, Mueller, 1999, p. 24) argued that the suitable target element of RAT can be broken into two components: "the proximity of potential targets to motivated offenders, and the material or symbolic attractiveness of a person or property target. The proximity of potential targets to motivated offenders is regarded as the physical proximity between potential targets and offenders. An attractive target is defined as an object that is not only small and expensive but also is insecure (De Coster, Estes, Mueller, 1999). The third element of RAT is a capable guardian. The primary guardians in society are individuals "whose presence, proximity and absence make it harder or easier to carry out criminal acts" (Hollis, Felson, & Welsh, 2013, p. 66).

Felson (1986) and Eck (1994) extended the guardianship concept along with three distinguishable elements: "(1) handlers – those who look after potential offenders to keep them out of trouble; (2) place managers – those who look after places to keep them secure from intruders; and (3) guardians (in a narrower sense) looking after particular crime targets" (Hollis et al., 2013, p. 66). All of these elements were contributors to building on the present crime triangle framework which is applied as the theoretical perspectives of the current study. Most of these elements are discussed in more detail in the next section.

In recent years, routine activity theory has been tested by scholars (e.g., Choi, 2008, 2015; Choi, Scott, & LeClair, 2016; Choi & Lee, 2017; Hinduja & Patchin, 2008; Holt & Bossler, 2008, 2013; Pratt et al., 2010; Reyns, 2013, 2015; Reyns & Henson, 2016; Reyns, Henson, & Fisher, 2011) to explain different types of cybercrime, including cyberbullying, cyberstalking, cyber-harassment, Internet fraud, identity theft, and malware infection.

Similar to the work of Cohen and Felson's (1979) RAT, Hindelang, Gottfredson, and Garofalo (1978) proposed lifestyle exposure theory, which focuses on victims' daily social interactions, rather than concentrating on the characteristics of individual offenders or individual causal variables. Hindelang, Gottfredson, and Garofalo (1978) found that individuals' vocational and leisure activities are directly associated with crime victimization. In short, Hindelang et al. (1978) asserted that differential lifestyle patterns are correlated with "role expectations, structural constraints, and individual and subcultural adaptations" (Choi, 2008; Hindelang et al., 1978 p. 245).

Cybercriminologists (e.g., Choi, 2008, 2015; Choi, Scott, & LeClair, 2016; Choi & Lee, 2017; Hinduja & Patchin, 2008; Holt & Bossler, 2008, 2013; Marcum, Higgins, Ricketts, 2010; Reyns, 2013, 2015; Reyns & Henson, 2016; Reyns et al., 2011) argue that

Cohen and Felson (1979) incorporated lifestyle-exposure theory (Hindelang et al., 1978) into their routine activities theory by expanding upon the existent tenet: individual's vocational and leisure activities. In Cohen and Felson's (1979) view, target suitability is created and influenced by an individual's vocational and leisure activities, which reflect the individual's routine activities such as social interaction and social activities (Choi, 2008). Also, Cohen and Felson (1979) developed two other tenets – capable guardianship and motivated offender – and integrated these two tenets with the suitable target tenet from lifestyle-exposure theory. Choi (2008), Holt, Burruss, and Bossler (2015), and Reynes et al. (2011) argued that routine activities theory could be extended from the lifestyle-exposure theory to explain crimes in online settings.

The Cybercrime Triangle Framework

As noted earlier, the crime triangle framework can be a very powerful investigative tool to predict emerging crime problems and develop crime prevention strategies. The crime triangle framework helps reveal the characteristics of crime scene places, and offenders and victims along with their socio-demographic, and temporal and spatial features, providing tactical advice to law enforcement for their crime prevention strategies.

The crime triangle framework can explain how crime problems are created by opportunities instead of what makes people criminal (Clarke & Eck, 2005). This triangle consists of an inner triangle (i.e., offender, target/victim, and place) and an outer triangle (i.e., handler, guardian, and manager; see Figure 3). Spelman and Eck (1989) have portrayed the problem of the triangle as "wolf," "duck" and "den" problems (Clarke & Eck, 2005). Wolf problems occur when repeat offenders attack a series of different targets at different places. Duck problems occur when repeat victims consistently are attacked by

different offenders. Den problems occur when different offenders and different targets encounter each other at the same place where management strategies are poor. Clarke and Eck (2005) explain that crime occurs when all "wolfs," "ducks" and "dens" must be present and all outer elements (handler, guardian, manager) are ineffective or absent. The following sections explain each tenet of the cybercrime triangle framework.

Figure 3. The Problem Analysis Triangle; Source. – Adapted from POP Center (2018) and Clarke & Eck (2005).

Offender. Individual cyber criminals are motivated by various factors (Grabosky, 2015). Grabosky (2015) asserted that cyber criminals' motivation might be complex, or mixed. Plenty of motivated cyber criminals seek to catch valuable targets in the form of online users who connect to the Internet with little or no computer security (Grabosky, 2015). Normally, cyber criminals are motivated by their desire to control cyberspace and computer networking systems (Grabosky, 2015). Cyber criminals randomly plant malicious viruses and worms on social networking sites (SNSs) or web forum sites to receive individuals' information when online users click a pop-up window or fake link (Choi, 2008; Piazza, 2006, p.54). However, the characteristics of individuals engaged in online interpersonal crimes (cyber harassment and cyberstalking) may be

different from that of cybercrime perpetration in hacking, cyberattack, and internet fraud. Online interpersonal criminals intentionally search for attractive targets on SNSs or online dating sites. Cyber harassers and stalkers may seek to "exert power over their victims" by invoking fear (McGrath & Casey, 2002, p. 89). By increasing their knowledge of the victim's information, the perpetrator can terrorize and control them. Specifically, cyber harassers and stalkers utilize or post on SNSs a victims' personal information, such as mobile phone numbers, addresses, e-mail addresses, personal preferences, and photos (including nude photos) in order to threaten their victims' lives (McGrath & Casey, 2002).

Target/victim. Like suitable targets in physical space, many suitable targets exist in the cyber world. A person's vocational and leisure activities are the key factors in making him/her a suitable target (Choi, 2008). During online activities in cyberspace, individuals can persistently interact with other users through online toolkits and smartphone apps such as e-mail, online messengers, and SNSs. Also, online users set up their lifestyle by joining "various cyber communities based on their interests, such as cyber-café's, clubs, and bulletin boards" (Choi, 2008, p. 13). Similarly, individuals may also join smartphone apps for dating and SNSs. They are more likely to be suitable targets for online sexual crime than someone who does not join such smartphone apps. Likewise, individuals who use unsecured public wireless networks are more likely to be suitable targets from cybercriminals because of the inherent vulnerabilities (Brody, Gonzales, & Oldham, 2013). For example, cyber perpetrators can monitor and store sensitive user data (e.g., login credentials, bank account information, and social security numbers) and stolen data can be utilized to conduct fraudulent activity or sell the information to other criminals for monetary gain.

Place. In the physical world, the place could mean a point in space (such as a building, park, intersection, or classroom) or an area (such as a country, city, police district, neighborhood, or census block). Sherman, Gartin, and Buerger (1989) argued that there are certain "hot spots" in the physical world where crimes routinely occur. Sherman et al. (1989) explained that the places (such as bars, liquor stores, bus depots, homeless shelters, downtown malls, and theaters) are regarded as the hot spots for crime in the physical world. In the cyberworld, virtual places exist in as real a context as the physical world does – like websites/web pages or social networking sites (Madensen & Eck, 2013). Some cyber places can have extraordinarily high-crime rates, whereas most places have little or no crime. Some scholars (e.g., Kennedy, Caplan, & Piza, 2011; Madensen & Eck, 2013; Spelman & Eck, 1989; Weisburd, 1997) contend that this sort of disparity in the real world can be created by characteristics of places. Like the physical world's crime hotspots, Holt (2013) posited that there exist some hot spots in the virtual world. For example, certain places (e.g., dark web forums, online dating websites, pornography websites) may have high-cybercrime levels, while other online places do not (Choi, 2015; Holt, 2013; Holt & Bossler, 2008).

Handler. The term handler refers to someone who can control motivated offenders (Wortley & Townsley, 2016). For example, parents, siblings, teachers, friends, and spouses of the offender can be considered as handlers. They are in the position to discourage deviant actions (Clarke & Eck, 2005). Madensen and Eck (2013) argue that handlers can emotionally support a potential offender and keep them away from committing a crime. For example, individuals with higher levels of parent attachment and parental supervision

or school attachment are less likely to engage in cyber deviant behaviors (Back, Soor, & LaPrade, 2018).

Guardian. The term guardian refers to someone who protects suitable targets or victims from offenders (Wortley & Townsley, 2016). In the physical world, lighting in areas and using locks, alarms and barriers are regarded as a means of target hardening for the capable guardian (Choi, 2008; Tseloni, Wittebrood, Farrell, & Pease, 2004). Cyber-criminologists (e.g., Choi, 2008, 2015; Choi, Scott, & LeClair, 2016; Choi & Lee, 2017; Hinduja & Patchin, 2008; Holt & Bossler, 2008, 2013; Marcum, Higgins, & Ricketts, 2010; Reyns, 2013, 2015; Reyns & Henson, 2016; Reyns et al., 2011) stress that digital capable guardianship is one of the most crucial elements to prevent cybercrimes. Digital capable guardianship is defined as a preventative tool that helps online users secure themselves from cyber criminals. Choi (2008) clarified that there are two types of digital capable guardians: physical capable guardians and cybersecurity guardians. The physical capable guardians – antivirus software, firewalls, and antispyware – protect computer systems and personal assets against computer criminals. The cybersecurity guardian – online security settings and security applications on SNSs – protects online users against interpersonal criminals online. Both physical capable guardianship and cybersecurity guardianship are associated with target hardening to hamper the efforts of criminals.

Manager. The term manager refers to someone who takes care of places or locations and protects them from offenders (Wortley & Townsley, 2016). In this regard, place managers can be defined as individuals (e.g., landlords, a bus driver, flight attendants, cybersecurity staffs in an organization, bar owners) who have some responsibility for controlling deviant behavior in the specific location (Clarke & Eck, 2005). Madensen and

Eck (2013) assert that place managers implement crime-control strategies at proprietary places through their authority to handle their properties. Using certain strategies, such as protecting vulnerable targets, not attracting potential offenders, and effectively controlling behavior, place managers can alter high-crime places into crime-free environments. In online settings, place managers (e.g., information security officials or internet providers) can impact high-cybercrime places (e.g., dark net, social network site, online dating sites, or school website) and the ecology of cybercrime in their institutions. Then managers in these places can set appropriate cybersecurity settings and behavioral expectations, and enforce rules of conduct, or provide guardians. Also, place managers can provide employees and students or customers cybercrime intervention programs (e.g., cybersecurity training or cybercrime awareness program) which may enhance the protection of potential victims.

In short, plenty of motivated offenders and suitable victims are at zero distance from one another in virtual space. If place managers and capable guardians are ineffective and inactive in protecting online users, cybercrimes can be remotely committed from across the country or even across the world (Yar 2005, p. 415; Hazelwood & Koon-Magnin, 2013). The next section discusses previous studies of the crime triangle framework and crimes.

Studies of the Crime Triangle Framework and Crimes

Despite public need to apply the crime triangle framework to crime events, to date, few studies have utilized this theoretical framework to analyze crime scenes and characteristics of offenders and victims. Some studies (Eck, 2002; Mandensen, 2007; Roberts, 2007) found that increasing place manager awareness and interventions in drug-related crimes and violent crimes in bars can play a critical role in preventing these types

of crimes. Other studies (e.g., Block & Block, 1995; Clarke, 1997; Danner, 2003; Eck & Weisburd, 2015; Felson, 1995; Mazerolle, Kadleck, & Roehl, 1998; Mazerolle & Roehl, 1998; Sherman, 1995) indicated that lack of active place management can be related to facilitating crime (Mandensen, 2007). Likewise, Pires, Guerette, and Stubbert (2014) examined whether kidnappings for ransom demonstrate connections to the crime triangle framework. They found that there were spatial-temporal and other concentrations for kidnappings in Colombia, South America. Yet, no studies to date have applied the crime triangle framework to cybercrime events. Thus, the current study is the first to establish and apply the tenets of the cybercrime triangle framework (i.e., offenders, victims, guardians, place, and place management) to the phenomenon of cybercrime.

In contrast, for the past two decades, scholars have extended the application of routine activity theory to virtual settings. Consistent with the application of RAT to physical crime, researchers tested whether suitable targets with unguarded exposure to motivated offenders are more likely to be victims of cybercrime than others. For example, Back (2016), Bossler and Holt (2009), Choi (2008), Choi and Lee (2017), Holt and Bossler (2008; 2013), Reyns (2013), Reyns et al. (2011), and Marcum, Higgins, and Ricketts (2010) have found that risky online lifestyles contribute to increasing cybercrime victimization. Holt and Bossler (2008) focused on using a lifestyle-routine activities framework to examine the causal factors for cyber harassment victimization among college students. Their study found that risky online activities increased college students' risks for cyber harassment (Holt & Bossler, 2008). Also, Reyns, Henson, and Fisher (2011) empirically tested the cyber-lifestyle routine activities theory for assessing cyberstalking and cyber

harassment. The findings of the study indicate that online risk-taking behaviors increase the likelihood of cyberstalking victimization.

In addition, several studies (i.e., Back, 2016; Choi, 2008; Choi & Lee, 2017; Choi, Choo, & Sung, 2016; Bossler & Holt, 2009; Holt & Bosseler, 2013; Leukfeldt, 2014; Leukfeldt & Yar, 2016; Hutchings & Hayes, 2008; Marcum, Ricketts, & Higgins, 2010; Reyns, 2013; Reyns, 2015; Reyns & Henson, 2016; Reyns et al., 2011) have attempted to empirically examine the associations between capable guardianship – especially digital capable guardianship (i.e., anti-virus software and cybersecurity settings) – and cybercrime victimization. The findings of these studies are mixed. In this regard, the findings of some studies (see Back, 2016; Choi, 2008; Choi & Lee, 2017; Choi, Choo, & Sung, 2016; Hutchings & Hayes, 2008; Reyns, 2013; Reyns & Henson, 2016) indicated that the presence of digital capable guardians reduced the likelihood of cybercrime victimization, whereas the results of other studies (see Bossler & Holt, 2009; Holt & Bosseler, 2013; Leukfeldt, 2014; Leukfeldt & Yar, 2016; Hutchings & Hayes, 2008; Marcum et al, 2010; Reyns & Henson, 2016; Reyns et al., 2011; Reyns, 2013; Reyns, 2015) demonstrated that digital capable guardianship did not mitigate cyber threats.

In accordance with the social science literature, most published research is limited to explain how opportunities for crime in both physical space and cyberspace are created through daily activities because the previous works mainly have examined two elements of the crime triangle: cybercrime victimization and digital capable guardianship (Madero-Hernandez & Fisher, 2013). Therefore, these limitations may preclude estimating the relative significance of routine activity compared to other theories and preclude isolating specific routines that consistently predict cybercrime offending, place, and victimization

(Madero-Hernandez & Fisher, 2012). The current study attempts to overcome these limitations of the previous studies. As an integrated theoretical framework, this study focuses on establishing and empirically examining the groundwork of the cybercrime triangle framework in collaboration with several theoretical concepts such as RAT, rational choice, situational crime prevention, and place management. Even though this study is unable to simultaneously examine the three elements of the crime triangle, it strives to respectively explore these three components in order to portray the characteristics and natures of cybercriminals, cybercrime victims, and place management in order to reveal the causal factors of cybercrimes.

Conclusion

This chapter broadly explored the relevant research on cybercrime and the cybercrime triangle framework. The chapter began by providing an overview of cybercrime and cybercrime trends. Then, following the overview, several theoretical frameworks relevant to the current study and the existing cybercrime research were explored. This review identified a significant gap in the literature concerning the application of routine activity theory to the criminological analysis of cybercrime. Specifically, previous research has explored the cybercrime phenomenon and developed cybercrime prevention strategies relying predominantly on cybercrime victimization and digital capable guardianship in line with the routine activity perspective. No studies have yet applied the broader framework of the crime triangle commonly used in the analysis and prevention of crime to an online setting. Thus, this dissertation seeks to expand the application of the "Crime Triangle," a derivative of routine activity theory, to cybercrime. In an effort to fill this gap in the literature, the following chapters (3, 4, and 5) strive to

independently explore these components in order to portray the characteristics and natures of cybercriminals, cybercrime victims, and place management.

CHAPTER 3

MOTIVATED CYBER OFFENDER AND CRIME OPPORTUNITY:

AN APPLICATION OF THE CYBERCRIMINAL PROFILING MODEL

Examining the crime scene is the backbone to discover the motives, opportunities, and means for potential perpetrators to commit crimes (Backer & Wolfer, 2003; Clarke, 1995; Cornish, 1993). In this regard, it can offer law enforcement officials with "the exact times and kinds of offenses, the offenders' methods of operation, the targets of attack, crime generators, hot spot locations and the underlying causes of crime" (Backer & Wolfer, 2003, p. 48). For example, police officers analyze the problem and causal factors of offenses in their jurisdiction, and then they can efficiently assign the department's personnel and assets to tackle hot spot locations. Recently, the Federal Bureau of Investigation (FBI) profiling model has been utilized to investigate common characteristics or patterns of criminals (e.g., demographics, motives, behaviors) to various crime scenes. Moreover, practitioners and scholars point out that the FBI's profiling technique is a robust tool to explain particular correlates between offender's behaviors and victim's patterns (Scott, Lambie, Henwood, & Lamb, 2006).

This chapter aims to provide scholars, practitioners, and policy makers an empirical application of the criminal profiling technique to help them better understand characteristics of cybercriminals and the cybercrime scene. Thus, this study strives to propose a new integrated framework of cybercriminal profiling, called the "Situational (S), Sociodemographic Background (SBA), Cybercrime Opportunity (CO): SSBACO Cybercriminal Profiling Model." It reflects multidisciplinary methods such as: (1) FBI

criminal profiling, (2) the conceptual frameworks of cybercriminal profiling provided by Kirwan (2011), Kwan and Stephens (2008), Nachreiner (2015), and Warikoo (2014), (3) the variables derived from the work of Beauregard, Lussier, and Proulx (2008), and (4) the Codebook for the Dyadic Cyber Incident and Dispute Dataset Version 1.1 provided by Maness, Valeriano, and Jesen (2019). The following sections discuss research on cybercriminal profiling along with sociodemographic, situational, and crime opportunity factors. Also, these sections discuss the research questions and hypotheses to be tested, the methods employed, and the results of the analysis.

Background

Cybercriminal Profiling. Criminal profiling is a multi-disciplinary forensic technique in which a profiler offers personality, behavioral, and demographic characteristics of offenders based on the analysis of crime scenes (Bartol, 1996; Douglas & Burgess, 1986; Hicks & Sales, 2006; Turvey, 1999). Turvey (1999) asserts that modern criminal profiling is grounded in the forensic sciences, criminology, psychology, and psychiatry. There are two major criminal profiling approaches – "crime scene profiling" and "investigative psychology" – utilized to explain crime scene characteristics and causal factors of crimes (see Scott et al., 2008). Despite the development of criminal profiling frameworks, there still exists an ongoing debate regarding the scientific rigor and accuracy of criminal profiling (Dowden, Bennell, & Bloomfield, 2007). Moreover, few empirical studies have been conducted to examine the validity and credibility of criminal profiling investigation procedures. In addition, according to a systematic review of the profiling literature provided by Dowden et al. (2007), there is an abundance of non-statistical and conceptualized research in the literature, but few quantitative studies exist. Dowden and

colleagues (2007) point out that researchers from criminology, forensic psychology, forensic psychiatry, sociology, and medical fields have strived to provide evidence that offender profiling is a useful tool for prioritizing suspects and establishing new lines of scrutiny in serial crime investigation over the past four decades. Ten major types of crime (e.g., serial homicide, rape, arson, homicide, burglary, unspecified, mixed, random violence, child crimes) have been examined (see Dowden et al., 2007) to discover the motives, opportunities, and means for potential perpetrators to commit crimes.

Attention now turns to the cybercriminal profiling approach, which may be of great use in uncovering the characteristics of cyber offenders and cybercrime opportunities. Cybercriminal profiling is defined as the examination of cyber offender behavior that includes "an educated attempt to provide specific information as to the type of individual who committed a certain crime. A profile is based on characteristics and patterns or factors of uniqueness that distinguishes certain individuals from the general population" (Jahankhani & Al-Nemrat, 2012; Warikoo, 2014, p 173). Currently, the FBI utilizes inductive profiling with statistical analysis in order to identify patterns of cybercriminals, especially cyber fraud profiles (Jahankhani & Al-Nemrat, 2012; Warikoo, 2014). In line with the FBI's cybercriminal profiling method, forensic psychology offender profiling techniques also have been used as a cybercrime investigation tool (Jahankhani & Al-Nemrat, 2012; Warikoo, 2014). Although several researchers and practitioners have made interdisciplinary attempts (e.g., criminology, psychology, computer science) to provide a cybercriminal profiling framework, there is still a lack of agreement on empirical and scientific frameworks of cybercriminal profiling (Jahankhani & Al-Nemrat, 2012; Hadzhidimova & Payne, 2019).

Research on Criminal Profiling. Several researchers (see Blanchette, 2002; Holmes & Holmes, 2008; Beauregard et al., 2008) have postulated a direct relationship between the personal characteristics of an offender (e.g., sociodemographic elements), personal attributes of the offender (e.g., antisocial attitudes, low self-control, impulsivity, substance abuse problems, dysfunctional family relationships), the method of criminal operation, the signature of the offender, and the characteristics of crime scenes. They hypothesize that personal attributes of the offender, situational conditions, and criminal opportunity are directly associated with crime scene characteristics (Beauregard, Lussier, & Proulx, 2008). Mokros and Alison (2002) suggested the "homology hypothesis," which explains when more than two offenders have similar background characteristics and criminal opportunities, they could show similar criminal behaviors in the crime scene.

Currently, a large body of literature has focused on research pertaining to criminal profiling of serial killing, rape, robbery, burglary, and terrorist attacks. For example, Woodhams and Toye (2007) investigated the relationship between offender behavioral consistency, offender behavioral distinctiveness, and homology between offender characteristics and behavior using serial commercial robberies. The work of Woodhams and Toye (2007) concluded that offender behavioral consistency and distinctiveness were statistically significant predictors for commercial robbery typologies; however, there was no significant relationship between previous convictions, sociodemographic background factors, and commercial robbery typologies.

Several studies (Prentky et al., 1989; Safarik, Jarvis, & Nussbaum, 2000; Van Patten & Delhauer, 2007) have attempted to examine serial sexual homicide cases to examine associations between four independent variables (offender race, offender age,

relationship of offender to victim, and distance of offender's residence from victim) and a set of dependent variables (crime scene, victim characteristics, and specific offender behaviors). Safarik and associates (2000) and Van Patten and Delhauer (2007) found that younger individuals (e.g., ages 20 to 35) were more likely to engage in serial sexual homicide than older individuals. Prentky and his colleagues (1989) found that serial murderers had a greater prevalence of violent fantasy in sexual homicide.

Using data from New Zealand, Scott, Lambie, Henwood, and Lamb (2007) compared the offense behaviors of 114 convicted stranger rapists with previous criminal convictions. Scott and colleagues found that intruding stranger rapists were more likely to have prior criminal convictions than non-intruding stranger rapists. Similarly, Davies, Wittebrood, and Jackson (1998) and Jackson, van den Eshof, and de Kleuver (1997) examined the relationship between the rapist's behavior and previous conviction respectively with 210 stranger rape cases out of 322 rape cases in the Netherlands. Both studies found that rapists who were extremely aggressive towards their victims were more likely to have previous convictions for theft and robbery than rapists who were not extremely violent.

In the existing literature, several scholars (Bennell & Corey, 2008; Goulette & Tardif, 2018; Sarangi & Youngs, 2006; Van Patten & Delhauer, 2007) have strived to explain the relationship between crime locations and the type of crime committed. Sarangi and Youngs (2006) compared the distance travelled to offense location of 30 burglars, committing a total of 150 crimes in India. Consistent with burglar patterns in North America, UK, and Australia, they found that burglars in India travelled close to where he or she lives. Bennell and Corey (2008) examined the applicability of geographic profiling

in the context of terrorism in order to identify the location of unknown terrorists. They pointed out that the terrorists had several anchor points (a residence or place of work) to avoid discovery. Van Patten and Delhauer (2007) pointed out that the very young and the very old are less likely to travel to commit sexual homicide than adults between the ages of 26-34, who travel an average 10 miles or more. Goulet and Tardif (2018) analyzed an offender's journey to property crimes using 7,807 burglary offense cases. Specifically, they examined the relationship between crime locations and generated paths based on crime pattern theory. The findings indicated that a high percentage of crimes occurred very close to the areas that offenders were familiar with.

Research on Cybercriminal Profiling. In efforts to better identify potential suspects when examining crime scenes, researchers (e.g., Douglas & Burgess, 1986; Douglas, Ressler, Burgess, & Hartman, 1986; Godwin, 2002) have attempted to establish a scientific and reliable profiling process for crime in the physical environment. Similarly, some scholars (e.g., Casey, 2012; Jahankhani & Al-Nemrat, 2012; Nykodym, Taylor, & Vilela 2005; Warikoo, 2014; Yu, 2013) have proposed cybercriminal profiling techniques, including inductive and deductive profiling (Shinder & Cross, 2008; Tennakoon, 2011; Warikoo, 2014, p. 173):

> Inductive profiling method utilizes the criminal profile database that "contain extensive data on criminals committing a type of crime in order to analyze the data, establish correlations, and deduce the characteristics common to statistically large number of offenders committing a specific type of crime. Deductive profiling method employs analysis of forensic evidence and victim profiling to determine the motive and criminal characteristics."

In line with these two types of profiling methods, Shaw (2006) reviewed recent empirical studies of insider computer attacks garnered from the inductive profiling method and then explored illustrative case studies using a deductive profiling approach. However, it is important to note that the application of criminal profiling techniques for cybercrime research is still in its infancy compared to the typical criminal profiling research. Therefore, this study seeks to provide the conceptual and operational frameworks of a cybercriminal profiling technique, so that law enforcement can accurately identify and apprehend cyber offenders by scrutinizing important suspect and crime scene characteristics.

SSBACO Cybercriminal Profiling Framework

Based on environmental criminological theories (e.g., the routine activity/rational choice/situational crime prevention perspectives), and the crime triangle framework, certain circumstances and crime opportunities can affect offender's decision-making pertaining to selecting targets and committing crime. In offering a conceptual framework for examining individual cyber offending, this paper draws on a body of work that has investigated the role of crime opportunities and situational factors as a source of explanation for crime patterns. Specifically, building on the previous works (see Beauregard & associates, 2008; Braga & Clarke, 2014; Cozens & Grieve, 2014; Leclerc, Wortley, & Dowling, 2016; Moreto, 2019; Osgood et al., 1996; Wortley 2001) the study in Chapter 3 provides a scientific method for better understanding the relationship between cyber offenders and situational and crime opportunities through proposing the SSBACO Cybercriminal Profiling Model.

This SSBACO Cybercriminal Profiling model is composed of Situational Factors (S), Sociodemographic Background Factors (SBA), and Characteristics of Cybercrime

Opportunity Factors (CO). According to criminal opportunity perspective (see Beauregard et al., 2008), two different variables (pre-crime situation and characteristics of the cybercriminal opportunity) can be considered as a criminal opportunity. First, situational factors or pre-crime situational factors may include (1) alcohol or drugs use prior to the offense, (2) pornography use prior to the offense, (3) being angry about something/someone, and (4) presence of a political objective. Second, characteristics of cybercrime opportunity factors may consist of (1) intimate relationship with the victim, (2) stranger victim, (3) presence of a weapon, (4) presence of co-offenders, (5) risk of being apprehended, (6) time spent with the victim, and (7) level of resistance of the victim or target (e.g., cybersecurity level). According to Beauregard and colleagues' (2008) study, sociodemographic background factors can include age, ethnic origin, nationality, cybercriminal type, and cybercrime recidivist. In addition, severity scale of cybercrime damage[8] and damage type[9] (also see Appendix C) are reflective of cybercrime scene or individual cyber offending characteristics. Thus, the following sub-sections briefly discuss the literature regarding sociodemographic, situational, and cybercrime opportunity factors.

Sociodemographic Background Factors. It is worth noting and necessary to empirically investigate the characteristics of cybercriminals such as country of origin, age, gender, and type of cybercriminal in order to understand cyber offending and the criminal

[8] Severity scale of cybercrime damage includes five-category scale: (1) probing without kinetic cyber; (2) harassment, propaganda, nuisance disruption; (3) stealing targeted critical information; (4) widespread government, economic, military, or critical private sector theft of information; (5) critical network and infrastructure destruction.

[9] Damage type includes four-category scale: (1) indirect and delayed; (2) indirect and immediate; (3) direct and delayed; (4) direct and immediate. Indirect in this context means that the damage done by the cyber incident was not the original intent of the initiator. Delayed in this context means that the impact of the attack takes months. (Maness, Valeriano, & Jensen, 2019)

justice system's response to these offenses (Hadzhidimova & Payne, 2019). Thus, this study seeks to advance scientific research on exploring the characteristics of cybercriminals. To achieve this goal, this study addresses the following research question:

Research question [Q1]: Who, what, where, and how do criminals commit cybercrime?

Several scholars have strived to examine the demographic characteristics of cyber offenders (age and gender), citizenship, and behavioral patterns. Rogers (2003), Fried (2001), Warner (2011), and Hadzhidimova and Payne (2019) note that the "stereotypical" cyber offender is 12-28 years old, single, male, and socially dysfunctional, possibly from a dysfunctional family. Interestingly, in a study of hackers in South Korea, Back, LaPrade, Shehadeh, and Kim (2019) found that 55% of youth hackers were motivated by monetary gain followed by hacktivism (24%), and entertainment (13%), whereas 87% of adult hackers were also motivated by monetary gain followed by entertainment (7%) and blackmail (3%). In addition, they found that 90% of the adult hackers had one or more accomplices when committing hackings, while 62% of youth hackers had one or more accomplices.

Situational Factors. As discussed in Chapter 2, the rational choice and situational crime prevention approaches are considered as the plausible theoretical perspectives to explain the decision-making of offenders. Criminals decide whether or not to engage in deviant acts by weighing the effort, rewards, and costs involved in alternative ways of action. Furthermore, certain situational factors can facilitate potential cyber perpetrators to engage in more severe violence (Cornish & Clarke, 2008; Leclerc, Wortley, & Dowling, 2016) and cause direct and immediate damages to targets. The review of the existing literature reinforced the present study's theoretical argument for a relationship between the

situational factors and crime. Nonetheless, a clear gap was found in the previous research, focusing on the influence of the situational factors in addressing crimes in the physical world. In an effort to fill this gap, the present study proposes the following research question and hypotheses:

Research question [Q2]: Is there a relationship between pre-cybercrime situational factors and cybercrime scene characteristics?

Hypothesis [H1]: Cyber offenders who possess illicit drugs will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

To extend the application of the rational choice approach, the existing literature looked at the decision-making of cybercriminals regarding situational factors during their offending process. For example, Beauregard, Lussier, and Proulx (2005) explored the role of sexual interests and situational factors on rapists' modus operandi. Their study utilized a sample of 118 offenders who sexually assaulted a female aged 16 or over and its data were analyzed using multiple regression models. The findings of their study demonstrated that there are links between sexual interests, situational factors, and rapists' modus operandi. First, individuals having a greater sexual interest in nonsexual violence showed a higher level of organization in the modus operandi. Second, the findings showed that alcohol consumption prior to the offence was positively associated with a higher level of coercion. Lastly, a negative emotional state prior to the crime was associated with a high

level of injury inflicted on the victim. Similar to the explanation in Beauregard et al.'s (2005) study, other empirical studies (Lussier, Proulx, & Leblanc, 2005; Lalumiere & Quinsey, 1996; Malamuth, 1998) have shown that offenders with a high antisocial tendency are more likely to engage in a higher level of physical coercion and more severe violence.

In the cyberworld, cyber perpetrators are allowed to commit cybercrime when their moral prohibitions have been weakened due to blaming alcohol or illegal drugs for cyber violence. Ullman (2007) found that alcohol is a common factor and one half to two thirds of these offenders used alcohol before sexual offenses. On the role of using drugs, Mieczkowski and Beauregard (2010) suggested that the use of drugs was positively associated with severity of crime events. Cumulatively, this study proposes that the possession of illicit drugs is positively associated with increased severity scale of damage or damage type.

Hypothesis [H2]: Cyber offenders who have political motivation(s) will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

With regard to political reason, for example, cyberterrorists and state-sponsored cybercriminals can be motivated by a specifically political and ideological reason to attack computer/network systems (Taylor & Colleagues, 2019). In this regard, they commonly engage in committing massive cyberattacks (DDoS attack, ransomware attack, cyber

espionage, botnet attack, etc.) which directly and immediately result in severe damages and pose threats to national security (e.g., critical infrastructure) and economic systems (Taylor & Colleagues, 2019). In the same vein, cyber offenders with a high antisocial tendency (e.g., frustration and anger) derived from political reasons are more likely to engage in more severe and direct cyber threats against targets.

Cybercrime Opportunity Factors. This study also seeks to advance scientific research on examining the link between the characteristics of cybercrime opportunity and cybercrime scene characteristics. To achieve this objective, this section addresses the following research question.

Research question [Q3]: Is there a relationship between cybercrime opportunity factors and cybercrime scene characteristics?

Previous studies have already demonstrated the importance of opportunity factors for offender behaviors during the crime. Beauregard and colleagues (2008) and Warr (2001, p. 69) contended that opportunity factors were important elements in predicting the characteristics of the criminal event or crime scene because "opportunity becomes the limiting factor that determines the outcome of potentially criminal situations, and thus, by extension, the incidence of criminal behavior in a jurisdiction."

In accordance with RAT, crime does not randomly occur in society. Wittebrood and Nieuwbeerta (2000) explained that: (1) a criminal-opportunity structure is derived from patterns of routine activities and lifestyles through the link between a potential criminal and target and (2) the offender's subjective value of the target attractiveness and situational or crime opportunity factors impact on the determination of selecting a certain crime target.

As a rational decision process, potential offenders generally select targets which give them enough rewards and which lack guardianship at that specific moment (Boudreaux, Lord, & Jarvis, 2001; Hough, 1987). Importantly, Beauregard and associates found that crime opportunity factors were important predictors in explaining sex offenders' behaviors such as selecting victims or committing rape/sexual assault.

Hypothesis [H3]: Cyber offenders who are not known to their target prior to the offense will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

Hypothesis [H4]: Cyber offenders who intentionally attack the target will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

Hypothesis [H5]: Cyber offenders who have intimate relationship with the target will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

Hypothesis [H6]: Cyber offenders who attack multiple targets will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

First and foremost, establishing a relationship between an offender and target/victim is a significant element in order for the offender to successfully select target/victim and completes the crime. The FBI (1995) found that stranger-perpetrated homicide occurs less frequently than homicides committed by know offenders. Also, the work of the Goetting (1995) indicated that children were victimized by a known offender in 69% of the cases, 17% by acquaintances, 14% by the parent's spouse or boyfriend/girlfriend, and others. As an attempt of the extension for the scope of RAT, the link between offender and victim in the physical world requires a different approach. As noted previously, Yar (2005), Choi (2008), Holt and Bossler (2008), Reyns (2013), and Leukfeldt and Yar (2016) argue that cybercrime events are very different from conventional crimes in the terrestrial domain because the virtual environment is zero-distance between motivated offender and suitable target. Cyber routine activity theory, as integrated by Choi (2008, 2015), places an emphasis on the idea that cybercrime does not require any convergence of space and time between offenders and victims (Back, LaPrade, & Soor, 2017). Thus, inconsistent with the previous studies, the majority of cyber offenders do not need to establish a relationship with the victim/target prior to committing the cybercrime. As such, cyber offenders who are not known to the victim/target prior to the

onset of an offense pervasively and severely attack random targets without convergence of space and time between offenders and victims. In short, cyber offenders may profoundly exploit these given crime opportunities derived from the nature of the virtual environment.

Hypothesis [H7]: Cyber offenders who have co-offender(s) will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

Warr (2001) also attested that co-offenders serve as an opportunity factor in the commission of the crime process as well as providing motivation before or even during the course of the attack. Likely, Osgood and his colleagues (1996) found that in the presence of peers, it is easier for individuals to participate in deviant acts. Weerman (2003) asserts that serious offences such as burglary and robbery are often conducted by more than one person, whereas general assault and minor thefts or shoplifting have much lower rates of co-offending. In a similar vein, as to tech-savvy cyber offenders against the targets/victims with a higher level of the resistance (i.e., strong cybersecurity countermeasure) and more valuable assets, some may require cooperation from others for completion of the crime (e.g., getting access to the computer/network systems, controlling the network servers, preventing resistance, and/or potential interference from cyber detection). Moreover, when cybercriminals target large institutions such as government/military or enormous companies, they need to have accomplices to successfully break into highly protected

systems and complete their criminal objective(s). In turn, it can lead to more severe damage to the targets which have more critical assets than individual online users.

Hypothesis [H8]: Cyber offenders who are further from the target will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

Environmental criminologists assert that most crimes occur near locations where the criminal is familiar or knowledgeable. The work of Brantingham and Brantingham (1990) explains that most criminal activities occur near where offenders live or work; however, with a buffer zone around the offender's residence where the offender is less likely to commit a crime due to fear of being easily recognized and apprehended (Rossmo, 2008; Block, Galary, & Brice, 2007). In the same sense, Canter and Hammond (2006) argue that distance estimation is a significant factor when offenders in the physical world shape their crime location choices and spatial behaviors prior to committing the crime. Back and colleagues (2018) found that due to the collapse of spatial distance there is no spatial border between the motivated offender and suitable target. In other words, cyber offenders can commit crimes against targets in different real-world time zones without any border controls. Yet, the question remains as to whether distance from the target is a key factor of deciding to commit a cybercrime (cyber offender behavior during the cybercrime and the level of violence) among cyber offenders. Specifically, it can be argued that the

physical distance between cyber offender and target does matter for cybercrime opportunity and the decision process of cyber offender.

Ouimet and Proulx (1994) provide a clear illustration that the level of violence of the crime is positively related to the distance traveled by the offender from his home to the target. This is because the farther offenders travel, the more they adapt a coercive approach, which in turn frequently leads to an increase in the level of violence during the commission of a crime (e.g., sexual offense). Moreover, although Rengert, Piquero, and Jones (1999) assert that the conventional rational choice analysis of criminal mobility would defend a least effort principle (e.g., there is no need to travel to a different location as opportunities are present here), Morselli and Royer (2008) and Clarke and Cornish (2001) argue that criminal mobility should also be considered a goal-oriented action (e.g., offenders who travel farther to commit their crimes had good reasons to do so). For example, criminal mobility might serve the goal of successfully completing the crime and avoiding detection (Beauregard & Busina, 2013; Hazelwood & Warren, 2004). According to Grabosky (2015) and Chang (2013), cybercriminals are prone to travel around the world in order to disrupt law enforcement's investigation and prosecution since they are likely to hide their physical location through a number of jurisdictions on the way to their target; moreover, cybercriminals prefer to stay in safe havens where cybercrime investigation treaties, extradition, and law enforcement cooperation are absent. In a study of cyberattacks, Holt and Kilger (2012) conclude that cyber offenders prefer to commit cyberattack against a foreign country's critical infrastructures and they tend to carefully prepare attacks against their targets. Given this situation, cyber offenders may be prone to travel further to commit crime with more severe damage or direct/immediate impact of damage to target. The

current study proposes to examine criminal mobility of cyber offenders during the cybercrime event.

Hypothesis [H9]: Cyber offenders who attack government or military entities will exhibit greater odds of committing more severe damage types (i.e., *outcome 1*: harassment/propaganda, stealing critical information, widespread theft of information, and critical network/infrastructure destruction; *outcome 2*: indirect/immediate, direct/delayed, direct/immediate) compared to the less severe damage type (i.e., *outcome 1*: probing without kinetic cyberattack; *outcome 2*: indirect/delayed).

According to Felson and Clarke (1998), accessibility is associated with the construction of communities, placing goods in easily accessible locations make it easy for offenders to commit crime. Hough (1987) asserted that the attractive targets of crime must be more attractive in that they are more accessible, or less guarded against the crime. When offenders search for targets, they select a certain target, which lack capable guardianship at that specific moment. Motivated cybercriminals abuse holes, gaps, or leaks in software (e.g., infect the online users' systems malware/virus) in order to successfully attack users (Leukfeldt, 2014). Additionally, Leukfeldt (2014) suggested that large organizations (e.g., government institutions and/or large companies) tend to defend their systems well against cyber threats by operating a higher level of digital capable guardianship as compared to smaller organizations or individual online users. Critical assets and sensitive information in these large organizations might become less accessible to cyber offenders when they take protective measures by installing and updating cybersecurity countermeasures and software. However, if these large organizations are hacked or destroyed by cyber offenders, it can lead to massive damage. Also, due to their higher level of cyber threat intelligence

and detection systems, cybercriminals prefer to attack quickly, achieve their goals, and then escape from these crime scenes as fast as they can. These offenders may also be more deliberate in their actions which should result in more severe damage. Therefore, the following analysis will test the hypothesis that attacks on government/military facilities will tend to be more severe. In this regard, the current study explores the association between the selection of cybercrime targets and cybercrime scenes.

In light of these research questions and hypotheses, this study, first, uses a descriptive research design to provide answers to the questions of who, what, where, and how US and international cybercrime offenders attacked suitable targets in the United States. Also, the SSBACO Cybercriminal Profiling Model is employed to empirically test the relationships between sociodemographic background factors, pre-cybercrime situational factors, cybercrime opportunity factors, and cybercrime scene characteristics.

Methodology

Data. Data were extracted from the Florida International University Law library website concerning cybercrime offense convictions. One database used for the foundation of the search was the Bloomberg Law for Case Dockets Research which contains federal and state court dockets and access case filings. To collect criminal record reports (i.e., indictment, complaints), the following terms were utilized for the query: cyber-fraud, hacking, cyberattack, online sexual crime, online illicit trade, cyberstalking, and cyberbullying, returning 1,829 federal court cases. Each case was read, and this search revealed 306 U.S. Federal court cases of cybercrime occurring between 2001 and 2018 which were used to empirically investigate the cyber-criminal profiling framework.

To collect quantitative data, the Dyadic Cyber Incident and Dispute (DCID)

Dataset, Version 1.5 Incident framework was employed to provide coding and interpretation of available variables applied to the 306 court cases. In fact, the DCID was able to provide the operational ideas of the variables, including offenses and offenders' information (i.e., age, gender, nationality, geographic information, type of cyber interaction for incidents, cyberattack methods utilized, type of target by cybercriminal, status of cybercriminal: individual/hacker or group/state-sponsored criminal, political objective, objective success, third-party initiator, severity level of cybercrime, and damage type). Previously, the DCID was designed to provide a method to construct a dataset for identifying cybercrime events. In addition, the Cyber Conflict Data Project was created to offer replicable and reliable datasets for all cyber threats between public and private sector targets. The original DCID dataset framework includes variables as the following lists (Maness, Valeriano, & Jensen, 2019) in Table 2. In other words, the DCID dataset framework provided a significant operational definition of measurement so that this study conceptualized and recreated new variables to measure the international and U.S. domestic cybercriminal profiles. The following sections specifically illustrate dependent and independent variables as well as the analytic plan.

Measures

Dependent variables. The current study focuses on measuring two dependent variables for each of the cases included in the analysis: 1) a severity scale of damage and 2) damage type. The severity scale of damage ranged from 1 to 5. Based on the codebook of the Dyadic Cyber Incident and Dispute (DCID), five-category scale for the severity of damage is as follows: 1 = probing without kinetic cyberattack, 2 = harassment, propaganda, nuisance disruption, 3 = stealing targeted critical information, 4 = widespread government,

economic, military, or critical private sector theft of information, 5 = critical network and infrastructure destruction. Damage type ranged from 1 to 4. Based on the codebook of the Dyadic Cyber Incident and Dispute (DCID), the four-category scale for damage type to victim/target was as follows: 1 = indirect and delayed, 2 = indirect and immediate, 3 = direct and delayed, and 4 = direct and immediate.

Independent Variables. As stated in the literature review, several researchers (see Holmes & Holmes, 2008; Beauregard, Lussier, & Proulx, 2008) have postulated a direct relationship between the personal characteristics of offender, the method of operation, the signature of offender, and the characteristics of crime scenes. Consistent with Beauregard and his colleagues' study (2008), the current study employed 13 items to measure individual characteristics of offenders, pre-cybercrime situational factors, and characteristics of the cybercrime opportunity.

Sociodemographic background factors. Sociodemographic background factors were measured using four variables: sex, age, offender type, and origin of cybercriminal. Sex was coded as 0 = female and 1 = male. Age is a continuous variable ranging from 18 to 68. The offender type variable is measured using dummy variables: individual cybercriminal (1 = individual, 0 = otherwise), hacking group (1 = hacking group, 0 = otherwise), organized cybercriminal syndicate (1 = organized cybercriminal syndicate, 0 = otherwise), state-sponsored cybercriminal (1 = state-sponsored cybercriminal, 0 = otherwise). Scaling for the cybercriminal's nationality was coded as 0 = Cybercriminal is US national and 1 = cybercriminal is foreign national.

Pre-cybercrime situational factors. Pre-cybercrime situational factors were measured from two variables including presence of illicit object(s) and presence of political

objective(s). Scaling for the above variables is as follows: presence of illicit object(s): 0 = did not possess drug, 1 = possessed drug; presence of political objective(s): 0 = no political objective, 1 = existence of political objective(s).

Characteristics of the cybercrime opportunity factors. To measure characteristics of the cybercrime opportunities, seven variables were utilized: (1) offender knew victim; (2) offender distance from victim or target; (3); single or multiple target (4) presence of co-offenders; (5) random or intended violence in cyberspace; (6) target type; (7) intimate relationship with target (see Appendix C). Scaling for whether the offender knew the victim is as follows: 0 = no, 1 = yes. Scaling for jurisdictional distance between offender and target locations are as follows: intracity level (1 = intracity level, 0 = otherwise), intercity level (1 = intercity level, 0 = otherwise), interstate level (1 = interstate level, 0 = otherwise), and international level (1 = international level, 0 = otherwise). Scaling for presence of co-offender is as follows: 0 = no, 1 = yes. Scaling for random or intended violence is as follows: 0 = random violence, 1 = intended violence. Scaling for target type variable is measured using dummy variables: individual (1 = individual, 0 = otherwise), business sector (1 = business sector, 0 = otherwise), government/military (1 = government/military, 0 = otherwise). Scaling for intimate relationship with victim is as follows: 0 = no, 1 = yes. Lastly, scaling for target count is as follows: 0 = single target, 1 = multiple targets.

Table 2. The Original DCID Dataset Framework

Variables
Cyber incident number (decided by dyad pair number and then earliest start date)
Dyad pair (combined the Correlates of War [COW] country codes)
State A (first state in the dyad by lowest COW country code)
State B (second state in the dyad by higher COW country code)
Name of cyber incident
Incident start date
Incident end date
Type of interaction (nuisance, defensive, offensive)
Method of interaction/incident, 1-4 with decimal denotations for infiltrations
Whether or not the incident is considered an advanced persistent threat (APT)
The type of target (private/non-state, government non-military, government military)
The initiator of the interaction (COW country code)
The specific coercive strategy of the cyber incident (disruption, short or long-term espionage)
Whether or not an information operation was used as a result of the cyber incident
Whether or not the incident successfully achieved its objective; did it breach the target's network and fulfill its intended purpose
Whether or not a third party was involved in the initiation or a target of the interaction
Whether or not an official government statement was issued by the initiator
Severity level on the 0-10 scale level
Damage type/period (1. Direct and immediate, 2. Direct and delayed, 3. Indirect and immediate, 4. Indirect and delayed)
Stated or interpreted strategic/political objective of the cyber incident
Key sources for the cyber incident

Analytic Method. All models were estimated using Statistical Package for the Social Sciences (SPSS) 23. First, a series of descriptive statistics were employed in order to provide the information regarding sociodemographic background factors (i.e., sex, age, cybercriminal types, domestic or international cyber offenders), situational factors (i.e.,

possessing illicit drugs, presence of political objectives), and criminal opportunity factors (i.e., offender distance, co-offending, type of targets, intimate relationship with target), and characteristics of cybercrime scenes. Second, Pearson's r was used to investigate correlations between variables. Third, multinomial logistic regression (MLR) equations[10] were utilized to model the associations between covariates, severity scale of damage, and damage type. The MLR is "a promising statistical technique that can be utilized to predict the likelihood of a categorical outcome variable" (Abdulhafedh, 2017; Peng & Nichols, 2003, p. 177). The MLR model estimates (k – 1) models, where k is the number of outcome levels of the dependent variable, and the k^{th} equation is associated with the reference group (Abdulhafedh, 2017); therefore, the categories "probing without kinetic cyberattack" and "indirect and delayed" are considered as the reference groups in these analyses.

Results

Descriptive Statistics. Descriptive analyses were performed to demonstrate the sample characteristics and responses to the candidate variables. Table 3 provides the descriptive statistics (i.e., minimum and maximum counts, means, standard deviations, and a number of the sample) for each dependent and independent variable in the bivariate and multivariate analyses in this study.

[10] Due to the ordinal nature of the dependent variables (severity scale of damage and damage type) in this chapter, a viable analytical strategy would be to use an ordinal regression equation. The issue, however, is that the model specification did not pass the test of parallel lines rendering the cumulative ordered logit estimates inaccurate. To clarify, the slope varies across each regression line generated from the equation, making the singular parameter estimate inaccurate. To remedy this situation, this study utilizes multinomial regression which generates a unique parameter estimate between each category in the outcome variable to preserve the accuracy of the interpretations in this dissertation.

Table 3. Descriptive Statistics: SSBACO Variables

Variables	Mean	SD	Min	Max
Dependent Variables				
Severity scale of damage	2.26	1.24	1	5
Period of damage initiation to victim/target	1.92	1.19	1	4
Background of Sociodemographic Factors				
Offender sex (Male =1)	.94	.24	0	1
Offender age	34.24	9.95	18	68
Offender type				
Individual criminal	.65	.47	0	1
Hacking group	.10	.30	0	1
Organized criminal group	.16	.36	0	1
State sponsored	.08	.26	0	1
International vs. U.S. cyber offender	.35	.47	0	1
Situational Factors				
Presence of illicit object (drugs)	.05	.21	0	1
Presence of political objective(s)	.06	.23	0	1
Characteristics of the Cybercrime Opportunities				
Offender knew victim or target	.40	.49	0	1
Random or intended violence (Intended = 1)	.42	.49	0	1
Intimate relationship with victim	.07	.24	0	1
Single or multiple victim/target (Multiple =1)	.76	.42	0	1
Presence of co-offender(s)	.63	.48	0	1
Jurisdictional distance between offender and target				
Intra-city level	.20	.39	0	1
Inter-city level	.11	.31	0	1
Inter-state level	.39	.48	0	1
International level	.30	.46	0	1
Victim or target type				
Individual online user	.48	.50	0	1
Business	.31	.46	0	1
Government & military	.19	.39	0	1

Table 4. Descriptive Statistics: Cybercriminals by country of origin

	N	%
Country of origin (N = 306)		
USA	199	65.0
Russia	22	7.2
Nigeria	16	5.2
Iran	14	4.6
Romania	12	3.9
Ukraine	8	2.6
China	5	1.6
Kazakhstan	5	1.6
Canada	4	1.3
UK	3	1.0
India	2	.7
Pakistan	2	.7
Israel	2	.7
Other (Australia, German, Italy, Moldova, North Korea, Sweden, Turkey, Latvia, Lebanon, Dominican Republic, Greece, Macedonia)	12	3.6

Table 4 shows that 65% of cybercrime incidents originated from the United States to victimize American citizens or targets followed by Russia (7.2%), Nigeria (5.2%), Iran (4.6%), Romania (3.9%), Ukraine (2.6%), China (1.6%), Kazakhstan (1.6%), Canada (1.3%), UK (1.0%), India (0.7%), Pakistan (0.7%), and Israel (0.7%).

Table 5. Descriptive Statistics: Cybercriminals by sex, age, accomplice, and type of targets

	N	%
Sex (N = 306)		
Female	19	6.2
Male	287	93.8
Age (N = 306)		
18 to 24	51	16.7
25 to 34	131	42.8
Over 34	124	40.5
Accomplice (N = 306)		
No	115	37.5
Yes	191	62.4
Type of Targets (N = 306)		
Individual user	148	48.0
Business sector	98	32.0
Government & Military	60	20.0

Table 5 indicates the descriptive statistics: cybercriminals by sex, age, accomplice, and type of targets. The results show that cybercrime was a male-dominated criminal activity (male, 93.8% and female, 6.2%). Inconsistent with literature (e.g., Back, LarPrade, Shehadeh, & Kim, 2019; Hadzhidimova & Payne, 2019) which contended the youth offenders are major populations of cybercrimes, 83% of cyber offenders were over age 25 (adult criminals). Further, 62.4% of cyber perpetrators have co-offended with one or more criminal(s). The most frequently targeted entities of cybercrime were individual users (48%), followed by the business sector (32%), and government and military (20%).

Regarding cybercriminal types in Table 6, 65% of offenders were individual cybercriminals followed by hacking groups (10.5%), organized crime groups (15.7%), and state-sponsored cybercriminals (7.8%). According to the results of the cybercrime typology (see Table 6), cyber fraud (39.5%) and hacking (31.4%) have been most pervasively committed by cybercriminals followed by cyberattacks (12.4%), online sexual crime (8.2%), online illicit trade (4.2%), and cyberstalking and cyberbullying (3.6%).

Table 6. Descriptive Statistics: Cybercriminal types and typology

	N	%
Cybercriminal types (N = 304)		
Individual cybercriminal	199	65.0
Hacking group	32	10.5
Organized group cybercriminals	48	15.7
State-sponsored cybercriminals	24	7.8
Cybercrime typology (N = 304)		
Cyber-fraud	121	39.5
Hacking	96	31.4
Cyberattack	38	12.4
Online sexual crime	25	8.2
Online illicit trade	13	4.2
Cyberstalking & Cyberbullying	11	3.6

Bivariate Relationships. The current study examines the relationships between sociodemographic background factors (i.e., sex, age, cybercriminal types, domestic or international cyber offenders), situational factors (i.e., presence of drugs or political

objectives), criminal opportunity factors (i.e., offender distance, co-offending, type of targets), severity scale of damage, and damage type.

Table 7 shows the bivariate correlations of the study variables. Certain SSBACO variables were significantly correlated with both the cybercrime severity scale of damage and damage type. First, state-sponsored cybercriminals (r = 0.41, $p < .01$), political objective (r = 0.33, $p < .01$), international level distance (r = 0.24, $p < .01$), and government/military (r = 0.44, $p < .01$) were significantly correlated with cybercrime severity scale of damage. Second, individual cybercriminal (r = 0.29, $p < .01$), organized criminal group (r = - 0.31, $p < .01$), co-offending (r = -0.27, $p < .01$), and intra-city level distance (r = 0.31, $p < .01$) were correlated with damage type. In accordance with the bivariate relationships, the cybercriminals who were international cyber offenders with political objective(s) were more likely to cause more severe damage to targets. Also, individual cybercriminal and organized cybercriminal group were more likely to engage in indirect and delayed cybercrime damages to targets; cyber offenders who were from other states or international cybercriminals tended to engage in direct and immediate damages to targets.

Table 7. Correlation Matrix: SSBACO Variables

	1	2	3	4	5	6	7	8	9	10	11
1	1										
2	.54**	1									
3	-.04	.02	1								
4	-.07	-.04	-.11*	1							
5	-.12*	.29**	-.07	-.02	1						
6	-.11	-.05	-.01	.12*	-.46**	1					
7	-.05	-.31**	.07	-.05	-.58**	-.14**	1				
8	.41**	-.01	.02	-.01	-.39**	-.10	-.12*	1			
9	.24**	-.06	.10	-.01	-.35**	-.04	.24**	.37**	1		
10	-.01	-.10	.06	.01	.01	-.07	.10	-.06	-.10	1	
11	.34**	.08	.06	.03	-.16**	-.08	-.11	.54**	.19**	-.05	1

Note: *$p < .05$; **$p < .01$; 1 = Severity scale of damage; 2 = Damage type; 3 = Offender sex; 4 = Offender age; 5 = Individual cybercriminals; 6 = Hacking group; 7 = Organized criminal group; 8 = State-sponsored cybercriminals; 9 = International cybercriminals vs. U.S. cyber offenders; 10 = Possession of illicit objects; 11 = Political objectives

Table 7. Continued

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1													
2	.54	1												
3	.17**	.15**	1											
4	.22**	.15**	.89**	1										
5	-.02	.10	.33**	.25**	1									
6	-.03	-.15**	-.35**	-.30**	-.10	1								
7	.05	-.27**	-.29**	-.27**	-.10	.20**	1							
8	-.06	.31**	.16**	.16**	.17**	-.13*	-.45**	1						
9	-.07	.04	.10	.06	-.04	-.20**	-.17**	-.17**	1					
10	-.13*	-.21**	-.05	-.05	-.02	.01	.16**	-.39**	-.27**	1				
11	.24**	-.07	-.15**	-.12*	-.09	.24**	.32**	-.32**	-.23**	-.53**	11			
12	-.28**	-.11*	-.15**	-.20**	.24**	.27**	-.02	.15**	-.20**	.21**	-.22**	1		
13	-.09	.01	.01	.06	-.18**	-.28**	-.09	-.06	.19**	-.11	.04	-.65**	1	
14	.44**	.10	.19**	.19**	-.09	-.01	.12*	-.09	-.01	-.14**	.24**	-.46**	-.32**	1

Note: *$p < .05$; **$p < .01$; 1 = Severity scale of damage; 2 = Damage type; 3 = Offender knew victim; 4 = Random or Intended violence; 5 = Intimate relationship with target; 6 = Single or Multiple target(s); 7 = Co-offender; 8 = Intra-city; 9 = Inter-city; 10 = Inter-state; 11 = international; 12 = Individual user; 13 = Business sector; 14 = Government/military

Multinomial Logistic Regression (MLR) Results of Severity Scale of Damage. Table 8 presents the results of the series of MLR models conducted in order to investigate the relationships between sociodemographic background factors, situational factors, and cybercrime opportunity factors and the dependent variable (severity scale of damage) in this study. To that end, in the regression models, "individual cybercriminal" is the reference for offender type variable; "international level" is the reference for jurisdiction distance between offender and target variable; "individual online user" is the reference for target type variable. The Goodness of Fit Table shows that Pearson's chi-square and a deviance chi-square for the tests were not statistically significant. The pseudo R-square values produced in these MLR models are 0.65 (Cox and Snell) and 0.69 (Nagelkerke) respectively, suggesting that between 65% and 69% of the variability is explained by this set of variables used in the models. Given these results of statistics, data fits the model used in this dissertation very well.

To scrutinize the relationship of independent and dependent variables, the likelihood ratio test evaluates the overall relationship between independent and dependent variables. As shown in Table 8, organized criminal groups were on average 4.12 times more likely to engage in harassment, propaganda, and nuisance disruption in comparison to probing than individual offenders (OR = 4.12, 95% CI = [1.21, 14.05]). Overall, however, there were no statistically significant effects for sociodemographic background factors.

Table 8. MLR Results of Severity Scale of Damage (N = 306)

	Harassment, Propaganda		Stealing Critical Info		Widespread Theft		Critical Infra Destruction	
	B	OR	*B*	OR	*B*	OR	*B*	OR
Sociodemographic								
Offender sex	2.40	11.07	16.99	24.21	-.60	.54	-1.13	.32
Offender age	.01	1.01	.04	1.05	-.08	.99	-.04	.95
Offender type								
Hacking group[a]	.68	1.98	.06	1.06	-1.51	.22	-17.40	2.76
Organized criminal group[a]	1.41*	4.12	.74	2.09	-.18	.83	-16.04	1.08
State sponsored[a]	17.12	101.33	-1.06	.34	17.34	34.68	15.31	44.86
International vs. U.S. offender	-1.00	.36	-1.37	.25	.46	1.58	.73	2.09
Situational Factors								
Presence of illicit drugs	-15.21	2.46	1.67	5.33	1.02	2.79	-31.62	1.83
Presence of political objective(s)	15.79***	72.67	17.96***	63.16	17.57***	43.61	18.39***	97.16
Cybercrime Opportunities								
Offender knew target	-1.38	.24	-.97	.37	-1.14	.31	-.65	.52
Random or intended violence	1.46	4.31	2.40	11.09	2.35	10.53	1.82	6.20
Intimate relationship with target	32.35	112.92	-1.25	.28	-2.38	.09	29.92	99.79
Single or multiple target(s)	.52	1.69	-.09	.90	-.80	.44	-.31	.73
Presence of co-offender(s)	-1.44**	.23	-.71	.48	1.25	3.50	.19	1.21
Distance between offender and target								
Intra-city[b]	.35	1.42	-3.15*	.04	-1.26	.28	-.17	.83
Inter-city[b]	.34	1.41	-1.04	.35	-2.32	.09	-16.35	7.86
Inter-state[b]	-.44	.64	-3.15**	.04	-.71	.49	.81	2.26
Target type								
Business[c]	-1.27*	.28	-.92	.39	.50	1.65	-1.22	.29
Government & military[c]	.70	2.02	-.52	.59	2.81***	16.62	2.18*	8.86

Note: *$p < .05$; **$p < .01$; ***$p < .001$; [a] reference for offender type variable is individual cybercriminal; [b] reference for jurisdictional distance variable is international; [c] reference for target type variable is individual online user

Also, Table 8 indicates that there is a statistically significant, positive association between presence of political objective(s) and severity scale of damage. For example, when cyber offenders have political objective(s), they caused 72, 63, 43, and 97 times more severe damages to the target (i.e., harassment, propaganda, and nuisance disruption [OR = 72.67]; stealing targeted critical information [OR = 63.16]; widespread theft [OR = 43.61]; critical network/infrastructure destruction [OR = 97.16]) in comparison to probing. In contrast, there were no statistically significant effect for presence of illicit drugs.

Cyber offenders had 77% lower odds of working with an accomplice when committing harassment, propaganda, and nuisance disruption in comparison to probing (OR = 0.23, 95% CI = [0.08, 0.66]). As a type of targets, business sectors had 72% lower odds of being targeted for harassment, propaganda, and nuisance disruption in comparison to probing than individual online users (OR = 0.28, 95% CI = [0.10, 0.78]). On the other hand, government sectors exhibited 16 times greater odds of being targeted for widespread theft in comparison to probing than individual online users (OR = 16.62, 95% CI = [3.47, 79.65]). Similarly, government sectors experienced 8 times greater odds of being targeted for critical network and infrastructure destruction in comparison to probing than individual online users (OR = 8.86, 95% CI = [1.02, 76.86]). As offender's distance level from target, intra-city level distances exhibited 96% lower odds of engaging in stealing targeted critical information in comparison to probing than international level distances (OR = 0.04, 95% CI = [0.003, 0.530]). Also, inter-state level distances exhibited 96% lower odds of engaging in stealing targeted critical information in comparison to probing than international level distances (OR = 0.04, 95% CI = [0.005, 0.382]).

As with these findings, cybercriminals with political objective(s) had greater odds of causing more severe damage than cybercriminals without political objective(s); cyber offenders who were close to the victim/target had lower odds of engaging in severe damage than cybercriminals residing far from the victim/target; cyber offenders who attacked governmental/military targets had greater odds of engaging in more severe damage than cyber offenders who attacked individual online users. Of these, the findings of this study provide support for hypothesis 2, 8, and 9.

Multinomial Logistic Regression (MLR) Results of Damage Type. Table 9 displays the results of the series of MLR models conducted in order to examine associations between situational factors, cybercrime opportunity factors, sociodemographic factors, and a dependent variable (damage type) in this study. Likewise, in the regression models, "individual cybercriminal" is the reference for offender type variable; "international level" is the reference for jurisdiction distance between offender and target variable; "individual online user" is the reference for target type variable. The Goodness of Fit Table shows that Pearson's chi-square and a deviance chi-square for the tests were not statistically significant. The pseudo R-square values produced in these MLR models are .53 (Cox and Snell) and 0.59 (Nagelkerke). Thus, the model with the variables fit well to analyze the proposed hypotheses in the present study.

Table 9. MLR Results of Period of Damage Type (N = 306)

	Indirect&Immediate		Direct & Delayed		Direct&Immediate	
	B	OR	*B*	OR	*B*	OR
Sociodemographic						
Offender sex	17.83	55.19	-.09	.90	.47	1.60
Offender age	.04	1.04	-.01	.98	-.02	.97
Offender type						
Hacking group[a]	.17	1.19	-1.60	.20	.28	1.32
Organized criminal group[a]	-2.68	.06	-3.26	.03	-17.35	2.90
State sponsored[a]	2.29	9.87	-19.44	3.59	-2.74	.06
International vs. U.S	.92	2.51	.69	2.01	-.76	.46
Situational Factors						
Presence of illicit drugs	.68	1.98	-18.30	1.12	-1.76	.17
Presence of political objective(s)	.06	1.06	1.77	5.89	2.25	9.57
Cybercrime Opportunities						
Offender knew target	.30	1.35	.16	1.17	-.33	.71
Random or intended violence	-.79	.45	.09	1.10	.07	1.07
Intimate relationship with target	1.68	5.37	3.48***	32.55	.32	1.38
Single or multiple target(s)	-.72	.48	1.41	4.12	-1.01	.36
Presence of co-offender(s)	-.41	.66	.07	1.07	-.50	.60
Jurisdictional distance between offender and target						
Intra-city[b]	-1.49	.22	1.62	5.09	-.11	.89
Inter-city[b]	.80	2.22	1.44	4.24	-2.79*	.06
Inter-state[b]	-1.28	.27	-.03	.96	-1.91*	.14
Target type						
Business[c]	-.29	.74	.67	1.95	-.01	.99
Government & military[c]	.86	2.37	-1.44	.23	1.26*	3.55

Note: *$p < .05$; **$p < .01$; ***$p < .001$; [a] reference for offender type variable is individual cybercriminal; [b] reference for jurisdictional distance is international; [c] reference for target type variable is individual online user

According to Table 9, cyber offenders who had an intimate relationship with targets had 32 times greater odds of causing direct and delayed damage in comparison to indirect and delayed damage than cyber offenders who did not have intimate relations with targets (OR = 32.55, 95% CI = [4.10, 258.40]). In this case, cybercriminals who had an intimate relationship with targets tend to cause direct damages to the target; however, the costs of damage would be felt at a future point in time. For example, the former employee of a nuclear plant who had an intimate relationship with an employer could disrupt its facility by directly damaging the centrifuges, but the impact of this attack might take a number of months. To that end, this result provides support for hypothesis 5.

In terms of the offender's distance from the target, Table 9 indicates that cyber offenders at inter-city level distances had 94% lower odds of causing direct and immediate damage in comparison to indirect and delayed damage than international level distances (OR = 0.06, 95% CI = [0.007, 0.55]). Likewise, cyber offenders at inter-state level distances had 86% lower odds of causing direct and immediate damage in comparison to indirect and delayed damage than international level distances (OR = 0.14, 95% CI = [0.03, 0.68]). Given these results, cyber offenders who were close to the victim/target had lower odds of engaging in direct/immediate damage initiation than cyber offenders residing far from the victim/target. As such, the results in Table 9 provide support for hypothesis 8.

Lastly, cyber offenders who attacked government sectors had 3.55 times greater odds of causing direct and immediate damage in comparison to indirect and delayed damage than individual online users (OR = 3.55, 95% CI = [1.05, 11.97]). As stated in the literature review section, the large organizations such as businesses and governmental/military entities have better protective measures through cybersecurity

countermeasures. Therefore, to avoid detection and prosecution by information security officers or law enforcement, cybercriminals who attack government/military entities might prefer to directly conduct their criminal operations against its targets which lead to immediate damages occurred. In this sense, this result provides support for hypothesis 9. However, there were no statistically significant effects for sex or age or offender type or international cyber offender/U.S. domestic cyber offender.

Discussion and Conclusion

While previous research has applied criminal profiling techniques to empirically examine patterns and crime event for conventional criminals (e.g., theft, serial killer, serial sexual offender, terrorists, etc.), little has empirically been conducted on cybercriminal profiles and cybercrime scenes. In addition, there is lack of cybercriminal profiling theoretical framework. Thus, this study contributes to the existing literature by proposing a theoretical framework, called the SSBACO cybercriminal profiling model, for assisting law enforcement in solving an emerging field of crime. As such, this study sought to examine whether there were relationships between the sociodemographic background characteristics of offenders, pre-cybercrime situational factors, and characteristics of the cybercrime opportunity factors, and cybercrime damage and type. To that end, the main findings of this study support the extension of the crime triangle framework (i.e., motivated offender) to the context of cybercrime offenses.

Sociodemographic Factors. This study shows that, overall, sociodemographic factors were not strongly associated with the characteristics of the cybercrime scene. Interestingly, cybercriminals affiliated with an organized crime group caused less severe damage to targets than individual cybercriminals. Otherwise, the findings of this study

show that other sociodemographic background factors (i.e., gender, age, and international/US offenders) were not statistically significant predictors of the severity of damage and damage type. Nevertheless, in light of interpersonal cybercrime patterns in the analysis, one thing that needs to be discussed is that female cyber offenders have rarely been involved in online sexual crimes (e.g., presence or production and distribution of child porn, online sexual solicitation), whereas some female offenders have engaged in cyberstalking and cyberbullying offenses. In other words, online sexual crimes have been male-dominated cybercrime (Shannon, 2008; Taylor et al., 2019).

Situational Conditions and Cybercrime Opportunity Factors. Similar to previous studies (Marshall & Barbaree, 1990; Earls & Marshall, 1983; Salfati, 2000; Beauregard et al., 2008), the results indicated that some situational/opportunity factors influenced the characteristics of cybercrime scenes. First, there is a relationship between pre-crime situational factor (presence of political objective) and the characteristics of cybercrime scenes. For example, when cybercriminals had political objective(s), they were 97 times more likely to engage in critical network/infrastructure destruction in comparison to probing than cybercriminals did not have political objective(s). This result may suggest that, in response to a political situation or conflict, these motivated offenders might want to immediately demonstrate more aggressive political protests or damage targets more severely through cyberattacks or cyberterrorism.

Second, this study also found that certain cybercrime opportunities – (1) offender's distance from target, (2) type of target, and (3) intimate relationship with target – were significant predictors for cybercrime scenes. Remarkably, cyber offenders tended to select and attack targets in different jurisdictions (different countries or states) and targets'

physical location are farther from where they live (Hadzhidimova & Payne, 2019). In addition, 211 out of 304 cybercrime cases were committed beyond the intercity level. This pattern can trigger the jurisdiction issue for cybercrime investigation and prosecution. This finding does not support the evidence (Block & Block, 1999; Canter & Gregory, 1994; Jahankhani, & Al-Nemrat, 2012; Sarangi & Youngs, 2006; Jansen & van Koppen, 1998) provided from prior studies in which the offender in the physical world travelled close to where he or she lives. Moreover, when cyber offenders travelled further, they were more likely to engage in more severe types of cybercrime and damage with direct and immediate impact of damage to target.

Given the borderless nature of cybercrime, cyber perpetrators can more easily victimize many people all over the globe including the United States. They can commit cybercrime more severely and anonymously without ever setting foot in the targeted victim's location. Grabosky (2015) asserted that cyber offenders attempt to conceal their physical location through a number of jurisdictions on the way to their target. Sophisticated cybercriminals have more opportunities to reach into the targets over the Internet from the nations called safe havens where cybercrime investigation treaties, extradition, law enforcement cooperation, and technical capacity are absent in order to hide in the shadows of Internet. In short, the findings of these characteristics of crime events may explain that cyber offenders' geospatial behaviors differ from offenders in the physical world due to the collapse of spatial and temporal orderings. However, offender- and victim- physical locations are still crucial factors to effectively prosecute cybercrime scene and to reduce cybercriminal opportunities.

Lastly, the results indicated that target type was a significant predictor of the severity of damage and damage type. In particular, government/military entities or some business sectors (Simon, 2017) oversee the operation of critical infrastructures (e.g., water and food supplies, electricity and gas, telecommunications and broadcasting, health services, the financial system and the transportation system). Recently, these critical infrastructures are driven by computer/network systems as a result of the growing interconnectedness. This reliance on computers and networks raises critical infrastructure's vulnerability since disrupting these high-value cybercrime targets results in massive economic, political and social effects (Moteff & Parfomak, 2004). Thus, normally these entities have higher level of cybersecurity systems and agile cyber threat detection systems. However, if a cyber offender exploits a vulnerability in the system, it can cause a massive damage to critical infrastructure. In line with offender decision making perspective, cybercriminals may want to quickly approach these entities and achieve their criminal goals and then immediately escape from cybercrime investigation and prosecution. As such, government/military targets were more likely to be experienced in more severe damage and direct/immediate cyber threats.

In sum, the major findings suggest that the SSBACO Cybercriminal Profiling model can be a scientific and useful tool to prioritize suspects, establishing new lines of scrutiny in cybercrime investigation. In this study, the findings highlight that situational/opportunity factors (i.e., pre-crime situational conditions, offender's geospatial behaviors, victim/target type) are associated with cybercrime scene, especially cybercrime damage.

Policy Implications. The findings of this study provide significant implications for practice. First, according to the results of cybercriminals' geospatial behaviors, cyber offenders often commit cyber violence from one jurisdiction against a target in another jurisdiction (e.g., state or country). For example, an American prosecutor indicted two Russian state-sponsored hackers who resided in Bulgaria and Ukraine for their commission of cyberattacks and cyber espionages against US government agencies. The hackers never set foot in the United States. Thus, the question remains: who is responsible for investigating and prosecuting the cybercrime case (Grabosky, 2016)? The lack of extradition relationships between certain nations makes it hard to proactively deter cybercrimes (Holt, 2013; Brenner, 2010; Holt & Bossler, 2013; Holt, Freilich, & Chermak, 2017). As such, it is necessary to improve the jurisdiction issue along with cybercrime investigation treaties or extraditions as well as international cooperation with foreign law enforcement partners, which eventually facilitates reduced cybercriminal opportunities derived from the borderless nature of cybercrime.

Second, cyber patrol can reduce cybercriminal opportunities. Cybercrime units or specialized forces are essential to patrol cyberspace, and to detect high tech cybercriminals who strive to hide behind geographic borders by using various encryption and hacking toolkits or the dark web, which makes it very difficult to identify a suspect. Thus, through enhancing cybercrime units or specialized cybercrime forces, law enforcement can have an exponential impact on detecting and prosecuting cybercrime offenses, which will help to disrupt cybercriminal opportunities.

Limitations. The study in this chapter had two noteworthy limitations. First, although court complaint/indictment documents provided significant information

regarding features of cybercriminals and victims, and cybercrime scenes, there is room to fill in the gaps in order to increase the accuracy and validity of cybercriminal profiling. For example, there is an absence of information concerning victim's characteristics (e.g., gender, age, address, type of damage, occupation, online activity at the time of the crime), making it difficult to examine the relationships between victim's characteristics, crime scene, and offender features as well as offender-victim interaction. Thus, future studies of cybercriminal profiling can fruitfully analyze the following features in light of the work of Farrington and Lambert (1997):

1. Offender: Address, sex, age, ethnicity, marital status, nationality, distinctive physical features, felony history, occupation, accomplice, intent, motivation.
2. Offense: Location, site, physical location of computer server to attack, time, day, date, cybercrime method, instruments or weapons, methods of escape, offender using drink or drugs or pornography, presence of illicit objects, severity of damage, typology.
3. Victim: Address, sex, age, ethnicity, marital status, occupation, online activity at the time of the crime, type of damage, monetary loss.
4. Victim report of offender: All offender variables except address.

A second limitation highlights the difficulty of measuring the relationships between individual characteristics of the offender (i.e., motivation, antisocial tendency, psychosocial deficits) and severity of damage and typology using court documents. As such, I was unable to reveal the causal factors about why the offenders engage in the commission of cybercrime. Third, many potential profiles of cyber offenders were not included in this cybercriminal profiling analysis because the current study has only utilized

the profiles of the offenders who have been sentenced during a particular time-period (2001-2018) in the United States. Therefore, it may lead to errors and misleading results due to a sample selection bias. Lastly, the present study was limited to reveal the relationship between the use of drug(s) and cybercrime offending since the court documents analyzed in this study did not provide information as to whether cyber offenders had taken illegal drug(s) when they committed cyber violence. Thus, future research should address these issues stated above by including qualitative interviews and self-report survey methods which help provide an in-depth understanding of cyber offender's motive, psychosocial status, etc.

CHAPTER 4

IMPACTS OF PERCEIVED RISK OF CYBER-THREATS, DIGITAL CAPABLE GUARDIANSHIP, AND ONLINE ACTIVITY ON CYBERCRIME VICTIMIZATION

Following the exploration of cybercrime offenses, this chapter seeks to explore another dimension of the cybercrime triangle – cybercrime victimization. According to the literature review chapter, a large body of research has been conducted in order to examine the application of routine activity theory to cybercrime victimization. Many criminologists contend that traditional routine activity theory can be a useful framework to explain the occurrence of cybercrime victimization. Specific behaviors and the status of online users can generate new opportunities for criminals to commit cyber-threats when capable guardians are absent. For example, researchers (e.g., Choi, 2008; Holt & Bossler, 2008; Bossler, Holt, & May, 2012; Newman & Clarke, 2003; Pratt et al., 2010; Reyns et al., 2011; Wilsem, 2011, 2013) argue that online exposure (e.g., spending time online and purchasing from online retailers) and digital capable guardianship (e.g., target hardening techniques) might be significantly associated with cybercrime victimization. However, these empirical tests have generated mixed results (Williams & Levi, 2015).

To prevent cyber-threats, state-of-the-art cybersecurity systems and cyber hygiene – maintaining healthy circumstances of computer/network systems from malicous codes or viruses – are the most important factors; however, cybersecurity professionals also say human factors can be critical components of cybercrime prevention strategies. On one hand, the human element is a pivotal component to disrupt cyber threats. On the other hand, humans can be very vulnerable and easily deceived by advanced technologies and social

engineering schemes along inadequate countermeasures in the combat against cybercrime (Back & LaPrade, 2019). In a broad sense, some scholars (Lee & Downing, 2019; Lee, Choi, Choi, & Englander, 2019) assert that certain human factors (e.g., the perceived risk of crime or online users' behavior) can be crucial predictors to decrease the likelihood of crime victimization in the physical and cyber world. Typically, the perceived risk of crime threats may alter a potential victim's routine activities, which may lead to fewer risky situations (Rengifo & Bolton, 2012). Unfortunately, the risk perception factor has rarely been applied to empirically examine cybercrime victimization. Most studies focused on examining the relationships between online behavior, online lifestyle, cybersecurity management, and cybercrime victimization. Nevertheless, few studies have investigated the link between perceived risk of cyber-threats and cybercrime victimization. To fill the gaps in the literature, this study focuses on the concepts of perceived risk of cyber-threats, online activity, and digital capable guardians as predictors of cybercrime victimization. The following sections in this chapter discuss the theoretical background (i.e., online routine activity, digital capable guardian, perceived risk of crime), research questions, hypotheses, methods, variables, and major findings.

Background

From the crime triangle framework, capable guardian and routine activity tenets contribute to the cybercrime victimization model in this study. In addition, perceived risk of cybercrime victimization derived from the perceived risk of crime literature was employed to test mediation effects on the relationship between online routine activity, capable guardianship, and cybercrime victimization.

Digital Capable Guardianship and Online Routine Activity. Since the original RAT developed by Cohen and Felson (1979), a large body of research focused on examining the capable guardian measure and routine activity to explain how the absence of capable guardian and regular routines of potential victims can increase the risk of crime victimization. The capability of persons and/or objectives that protect citizens and facilities against criminals are regarded as guardianship. Typically, capable guardians, especially physical capable guardians, have been commonly utilized to prevent residential burglary. Existing studies found that burglar alarms, external lights, extra locks, and other security devices help decrease the risk of burglar and larceny victimization (Coupe & Blake, 2006; Cromwell & Olson, 2004; Miethe & McDowall, 1993). Routine activity refers to the daily routine activities, some of which can put individuals in greater danger of crime in physical and virtual spaces, since certain activities place individuals in closer proximity to motivated offenders (Cohen & Felson, 2016; Bossler & Holt, 2009). In the cyber world, daily routine activities include online banking, online shopping, accessing social network sites, and email. Newman and Clarke (2003) were the first criminologists to apply the concepts of Internet target accessibility (increased by the absence of capable guardianship) and visibility (increased by the variety and frequency of online routine activities, e.g., shopping and banking) derived from RAT to cybercrime (Williams, 2016, p. 23). Bossler and Holt (2009), Reyns (2013), and Williams (2016) assert that Choi (2008) was the first cyber-criminologist to examine the relationship between physical capable guardians (i.e., anti-virus software), online routine activities, and cybercrime victimization.

Grobosky and Smith (2001) argue that capable guardianship has commonly been used to protect online users from cyber-threat since the 1990s. According to Williams

(2016), the forms of personal capable guardianship can be composed of three types: (1) passive physical guardianship, (2) active personal guardianship, and (3) avoidance personal guardianship. First, passive physical guardianship includes individuals' protective behaviors such as using only their own computer, email spam filtering, installing anti-virus and secure browsing. Second, active personal guardianship consists of active protective actions (e.g., changing security settings and passwords). Third, avoidance personal guardianship is composed of passive online actions (e.g., doing less online banking and shopping).

The applications of capable guardianship to various cybercrimes (e.g., malware infection, cyber piracy, cyberbullying, cyber-harassment, cyberstalking, unauthorized access, and identity theft) have been empirically tested and obtained mixed results (Welsh & Farrington, 2014; Wilcox & Cullen, 2018; William, 2016). For example, digital capable guardianship was not a significant predictor of cyber-harassment or hacking attacks (e.g., Bossler & Holt, 2009; Holtfreter et al, 2008; Marcum et al., 2010). Consistent with prior research, Leukfeldt (2014) explored the relationship between digital capable guardians and phishing victimization; however, no relationship was observed between the two variables. Interestingly, some studies found that passive physical guardianship (e.g., Choi, 2008; Choi & Lee, 2017; Williams, 2016) is a strong predictor to mitigate the risk of computer crime (e.g., malware infection and identity theft) or cyber-harassment (e.g., Back, 2016).

Remarkably, Williams (2016) applied RAT to online identity theft in Europe at the country and individual level. Similar to the current study, the work of Williams used data derived from the Special Eurobarometer 390 survey on cybersecurity, collected in 2012. The sample size was 26,593 and country-level multistage random probability sampling was

adjusted. Williams' study focused on the concepts of online routine activities, active personal, avoidance personal and passive physical guardianship as predictors of online identity theft victimization. In addition, he tested the relationships between the country level capable guardianship, Internet penetration, economic performance, and level of urbanicity through the series of multi-level Poisson regression models.

Similar to the application of digital capable guardianship to cybercrime victimization, criminological research has largely explored various types of cybercrime victimization using the online routine activity component of RAT as a framework (Holt & Bossler, 2013). Choi (2008, 2017), Reyns (2013), and Williams (2016) elaborate that the online routine activity tenet includes Internet activities (online banking and shopping, and social networking and emailing), location of Internet access (home, university, public, café, work), and frequency of Internet use. Accordingly, there are also mixed results for the association between online routine activities and cybercrime victimization. In this regard, while many researchers (e.g., Al-Nemrat, Jahankhani, & Preston, 2010; Bossler & Holt, 2009; Holtfreter, Reisig, & Pratt, 2008; Hutchings & Hayes, 2009; Marcum, Higgins, & Ricketts ,2010; Pratt et. al, 2010; Pyrooz, Decker, & Moule, 2015; Reyns, 2013; Reyns, 2015; Reyns & Henson, 2016; Williams, 2016; Wolfe et al., 2016) provide support for the hypothesis that online routine activity (e.g., online exposure) increases the likelihood of cybercrime victimization, some studies found that there is no effect of online routine activity on cybercrime victimization (e.g., Holt & Bossler, 2008; Holt & Bossler, 2013).

Interestingly, online routine activity is strongly associated with interpersonal cybercrime (e.g., cyberbullying, cyberstalking, cyber-harassment, internet fraud), whereas online routine activity is less likely to influence the likelihood of computer crime

victimization (e.g., hacking, malware infection, unauthorized access, identity theft). For instance, Pratt and associates (2010) empirically examined the associations between personal characteristics, online routines, and Internet fraud victimization. Data from a representative sample of 922 respondents from a statewide survey in Florida were analyzed. Pratt and colleagues assessed whether online routine activities and sociodemographic characteristics increase the likelihood of Internet fraud victimization. The findings of their study showed that online routine activities such as online purchases and visiting online forums were statistically significant factors to increase the risk of internet fraud victimization. Additionally, Reyns (2013) found that online routine activity variables – online banking, online shopping, e-mail or IM, and downloading free software/music/video – were positively related with the odds of identity theft victimization.

Despite numerous studies estimating the effects of capable guardianship and online routine activity theory on reducing cybercrime victimization, there is a gap in the literature. For example, Williams' study was limited due to only focusing on the online identity theft victimization. Also, other studies (e.g., Bossler & Holt, 2009; Reyne, 2013; Choi, 2008; Choi & Lee, 2017) have significant limitations with their sample derived from college student populations that may make the findings hard to generalize to the broader population. Therefore, the present study contributes to extend previous works aimed at testing the effect of guardianship on various types of cybercrime victimization (i.e., online identity theft, phishing email, purchase fraud, extremist materials, and cyberattack) and diverse population with the Special Eurobarometer Surveys from 2012 through 2014.

Perceived Risk of Cybercrime Victimization. Several studies have suggested that there is a link between perceived risk of crime and crime victimization. Rader, May, and

Goodrum (2007) and Ferarro (1995) contend that perceived risk is a cognitive or rational judgment that determines the likelihood of crime victimization. The perceived risk of crime may be directly/indirectly formed by experience of crime victimization or certain crime awareness programs. Further, Reisig, Pratt, and Holtfreter (2009) and Warr (2000) assert that perceived risk of crime victimization may cause individuals to constrain themselves to change their daily routine activities.

It is important to note that perceived risk of cyber-threats, in conjunction with individuals' online routine activities and implementing digital capable guardians, operates to increase or decrease the likelihood of cybercrime victimization (Reyns, 2013). Few studies have been conducted on the relationship between perceived risk of cyber-adversaries and cybercrime victimization. For example, Reyns (2013) found that perceived risk of identity theft victimization was statistically and positively associated with the odds of identity theft victimization. The finding of Reyns' (2013) study revealed that those perceiving themselves as at high risk of identity theft were three times more likely to be victimized for identity theft. Consistent with previous research, Riek, Bohme, and Moore (2015) examined whether the relationship between cybercrime experience and avoidance of online services is mediated by perceived risk of cybercrime. They asserted that individuals who perceived less cybercrime risk are more likely to participate in online activities. To that end, findings of the relationship between perceived risk of cyber-threats and cybercrime victimization have been inconsistent or in an unpredicted (inverse) direction. Illustrating the causal relationship between perceived risk of cyber-threats and cybercrime victimization remains an open empirical question; thus, future studies are needed to clarify the nature of those associations. This study employed a single pooled

sample drawn from three existing cohort studies which have been collected at three consecutive time points (i.e., 2012, 2013, 2014) from individuals across twenty-eight European countries because integrative data analysis can have "the potential to provide substantial increases in statistical power for testing research hypotheses through the combination of multiple individual data sets" (Cohen, 1992; Maxwell, 2004; Curran & Hussong, 2009, p, 5).

Mediation Effects on Cybercrime Victimization Through Perceived Risk. To date, studies concerning mediation effects of perceived risk on cybercrime victimization are very rare. Riek, Bohme, and Moore (2015) found the relationship between cybercrime victimization and avoidance intention from online services is mediated by perceived risk of cybercrime. Although Riek and colleagues' (2015) study applied the perceived risk of cybercrime concept to measure the mediation effect on avoidance intention from online services, it was not a study to investigate the mediation effect on the relationship between perceived risk of cyber-threat and cybercrime victimization. To that end, there is no study investigating whether online routine activity and capable guardianship mediate the impact of perceived cyber threat risk on cybercrime victimization. This phase of the dissertation examines whether the variables (online routine activity and digital capable guardianship) mediate the relationship between perceived risk of cyber threats and cybercrime victimization. As a result, the current study contributes to the existing literature by testing the theoretical explanation and the statistical significance of mediating analysis for the associations between human factors (e.g., perception of risk and online behavior) and the nature of cybercrime victimization.

In reviewing the literature, previous studies provide mixed evidence regarding the associations between online routine activity (i.e., online exposure), digital capable guardianship, and cybercrime victimization. In a broad sense, there is no specific study to provide support that these variables have mediation effects on the relationship between perceived risk of cyber-threat and cybercrime victimization. Therefore, the current study aims to build on the study of the existing literature (e.g., Riek, Bohme, & Moore, 2015) and add to the embryonic literature on cognitive and behavioral research of cybercrime. The specific research questions and hypotheses related to the relationships between the perceived risk of cyber-threat, online routine activity, digital capable guardianship, and cybercrime victimization among European citizens are described below.

First, Riek, Bohme, and Moore (2015) found that perceived cybercrime risk decreases the likelihood of online activities (e.g., online shopping, banking, emails, social networking). Similar to the work of Riek and colleagues (2015), these two hypotheses test the associations between perceived risk of cyber-threat, online routine activity, and digital capable guardianship.

Research question [Q4]*:* Is there a relationship between online routine activity, digital capable guardianship, perceived risk of cyber-threat, and cybercrime victimization?

Hypothesis [H10]: Perceived risk of cyber-threat is negatively associated with online routine activity.

Hypothesis [H11]: Perceived risk of cyber-threat is positively associated with digital capable guardianship (avoidance personal guardianship and passive physical guardianship).

Hypothesis [H12]: Perceived risk of cyber-threat is negatively associated with cybercrime victimization.

Hypothesis [H13]: Online routine activity is positively associated with cybercrime victimization.

Hypothesis [H14]: Digital capable guardianship (avoidance personal guardianship and passive physical guardianship) is negatively associated with cybercrime victimization.

Lastly, the final hypothesis in this chapter tests the mediation effect of perceived risk of cyber-threat on cybercrime victimization through online routine activity and digital capable guardianship.

Research question [Q5]*:* Is the relationship between perceived risk of cyber-threat and cybercrime victimization mediated by online routine activity or digital capable guardianship?

Hypothesis [H15]: Online routine activity and digital capable guardianship mediate the relationship between perceived risk of cyber-threat and cybercrime victimization.

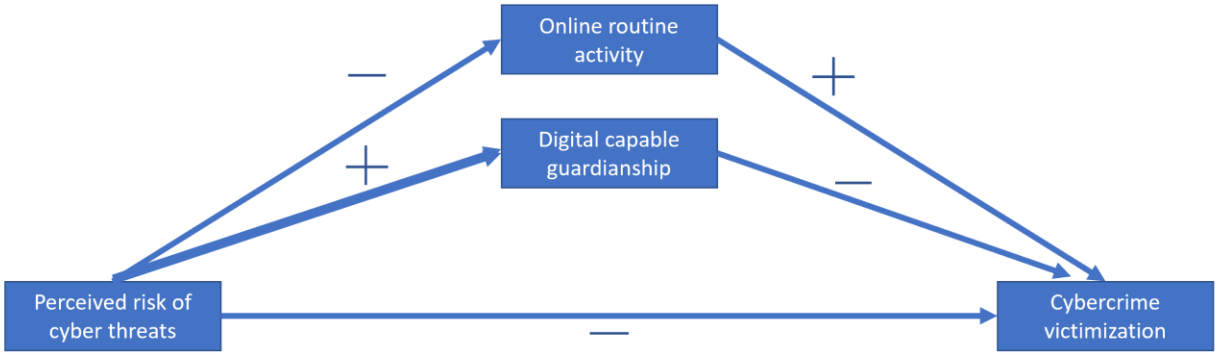


Figure 4. Mediation Effects

Methodology

Data. Data used in this study was derived from the Special Eurobarometer Surveys, which were conducted from 2012 through 2014. The Eurobarometer series is a cross-national survey program conducted on behalf of the European Commission. The main purpose of the Eurobarometer survey is to monitor public opinion in the European Union (EU) member countries. The Eurobarometer consists of standard modules and special topic modules. The special topic modules include Quality of Transport, Cyber Security, Value Added Tax, and Public Health. Regarding the topic of cybersecurity, citizens in the European countries were asked their views concerning risks of cybercrime, respondents' use of the internet, how cybersecurity concerns have altered respondents' online behavior, prevention of online harassment of household children, and concern about and experience with being victims of cybercrime. In addition, demographic and other background information (i.e., age, gender, nationality, marital status, occupation, political preference, education, household composition, ownership of a fixed or mobile telephone and other goods, and Internet use) were collected.

Face-to-face survey interviews were implemented in participant's homes in the appropriate national language. Also, Computer Assisted Personal Interview (CAPI) was utilized in those countries where this technique was applicable. The process of data collections has been sequentially carried out by different sample populations in the European Union member countries. First, the data collection of Eurobarometer 77.2: Economic and Financial Crisis, Helplines for Social Services, Railway Competition, Food Production and Quality, and Cyber Security, March 2012 was conducted for 26,593 respondents (the 27 nationalities of the European Union) aged 15 and over between March

10-25, 2012 (67.4% response rate). Second, the data collection of Eurobarometer 79.4: Economic and Financial Crisis, Helplines for Social Services, Railway Competition, Food Production and Quality, and Cyber Security, May-June 2013 was executed for 27,680 respondents aged 15 and over between May and June 2013 (67.5% response rate). Third, the data collection of Eurobarometer 82.2: Economic and Financial Crisis, Helplines for Social Services, Railway Competition, Food Production and Quality, and Cyber Security, October 2014 was executed for 27,868 respondents (the 28 nationalities of the European Union) aged 15 and over between October 11-20, 2014 (70.5% response rate). Using listwise deletion, all cases with missing values are dropped from the analysis. To that end, a sample of 51,407 was utilized in this study in order to maintain the consistency of using exact same question items for independent and dependent variables from 2012 to 2014.

Measures. According to Haynes and Giblin (2014), some researchers apply factor analysis to decrease the number of survey items to a single causal factor (e.g., Pelfrey, 2007), or sum the survey items into a single additive index (e.g., Burruss, Giblin, & Schafer, 2010; Randol, 2012). While the current study employs a single additive index to create a dependent variable, factor analysis is applied for creating independent variables.

Dependent variable. A dependent variable for cybercrime victimization was created through adding five survey items. The experience of cybercrime was measured by asking the question: "How often have you experienced or been a victim of the following cybercrime types in the past year?" To answer the question, respondents chose from the following lists: 1) identity theft, 2) fraudulent e-mail, 3) purchase fraud, 4) extremist materials, and 5) cyberattacks. In the present study, survey responses for each of the five

items were coded (0 indicating *never*; 1 indicating *occasionally*; 2 indicating *often*) and summed into an index ranging from 0 to 10 ($\alpha = .64$).

Independent variables. Eighteen survey items were gathered to measure five aspects of the online users' behaviors and perception, including perceived risk of cyber-threat, online exposure, and cybersecurity actions. A series of factor analyses, specifically principal components extraction with varimax rotation, was employed to reduce the number of survey items into each component without significant loss of items (see Table 11). Rather than enter all 18 items simultaneously, items were entered into individual analyses based on Cronbach's Alpha reliability tests and empirical literature (Back, Sung, & LaPrade, 2017; Engel, de Vasconcelos, & Zannin, 2014; Haynes & Giblin, 2014; Monyai, Lesaoana, Darikwa, & Nyamugure, 2016).

Perceived risk of cyber-threat. Survey respondents were asked: "How concerned are you personally about experiencing or being a victim of the following cybercrimes?" Responses to six items, each reflecting a different type of cybercrime (identity theft, fraudulent e-mail, purchase fraud, child pornography, extremist materials, cyberattacks), were scored on a scale (1 indicating *not at all concerned*; 2 indicating *not very concerned*; 3 indicating *fairly concerned*; 4 indicating *very concerned*). The scores created a single perceived risk component accounting for 70% of the variance in the indicators ($\alpha = .91$) which means that 70% variance will be explained by the other factor.

Online routine activity. Online routine activity was measured as the second component. Online exposure is captured using measures derived from Holt and Bossler (2013), Reyns and Henson (2016), Choi and Lee (2017). Respondents were asked: "Which of the following activities do you do online?" The routine online activities include online

banking, online purchase, online selling, using social networking sites, and using email. Original survey responses were dichotomously coded (0 indicating no; 1 indicating yes). The scores provided a single online routine activity component accounting for 38% of the variance in the indicators ($\alpha = .59$) which means that 38% variance will be explained by the other factor.

Avoidance personal guardianship. Consistent with Williams' (2016) definition, "avoidance personal guardianship" was assessed with 2 survey items. Respondents were asked: "Has concern about cyber-threat issues made you less likely to engage in online purchases?" and "Has concern about cyber-threat issues made you less likely to engage in online banking?" Responses were dichotomously coded (0 indicating no; 1 indicating yes). A correlation matrix indicates that there is an association between these two items ($r = 0.42$, $p < .001$). The scores established a single additive component accounting for 65% of the variance which means that 65% variance will be explained by the other factor.

Passive physical guardianship. Passive physical guardianship consists of target hardening efforts (e.g., anti-virus software execution, using only one computer, using spam filtering system), which can reduce the likelihood of a cybercriminal event occurring (Bossler & Holt, 2009; Choi, 2008; Choi & Lee, 2017; Choi, Scott, & LeClair, 2016; Holt & Bossler, 2008; Reyns et al., 2011; Ngo & Paternoster, 2011; Williams, 2016). Respondents were asked: "Has concern about cyber-threat issues made you only visit websites you know and trust?," "Has concern about cyber-threat issues made you not open emails from people you don't know?," "Has concern about cyber-threat issues made you only use your own computer?," and "Has concern about cyber-threat issues made you install anti-virus software?" Responses were dichotomously coded (0 indicating no; 1

indicating yes). The scores provided a single passive physical guardianship component accounting for 46% of the variance in the indicators (α = .61) which means that 46% variance will be explained by the other factor.

Control variables. Control variables in this study include two demographic background variables: gender (0 = female, 1= male) and age (ranged from 15 to 99).

Table 10. Descriptive Statistics (N = 51407)

Variables	Mean	SD	Min	Max
Dependent Variable: *Cybercrime Victimization*	.90	1.87	0	10
Items for variables				
Identity theft experience	.07	.29	0	2
Fraudulent email experience	.40	.62	0	2
Purchase fraud experience	.11	.35	0	2
Extremist materials experience	.17	.43	0	2
Cyberattacks experience	.15	.38	0	2
Perceived risk: Identity theft	2.71	.97	1	4
Perceived risk: Fraudulent email	2.49	.97	1	4
Perceived risk: Purchase fraud	2.46	.96	1	4
Perceived risk: Child pornography	2.50	1.07	1	4
Perceived risk: Extremist materials	2.29	.98	1	4
Perceived risk: Cyberattacks	2.42	.95	1	4
Online activity: Online banking	.57	.49	0	1
Online activity: Online purchase	.52	.50	0	1
Online activity: Online selling	.19	.38	0	1
Online activity: Social network	.57	.49	0	1
Online activity: Email	.86	.35	0	1
Digital guardian 1: Less online purchase	.16	.36	0	1
Digital guardian 1: Less online banking	.12	.33	0	1
Digital guardian 2: Only trusted websites	.36	.47	0	1
Digital guardian 2: Reject unknown email	.47	.49	0	1
Digital guardian 2: Only use own computer	.34	.47	0	1
Digital guardian 2: Anti-virus	.55	.49	0	1
Control Variables				
Gender	.47	.49	0	1
Age	42.92	16.10	15	99

Table 11. Four-Factor Analysis Solutions with Indicators

Analysis	Components	Indicators	Cronbach's Alpha reliability	Factor loadings	Percent of variance explained by factor
1	Perceived risk of cyber-threat	Level of concern for (1) identity theft, (2) fraudulent emails, (3) online fraud for purchase, (4) child pornography, (5) extremist material, and (6) cyberattack	.91	.70-.80	70.07
2	Online exposure	Online backing, online purchase, online selling, using social networking sites, and using email	.59	.60-.80	38.60
3	Avoidance personal guardianship	Less likely to buy goods online, less likely to bank online	.50	.80-.90	65.91
4	Passive physical guardianship	Only visit websites you know and trust, do not open emails from people you don't know, only use your computer, have installed anti-virus software	.61	.60-.75	46.13

Analytic Method. All models were estimated using SPSS 23. First, a correlation matrix was provided to show bivariate relationships between variables. Second, a series of Ordinary Least Squares (OLS) regressions were employed in order to test hypothesis 10-15 concerning the association between perceived risk of cyber-threat, online routine activity, and digital capable guardianship (avoidance personal guardianship and passive physical guardianship). The OLS regression models were suitable to analyze this data since the relationship between the independent variables and dependent variable were linear. The Shapiro-Wilk test and Kolmogorov-Smirnov Test (K-S Test) determined that the dependent variable (see Flatt & Jacobs, 2019) was normally distributed (Shapiro-Wilk test: $p > .05$; 1-Sample Kolmogorov-Smirnov Test: $p > .05$). In addition, all the tolerance values are over .20 and all the VIF statistics are less than 10; therefore, there is no problem for multicollinearity among variables. The analyses began with a bivariate regression where perceived risk of cyber-threat is modeled as the sole predictor of cybercrime victimization in order to obtain a baseline association. Next, demographic variables (i.e., gender and age) were added to the OLS regression model. Also, online exposure and cybersecurity action 1 and 2 variables were added to the model.

To measure meditation effects between perceived risk of cyber-threat, avoidance personal guardianship and passive physical guardianship, and cybercrime victimization, the Process macro for SPSS developed by Hayes (2017) was employed. The analysis proceeds in a series of steps for mediation testing. As the first step, this analysis starts with establishing a baseline model determining the direct effects of the independent variables (e.g., perceived risk of cyber-threat) on cybercrime victimization. The second step included estimating the direct effects of the perceived risk of cyber-threat on three mediators (e.g.,

online routine activity, avoidance personal guardianship, and passive physical guardianship) respectively. In the third step, three mediators were added as a full model to estimate both the direct effects on cybercrime victimization and the mediating effects on the relationship between the perceived risk of cyber-threat and cybercrime victimization. The results of the OLS regression models via Process macro are displayed in Table 14, 15, and 16.

Results

Bivariate Relationships. Table 12 shows the bivariate correlations of the study variables. Perceived risk of cyber-threat and online routine activity had positive relationships with cybercrime victimization. Other independent variables (i.e., avoidance personal guardianship, passive physical guardianship, and gender) were positively, though weakly, correlated with cybercrime victimization, whereas age was negatively correlated with cybercrime victimization. Overall, in Table 12, the independent variables were small effects on the dependent variable. However, as the concept of substantive significance, when considering the very large amount of sample size (N = 51,407) in this study, it was meaningful to explain the likelihood of cybercrime victimization by using these five independent variables. Additionally, small effects may also be considered meaningful if they trigger big consequences, if they change the perceived probability that larger outcomes might occur, or they accumulate into larger effects (Lewis-Beck, Bryman, & Liao, 2003; Ellis, 2010).

Table 12. Correlations of the Study Variables

	1	2	3	4	5	6	7
1. Cybercrime Victimization	1						
2. Perceived risk of cyber-threat	.140**	1					
3. Online routine activity	.197**	-.037**	1				
4. Avoidance personal guardianship (APG)	.034**	.133**	-.178**	1			
5. Passive physical guardianship	.034**	.080**	.238**	.057**	1		
6. Gender	.066**	-.088**	.021**	-.016**	-.024**	1	
7. Age	-.095**	-.086**	-.093**	.019**	.121**	.022**	1

Note: **$p < .01$

Regression Analyses. Table 13 presents the results of the series of ordinary least squares (OLS) hierarchical regressions and mediation analyses conducted in order to investigate the hypotheses. Model 1 indicates that there is a statistically significant, positive relationship between perceived risk of cyber-threat and cybercrime victimization ($b = .20$, SE = .001, $\beta = .14$, $p < .001$).This finding indicates that individuals with higher perceived risk of cyber-threat are more likely to experience cybercrime victimization which is the opposite of the predicted direction of hypothesis 12. Model 2 adds the demographic variables to account for differences in gender and age. As shown, gender ($b = .22$, SE = .012, $\beta = .08$, $p < .001$) and age ($b = -.01$, SE = .001, $\beta = -.09$, $p < .001$) variables are respectively

significant; moreover, the effect of perceived risk of cyber-threat was statistically unchanged (b = .20, SE = .001, β = .14, p < .001). These results reveal that male individuals were more likely to experience cybercrime victimization than females. Older individuals were less likely to experience cybercrime victimization.

Table 13. Ordinary Least Squares Results of Predicting Cybercrime Victimization (N = 51407)

	Model 1		Model 2		Model 3	
Variables	*b*	SE	*b*	SE	*b*	SE
Perceived risk	.20***	.001	.20***	.001	.20***	.001
Online routine activity					.29***	.004
Avoidance personal guardianship					.08***	.005
Passive physical guardianship					-.03***	.011
Gender			.22***	.012	.21***	.012
Age			-.01***	.001	-.01***	.001
$\mathbf{R^2}$	.020		.033		.074	

Note: ***p < .001

As predicted, Model 3 shows that greater online routine activity was positively associated with cybercrime victimization, while passive physical guardianship was negatively associated with cybercrime victimization. Specifically, individuals with higher levels of online routine activity were more likely to experience cybercrime victimization

(*b* = .29, *SE* = .004, β = .21, *p* < .001); individuals with a higher level of passive physical guardianship were less likely to experience cybercrime victimization (*b* = -.03, *SE* = .011, β = -.12, *p* < .001). Interestingly, avoidance personal guardianship was significant, but the sign was in the direction opposite to what was hypothesized; individuals with a higher level of avoidance personal guardianship were more likely to experience cybercrime victimization (*b* = .08, *SE* = .005, β = .05, *p* < .001).

Table 14. Testing for online routine activity as a mediator between perceived risk of cyber-threat and cybercrime victimization

Steps in testing for mediation	***b***	**SE**	**95% CI**	**β**
Testing Step 1 (Path c)				
Outcome: cybercrime victimization				
Predictor: perceived risk	.19***	.006	.18, .20	.14
Testing Step 2 (Path a)				
Outcome: online exposure				
Predictor: perceived risk	-.03***	.004	-.04, -.02	-.03
Testing Step 3 (Paths b and c')				
Outcome: cybercrime victimization				
Mediator: online routine activity (Path b)	.27***	.005	.26, .28	.20
Predictor: perceived risk (Path c')	.20***	.005	.19, .21	.14

Note:

***$p < .001$

Mediation Effects. Table 14 contains the analyses to investigate the mediation hypothesis. Perceived risk of cyber-threat was significantly associated with cybercrime victimization (b = .19, β = .14, p < .001), path c was significant and the requirement for mediation in Step 1 was met. In Step 2, perceived risk of cyber-threat was also significantly associated with online routine activity (b = -.03, β = -.03, p < .001); therefore, the condition for Step 2 was met (Path a was significant).

To test whether the hypothesized mediator, online exposure, was related to the outcome, cybercrime victimization was regressed simultaneously on both perceived risk of cyber-threat and online routine activity (Step 3). Step 3 of the mediation process showed that the mediator (online routine activity) was significantly associated with cybercrime victimization controlling for perceived risk (b = .27, β = .20, p < .001). Path b was significant and the condition for Step 3 was met. When path c' is zero or lessened, there is evidence for complete mediation. However, path c' was still significant, and it was larger than path c (b = .20, β = .14, p < .001). As such, online routine activity did not mediate the relationship between perceived risk and cybercrime victimization.

Table 15 presents the analyses of the mediation effect between avoidance personal guardianship, perceived risk of cyber-threats, and cybercrime victimization. Perceived risk of cyber-threats was significantly associated with cybercrime victimization (b = .19, β = .14, p < .001), path c was significant and the requirement for mediation in Step 1 was met. In Step 2, perceived risk of cyber-threat was also significantly associated with avoidance personal guardianship (b = .13, β = .13, p < .001), and thus the condition for Step 2 was met (Path a was significant).

Table 15. Testing for avoidance personal guardianship as a mediator between perceived risk of cyber-threat and cybercrime victimization

Steps in testing for mediation	***b***	**SE**	**95% CI**	**β**
Testing Step 1 (Path c)				
Outcome: cybercrime victimization				
Predictor: perceived risk	.19***	.006	.18, .20	.14
Testing Step 2 (Path a)				
Outcome: avoidance personal guardianship				
Predictor: perceived risk	.13***	.004	.12, .14	.13
Testing Step 3 (Paths b and c')				
Outcome: cybercrime victimization				
Mediator: avoidance personal guardianship (Path b)	.02***	.006	.01, .03	.01
Predictor: perceived risk (Path c')	.19 ***	.006	.17, .20	.14

Note:

***$p < .001$

To test whether the hypothesized mediator, avoidance personal guardianship, was related to the outcome, cybercrime victimization was regressed simultaneously on both avoidance personal guardianship and perceived risk of cyber-threat (Step3). Avoidance personal guardianship was significantly associated with cybercrime victimization controlling for perceived risk of cyber-threat ($b = .02$, $\beta = .01$, $p < .001$). Thus, path b was significant and the condition for Step 3 was met. When path c' was zero or lessened, we have evidence for complete mediation. Path c' was still significant, also it was same as path

c (b = .19, β = .14, p < .001). In short, avoidance personal guardianship did not mediate the relationship between perceived risk of cyber-threat and cybercrime victimization.

Table 16. Testing for passive physical guardianship as a mediator between perceived risk of cyber-threat and cybercrime victimization

Steps in testing for mediation	***B***	**SE**	**95% CI**	**β**
Testing Step 1 (Path c)				
Outcome: cybercrime victimization				
Predictor: perceived risk	.19***	.006	.18, .20	.14
Testing Step 2 (Path a)				
Outcome: passive physical guardianship				
Predictor: perceived risk	.07*	.004	.07, .08	.07
Testing Step 3 (Paths b and c')				
Outcome: cybercrime victimization				
Mediator: passive physical guardianship (Path b)	-.03***	.006	.02, .04	.02
Predictor: perceived risk (Path c')	.18 ***	.006	.17, .20	.13

Note:

*p < .05, **p < .01, ***p < .001

Table 16 contains the analyses to examine the mediation hypothesis for perceived risk of cyber-threat, which was significantly associated with cybercrime victimization (b = .19, β = .14, p < .001), path c was significant and the requirement for mediation in Step 1 was met. As Step 2, perceived risk of cyber-threat was also significantly associated with passive physical guardianship (b = .07, β = .07, p < .001), and thus the condition for Step 2 was met (Path a was significant). To test whether the hypothesized mediator, passive physical guardianship, was related to the outcome, cybercrime victimization was regressed

simultaneously on passive physical guardianship and perceived risk of cyber-threat (Step 3). Passive physical guardianship was significantly and negatively associated with cybercrime victimization controlling for perceived risk of cyber-threat (b = -.03, β = .02, p < .001). Therefore, path b was significant and condition for Step 3 was met. When path c' was zero or lessened, there was evidence for complete mediation. Path c' was still significant, but it was smaller than path c (b = .18, β = .13, p < .001). As such, passive physical guardianship did partially mediate the relationship between perceived risk of cyber-threat and cybercrime victimization. This means that perceived risk of cyber-threat increased the mediator (passive physical guardianship), and the mediator was in turn 4% more likely to reduce cybercrime victimization. While the findings indicate that the effect was partially mediated, it still remains the case that the association between perceived risk and victimization was positive, which was opposite to what was hypothesized.

Discussion and Conclusion

Despite a large body of literature that has estimated direct effects of digital capable guardianship (e.g., Choi, 2008; Choi & Lee, 2017; Williams, 2016; Back, 2016) and online routine activity (e.g., Al-Nemrat, Jahankhani, & Preston, 2010; Bossler & Holt, 2009; Holtfreter, Reisig, & Pratt, 2008; Hutchings & Hayes, 2009; Marcum, Higgins, & Ricketts ,2010; Pratt et. al, 2010; Pyrooz, Decker, & Moule, 2015; Reyns, 2013; Reyns, 2015; Reyns & Henson, 2016; Williams, 2016; Wolfe et al., 2016) on cybercrime victimization, few studies have empirically examined this association through perceived risk of cyber-threat for mediation effects. Thus, first, the present study contributes to the literature revealing the associations between perceived risk of cyber-threat, online routine activity, avoidance personal guardianship, passive physical guardianship, and cybercrime

victimization. Further, it sought to determine whether online routine activity, avoidance personal guardianship, and passive physical guardianship would fully or partially mediate the impact of perceived risk of cyber-threat on cybercrime victimization. The findings of this study provide support for the theoretical explanation of the crime triangle framework to illustrate cybercrime victimization risk. In this section, the results suggest implications for theory and practice as well as important directions of future criminological research.

The main findings of this study support the extension of the crime triangle framework to the context of cybercrime victimization. In terms of capable guardianship, first, passive physical guardianship was negatively associated with cybercrime victimization. It means that individuals with higher level of passive physical guardianship are less likely to experience cybercrime victimization. This finding is consistent with what Back (2016), Choi (2008), Choi and Lee (2017), and Williams (2016) reported. Second, the study showed that online routine activity was positively associated with cybercrime victimization. To do this, individuals who are with higher level of online exposure are more likely to experience cybercrime victimization. This finding is also consistent with what several researchers (Back 2016; Bossler & Holt, 2009; Choi, 2008; Choi & Lee, 2017; Holtfreter et al, 2008; Marcum et al., 2010; Pratt et al., 2010; Reyns, 2013) have reported. Third, similar to the results of Williams' (2016) study, avoidance personal guardianship was positively associated with cybercrime victimization which was the unpredicted direction of hypothesis 14. Fourth, the results indicate that perceived risk of cyber-threat is positively associated with cybercrime victimization which is the unpredicted direction of hypothesis 12, though it is consistent with what Renys (2013) reported. In line with previous research's findings for demographic profiles of cybercrime victims (e.g.,

Holtfreter, Reisig, & Pratt, 2008), these results also found that individuals who were female and older are less likely to experience cybercrime victimization.

Further, with respect to mediation effects, the results in this study provide evidence that passive physical guardianship has a mediation effect on the relationship between pereived risk of cyber-threat and cybercrime victimization; however, online routine activity and avoidance personal guardianship did not mediate the relationship between perceived risk of cyber-threat and cybercrime victimzation. There is a possible explanation as to why the passive physical guardianship had mediating effects. Higher perceived risk of cyber-threat reinforces the passive physical guardianship, and the higher passive physcial guardianship is in turn reducing the likelihood of cybercrime victimization. Overall, the main results hightlight that strong passive physical guardianship (e.g., installing/operating anti-virus software, avoiding to visit untrustful websites) is a key factor to efficiently protect online users against cybercriminals. Lastly, as stated above, there is no study to empirically test the mediating effect of percieved risk of cyber-threat on cybercrime victimization through capable guardianship; therefore, this study contributes to the existing literaure in cybercriminology and victimology.

Policy Implications. The findings of this study provide significant implications for practice. From a policy and practice standpoint, the findings of this study in table 12 and 13 point out the importance of efforts to reduce the potential for cybercrime victimization through reinforcing the level of passive physical guardianship. In fact, individuals' protective behaviors (e.g., using only their own computer, email spam filtering, running anti-virus and secure browsing) appear to be able to reduce the likelihood of cybercrime victimization. Holt, Lee, Liggett, Holt, and Bossler (2019) claim that training

programs can also effectively improve the importance of cybersecurity awareness in which it increases individuals' competence and preparation to prevent cybercrime rather than experience crime victimization. For instance, the City of London Police have had success by implementing the Economic Crime Academy Training series which trained stakeholders in the typology of the cybercrime, cybercriminals' behavior and victim response in a way that efficiently reduced their victimization experiences online (Levi, Doig, Gundur, Wall, & Williams, 2016). Similarly, according to Cyber-Digital Task Force Report provided by the U.S. Department of Justice (U.S. DOJ, 2018), DOJ attempts to help victims of cybercrime dampen the effects of exploitation and speed their recovery though building relationships and sharing cyber threat information with private and public sectors. For example, the FBI disseminates numerous reports geared directly to the private sector regarding ongoing or emerging domestic- and international level cyber threats. Recently, the FBI hosted workshops targeting multiple levels of stakeholders in collaboration with the Department of Homeland Security, the United States Secret Service, Healthcare and High-Risk Security Services, and the National Council of ISACs to implement a ransomware campaign which educated over 5,700 individuals about one of the emerging cyber threats, ransomware. As such, the dissemination of cybersecurity awareness can effectively reinforce individuals' protective behaviors for the online domain which may help defend themselves against sophisticated cyber threats.

Limitations. There are several limitations of this study in this chapter that must be discussed. First, although a series of cross-sectional datasets (2012, 2013, 2014) were utilized in this study, and thus, the findings provided correlations between perceived risk of cyber-threat, online activity, guardianships, and cybercrime victimization, it was unable

to reveal the time-ordering of causal effects. Bivariate relationships can exist between dependent variable and independent variables. For example, individuals who experience cybercrime victimization may be more likely to have higher level of perceived risk of cyber-threat or individuals who experiene cybercrime victimization may be less likely to engage in online activity. For future study, it will be beneficial to use panel data to better establish proper temporal order between perecived risk of cyber-threats, online activity, guardianship, and cybercrime victimization.

Second, although the current study has attempted to explain how perceived risk, online routine, capable guardianship would act as preventative predictors on cybercrime victimization, there were some measurement issues such as the low value of Cronbach's Alpha reliability and variations for principle components extraction. It is possible that the low alpha value occurred due to a low number of items for variables and the poor inter-relatedness between items of heterogeneous constructs. Another measurement issue is related to construct validity. The current study utilized online routine activity (e.g., online banking/shopping/selling/using SNSs) to explain how online exposure influence the likelihood of cybercrime victimization. However, it was limited to test the validity of the criminological theory (e.g., individuals who engage in risky online lifestyle are more likley to experience cybercrime victimization than individuals who engage in ordinary online lifestyle such as online banking and online shopping). Lastly, omitted-variable bias might occur in this study. The survey items utilized for creating variables in this study were somewhat changed at three consecutive time points (i.e., 2012, 2013, 2014). To that end, the statistical models leave out some relevant variables (e.g., active personal guardianship – changing security settings and use different passwords for different sites); thus, it may

result in the model attributing the effect of the missing variable to the estimated effects of the included variables (Riegg, 2008).

Future studies should seek to improve upon the measurement issues stated above to increase the vailidity of research. In addition, further research is needed to expand the application of risky online lifestyles element to cybercrime victimization and more specific measures of mediation effects for perceived risk of cybercrime and protective actions on cybercrime victimizaiton.

CHAPTER 5

CYBER PLACE MANAGEMENT: THE EFFECTIVENESS OF CYBERSECURITY AWARENESS TRAINING AGAINST A PHISHING CAMPAIGN

Recently, criminologists and crime prevention practitioners have recognized the importance of place to criminal activities and found that place management can effectively prevent potential crime events. For example, several studies demonstrate that increasing place manager awareness and involvement in or near bars can play a critical role in preventing drug and violence related crimes (Mandensen, 2007). In a systematic review of place-focused interventions, Eck (2002) concludes that interventions by owners of apartment buildings to deal with drug selling on their properties had positive results. In a broad sense, researchers (e.g., Block & Block, 1995; Clarke, 1997; Danner, 2003; Eck & Weisburd, 2015; Felson, 1995; Mazerolle, Kadleck, & Roehl, 1998; Mazerolle & Roehl, 1998; Sherman, 1995) suggest that a lack of active place management can facilitate crime (Mandensen, 2007).

Likewise, in the cyber world, place managers (e.g., information security officials) are key personnel in the implementation of cybercrime control strategies. In particular, through the management of accurate cybersecurity settings, the guiding of online users' behavior, or enforcing cybersecurity regulation, they can create a cybercrime-free environment for their institutions (Cavusoglu, Cavusoglu, Son, & Benbasat, 2009). Place managers (e.g., information security officials) can also implement security awareness programs in their institutions, which can enhance online users' protection. In addition, cybersecurity managers can facilitate the minimization of losses in these organizations and

mitigate any vulnerabilities, which can help entities increase the resiliency level of the emergency response to future cyber threats.

To that end, a large body of work (e.g., Block & Block, 1995; Clarke, 1997; Danner, 2003; Eck, 2002; Eck & Weisburd, 2015; Felson, 1995; Mazerolle, Kadleck, & Roehl, 1998; Mandensen, 2007; Sherman, 1995) has highlighted the significance of physical place and neighborhood, which has influenced criminal activities over the past several decades. Nevertheless, there has been a paucity of research evaluating virtual place management strategies and addressing cyber incident response tactics. Thus, this chapter seeks to investigate the effectiveness of the application of place management on crime prevention in an online setting. The next sections will discuss background, the research question, hypothesis, methods used, the variables included in the analysis and their operationalization criteria, and the major findings.

Background

Research on Cybersecurity Awareness Programs. Cybersecurity awareness program evaluations are important for assessing the effectiveness of and weaknesses in existing awareness programs in the chosen strategy and methods (Rantos, Fysarakis, & Manifavas., 2012). First, previous research (see Kritzinger & von Solms, 2010; Labuschagne, Burke, Veerasamy, & Eloff, 2011; Rantos et al., 2012; Rezgui & Marks, 2008; Pastor, Diaz, & Castro, 2010) regarding cybersecurity awareness programs has focused on demonstrating a conceptualized framework of cybersecurity awareness programs. For example, Rantos, Fysarakis, and Manifavas (2012) proposed an evaluation framework to assess cybersecurity awareness programs. This evaluation methodology includes the evaluation of user cybersecurity awareness and cybersecurity management.

The work of Labuschagne and colleagues (2011) proposed an interactive game hosted by social media sites in order to increase users' cybersecurity awareness level. They explained this training platform includes game-based applications such as hypermedia, multimedia, and hypertext in order to improve the effectiveness of online cybersecurity awareness programs.

Several studies have investigated the relationships between perception of risk for cybercrime, computer self-efficacy, attitude to cybersecurity, and the awareness of cybersecurity training. Generally, research found support (Kim, 2013; Mani, Choo, & Mubarak, 2014; Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2014; Ryan, 2007; Slusky & Partow-Navid, 2012) that the perceived risk of cyber-threats, computer self-efficacy, and personal innovation measures are positively associated with the awareness of information security practices. In an information security awareness evaluation study, Ryan (2007) pointed out that individuals with a higher level of personal innovation and computer self-efficacy were more likely to have a higher level of information security awareness.

Next, a large body of research has tested whether cybersecurity awareness programs are effective enough to make people aware of their roles, vulnerability, and cyber threats. Previous studies have examined the effectiveness of various platforms of cybersecurity awareness programs (e.g., web-based training, brochures and company magazine, posters, emails, interactive video games, puzzles). To measure effectiveness, several types of methods (interview, self-report survey, pre- and post- experimental study, vocabulary test, game tool, clicking on the phishing link) have been utilized. Most studies (e.g., Albrechtsen, 2007; Ariyapperuma & Minhas, 2005; Charoen, Raman, & Olfman,

2008; Chen, Shaw, & Yang, 2006; Cone, Irvine, Thompson, & Nguyen, 2007; Dasgupta, Ferebee, & Michalewicz, 2013; Denning, Lerner, Shostack, & Kohno, 2013; Drevin, Kruger, & Steyn, 2007; Furnell et al., 2010; Hagen, Albrechtsen, & Ole Johnsen, 2011; Talib, Clarke, Furnell, 2010) have found that the existing cybersecurity awareness programs have effectively increased user cybersecurity awareness. For example, the work of Charoen, Raman, and Olfman (2008) tested the issues inherent in password management and revealed that a cybersecurity training program helped to improve system user's behavior relevant to password management. Interestingly, Chen, Shaw, and Yang (2006) evaluated whether online users from the U.S. and Taiwan who received information security training in off-line and online platforms show different levels of cybersecurity awareness. The results in Chen and colleagues' (2006) study found that these training programs were effective to American users who received these training, whereas the programs did not have any impact on Taiwanese users who received this training. In addition, several scholars contend that traditional security awareness platforms such as classroom-based teaching, online education and poster/email campaigns are not effective in enforcing users' information security awareness or practice. Cone and colleagues (2007) and Foreman (2004) asserted that interactive computer-based training (e.g., video games) are powerful teaching tools for effective cybersecurity awareness training.

Cyber Awareness Programs. Previous studies have found that place managers build crime-free environments in certain locations by enforcing rules of conduct, acting as guardians, or providing employees and students with crime intervention training programs. Cybersecurity awareness or information security awareness programs are designed to train individuals regarding safety precautions and online defense methods (e.g., protecting

existing resources [Banerjee, Cronan, & Jones, 1998; Denning, 1999; Halibozek & Kovacich, 20017; Rezgui & Marks, 2008; Zegiorgis, 2002]). Drevin, Kruger, and Steyn (2007) explicated that cybersecurity awareness can assist in decreasing human error, identity theft, internet fraud, and misuse of digital assets. Given the importance of cybersecurity awareness, relevant training programs are considered as a vital prevention strategy to inspire, stimulate, establish, and rebuild information security capabilities for online users as a method of cyber place management (Dlamini & Modise, 2013).

In the last two decades, cybersecurity or information security awareness training programs have been implemented in academia, and private and public sectors. In order to create efficient cybersecurity awareness programs, these stakeholders (academia, private and public sectors) have had interdisciplinary approaches to develop various learning platforms such as off- and on-line training sessions, email messages, video games, intranet-based access, and poster campaigns. These cybersecurity awareness programs educate targeted audiences about up-to-date cyber threats and good cybersecurity practices (Piazza, 2006; Rezgui & Marks, 2008; Rantos, Fysarakis, & Manifavas, 2012).

In alignment with the trends of security education among universities, FIU's Division of Information Technology (DIT) initiated a *Cybersecurity Awareness Training* program aimed at enhancing the university community's awareness of protecting its data and facilities from cyber adversaries. The purpose of this cybersecurity awareness program is to enhance the awareness level of cyber threats as well as provide FIU's employees self-protection knowledge against potential cyber-threats. The FIU cybersecurity awareness training program is an online-based course. Online learning has several distinct advantages such as extendibility, accessibility, and suitability (Bonk, 2002; Habibi & colleagues, 2018;

James, 2002). For instance, online users can proceed through an online training at their own pace/place and access the training at any time. Also, online learning platform can save travel cost and time because learners directly received training materials through Web browsers and Internet connections instead of the other way around.

Given the significance of its purpose and convenience, this online cybercrime prevention program is in collaboration with the U.S. Department of Homeland Security and the U.S. National Cyber Security Alliance. In order to help the University community identify and prevent the loss of sensitive data and protect existing resources, FIU requires all FIU employees to take the training within 3 months of assignment. Specifically, the FIU's DIT provides this online training program to FIU employees with the option to complete a pretest for 18 Cybersecurity Core Knowledge modules or FIU employee can watch the video lectures for each module and complete the corresponding module quizzes (Awareness Training, 2019). The total view time for the cybersecurity awareness training is 1 hour and 10 minutes but the training ought not to be completed in one sitting. The topics of these training modules include social engineering, email and phishing, browsing safety, social networks, mobile devices, passwords, data security, hacking, targeted attacks, and malware. FIU is the fourth-largest university in the United States with 55,112 students and 2,900 faculty members (US News, 2019). Considering the tremendous population size and various academic facilities of FIU, the initiative of the cybersecurity awareness program can be a very significant strategy to help one of the biggest universities in the U.S. maintain its assets under cyber-hygiene.

Research Testing Cybersecurity Awareness Programs and Phishing Campaign Tests. Importantly, to date, few studies (Caputo, Pfleeger, Freeman, & Johnson,

2013; Kumaraguru & associates, 2009; Nyeste & Mayhorn, 2010; Sheng et al., 2007) have examined the practical phishing campaign to test online users' vulnerability against cybercrime. Phishing is defined as an act in which fraudulent email or websites or links make targeted online users succumb to a data breach or reveal their personal information, similar to identity theft (Kumarguru et al., 2009). The body of research examining the effectiveness of cybersecurity awareness programs via the application of phishing campaigns tests is mixed. For instance, in an evaluation study of anti-phishing training by Kumarguru et al. (2009), 515 individuals were randomly assigned to three groups (control group, 1st training session group, and 2nd training session group) and all participants received a series of 3 legitimate and 7 phishing campaign emails over the course of 28 days. Similar to Kumarguru et al.'s study, Caputo et al.'s (2014) study empirically investigated whether individuals who received a phishing training program would be less likely to click on spear phishing links as compared to others who were not recipients of the training. Shen et al. (2007) designed a cybersecurity awareness game and tested whether its game was influential in increasing participants' capability in identifying fraudulent web sites after the training. Nyeste and Mayhorn (2010) employed an experimental design study with a treatment group and control group in order to assess the effectiveness of anti-phishing programs.

While three studies (i.e., Kumaraguru et al., 2009; Sheng et al., 2007; Nyeste & Mayhorn, 2010) found that anti-phishing awareness programs were effective in reducing the number of users falling for phishing attacks, the results of Caputo et al.'s (2014) study revealed that phishing training programs did not help the treated group reduce the likelihood of falling for phishing attacks. Therefore, these observations call attention to the

goals of this chapter. The studies by Kumarguru et al., Caputo et al., and Sheng et al. were based on the computer science field of study, whereas Nyeste and Mayhorn's study was relied on the discipline of psychology.

As discussed in the literature review in Chapter 2, the roles of the victim, capable guardians, and place manager are very significant factors to fight against sophisticated cyber offenders. Wortley, Sidebottom, Tiley, and Laycock (2018) pointed out that place managers can play crucial roles in reducing the likelihood that cyber offenders exploit new crime opportunities in online platforms. In line with that, Wortley and colleagues (2018) and Scott et al. (2008) argued that the problem analysis triangle (crime triangle) can provides an efficient framework for enhancing existing approaches to cybercrime prevention. In considering this need, the literature may need to think carefully about the extension of place management theoretical perspective derived from cybercrime triangle framework to cybercrime prevention. Nevertheless, to date, there is no research to devise a comprehensive cybercrime triangle framework, especially with virtual place management. Despite the known implications of cyber place management (i.e., cybersecurity awareness programs) for enhancing online users' capabilities to defend against cyber threats, little attention has been directed at examining the effectiveness of cybersecurity awareness training or phishing awareness training on preventing cybercrime victimization by criminologists. Of these, the current study builds on this small body of research by the extension of crime triangle framework with place management to cyberspace and examining the effectiveness of an existing cybersecurity awareness training program through a criminological framework.

As a cyber place management strategy, currently, FIU cybersecurity online training teaches FIU employees a complicated set of rules for differentiating between safe and unsafe links; moreover, its training educates employees to never click a suspicious link and never give out personal information in response to suspicious requests. The existing literature (e.g., Kumaraguru et al., 2009; Sheng et al., 2007; Nyeste & Mayhorn, 2010; Broadhurst, Skinner, Sifniotis, Matamoros-Macias, & Lpsen, 2018) indicates that individuals who were trained by cybersecurity awareness programs were less likely to fall for phishing attacks. In order to build upon previous research, the current study in this chapter specifically seeks to investigate whether a cyber place management method (i.e., FIU's web-based cybersecurity awareness training program) successfully assists users in not falling prey to a phishing campaign. Similar to the works of Kumarguru et al. (2009) and Caputo et al. (2014), the research question and hypothesis are as the follows:

Research question [Q6]: As a cyber place management strategy, is the cybersecurity awareness training program at question effective in reducing the incidence of cybercrime, including phishing scams?

Hypothesis [H16]: An individual who completed the cybersecurity awareness training is less likely to fall for the phishing campaign trial than someone who did not complete this training.

Methodology

Data. The current study uses data derived from the Division of Information Technology (DIT) at FIU. This data includes 1) whether the FIU employees (i.e., student assistants, temporary non-student workers, staff, administration, faculty, and executives)

fell for the phishing campaign and 2) the FIU employees' status of completing the cybersecurity awareness program. As stated above, the main objective of the FIU's cybersecurity awareness program is to enhance the awareness level of cyber threats and provide FIU employees the self-protection knowledge to defend themselves – and thereby the institution itself – against potential cyber-threats. In October 2018, FIU's DIT launched its online based "Cybersecurity Awareness Training" to assist all FIU faculty and staff identify and prevent the loss of sensitive data.

To evaluate the effectiveness of the cybersecurity awareness program, a quasi-experimental research design was used. According to some scholars (Campbell & Stanley, 2015; Randolph, Falbe, Manuel, & Balloun, 2009; Thyer, 2012), quasi-experimental designs in evaluation are frequently employed in the evaluation of educational programs when random sample selection is not practical or possible. At the start of this study, the FIU's DIT staffs selected one group of the FIU staffs (1000 individuals) who completed the FIU cybersecurity awareness program between October 2018 and April 2019 while the FIU's DIT staffs selected the other group of the FIU staffs (1000 individuals) who did not complete the FIU cybersecurity awareness program from 41 departments or offices across the University. Additionally, the FIU's DIT staffs assigned them into two groups, one trained group comprising 1000 participants who completed the FIU cybersecurity awareness program and one comparison group comprising 1000 participants who did not complete the FIU cybersecurity awareness program (see Table 17).

Table 17. Participants from Each Organization

Organization	Frequency	Percent
1. ACAD PLAN & ACCOUNTABILITY	17	.9
2. ACADEMIC AND CAREER SUCCESS	23	1.2
3. ACADEMIC PROGRAM & PARTNER	9	.4
4. ADVANCEMENT	18	.9
5. ATHLETICS	49	2.5
6. BUSINESS AND FINANCE	27	1.4
7. COLL COMM ARCH & THE ARTS	56	2.8
8. COLL OF ENGINEERING & COMPUT	118	5.9
9. COLL OF NURSING & HLTH SCIENC	30	1.5
10. COLL PUBLIC HEALTH & SW	43	2.2
11. COLLEGE ARTS SCIENCES & EDU	482	24.1
12. COLLEGE OF BUSINESS	70	3.5
13. COLLEGE OF LAW	25	1.3
14. COLLEGE OF MEDICINE	203	10.2
15. CONTROLLERS	1	.1
16. ENROLLMENT SERVICES	30	1.5
17. EXTERNAL RELATIONS	75	3.8
18. FACILITIES	16	.8
19. FIU ONLINE	77	3.9
20. FROST ART MUSEUM	54	2.7
21. GOVERNMENT RELATIONS	3	.2
22. HEALTH CARE NETWORK	2	.1
23. HONORS COLLEGE	1	.1
24. HUMAN RESOURCES	14	.7
25. INFORMATION TECHNOLOGY	7	.4
26. JEWISH MUSEUM OF FLORIDA-FIU	18	.9
27. LIBRARY OPERATIONS	57	2.9
28. OFFICE OF ANALYSIS&INFO MGNT	5	.3
29. OPERATIONS AND SAFETY	37	1.8
30. PRESIDENT OFFICE	6	.3
31. PROVOST & EXEC ACAD AFFAIRS	44	2.2
32. REGIONAL LOC & INSTL DEV	4	.2
33. RESEARCH	20	1.0
34. SCH OF HOSPT & TOURISM MGMT	6	.3
35. SCHOOL INT'L & PUBLIC AFFAIRS	81	4.1
36. STUDENT ACCESS AND SUCCESS	15	.8
37. STUDENT AFFAIRS	72	3.6
38. THE WOLFSONIAN	13	.7
39. UNIVERSITY GRADUATE SCHOOL	141	7.0
40. COMMUNITY ENGAGEMENT	6	.3
41. GENERAL COUNSEL	25	1.3
Total	2000	100.0

All participants received one simulated phishing attempt between May 15 and 21, 2019. The phishing email indicated that they are a support team from “UTSHelp FIU”, which did not officially exist on the FIU internal university listserv. The phishing email announced that someone has attempted to sign into a user’s university web service account,

called MyFIU (see Figure 5). The phishing email recommended users to click an inserted link, sending their personal information (e.g., full name, Panther ID, email address, password, phone number) to UTSHelp FIU. During each trial, FIU security officers recorded clicks on the phishing links.

Measures

Dependent variables. The dependent variable was whether or not the FIU employee experienced a 'fall-for' cybercrime incident –the phishing scams – after completing (or not completing) the "Cybersecurity Awareness Program" provided by FIU's DIT. In this regard, FIU's DIT purposely committed the phishing attacks against the treatment group (who did complete the cybersecurity awareness training course) and the comparison group (who did not complete the cybersecurity awareness training course). Specifically, FIU's DIT distributed phishing campaign emails, which were composed of an illegitimate authority's name (i.e., UTSHelp FIU). Afterwards, FIU's DIT tested whether individuals, in the treatment/comparison groups, fell victim to these phishing scams. Three dependent variables are measured using dummy variables: opened email (1 = opened email, 0 = otherwise), clicked the inserted fraudulent link (1 = clicked link, 0 = otherwise), and submitted personal information to the inserted fraudulent link (1 = submitted information, 0 = otherwise).

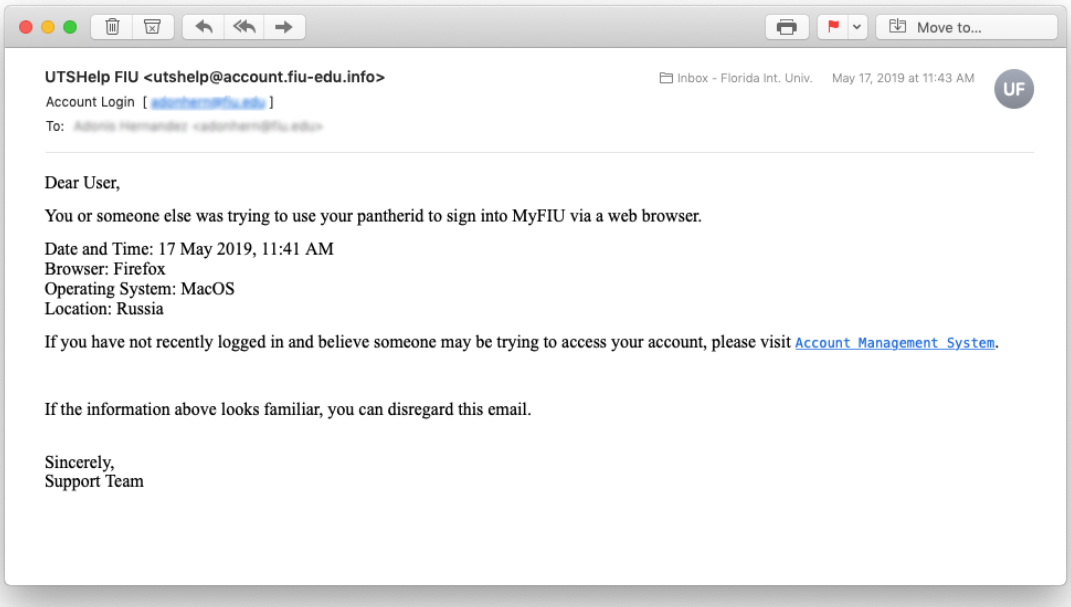


Figure 5. Template of Phishing Campaign

Treatment indicator. The treatment group was composed of 1000 staff members who completed the cybersecurity awareness program, whereas the comparison group consisted of 1000 staff members who did not complete the awareness program. The assignment to the treatment program is represented by the binary variable *TREAT*. Subjects coded 1 were those in the treatment group (TREAT = 1), and subjects who were coded 0 did not participate in the training program and thus were assigned to the comparison group (CONTROL = 0).

Sociodemographic background variables. Sociodemographic background factors are included in this study as statistical controls: age (ranged from 17 to 81), gender (0 = female, 1= male), education (1 = less than high school education, 2 = GED/high school graduation, 3 = technical school, 4 = Associate degree, 5 = Bachelor's degree, 6 = Master's degree, 7 = Doctoral degree), and length of employment (ranged from 1 year to 47 years).

The FIU DIT, first, received the information of these sociodemographic background for both treatment and comparison group from the Division of Human Resources at FIU. It was then combined with the results of the phishing campaign emails. Afterward, the identifiable information (i.e., name, FIU Panther Identification number [Panther ID]) have been deleted to keep the confidentiality of the participants in this study. The race variable is measured using dummy variables: white (1 = white, 0 = otherwise), black (1 = black, 0 = otherwise), Latino (1 = Latino/Hispanic, 0 = otherwise), and Asian (1 = Asian, 0 = otherwise); White is used as the reference category. The job category variable is measured using dummy variables as well: temporary non-student workers (1 = temporary non-student workers, 0 = otherwise), work study student (1 = work study student, 0 = otherwise), student assistant (1 = student assistant, 0 = otherwise), graduate assistant (1 = graduate assistant, 0 = otherwise), staff (1 = staff, 0 = otherwise), administrative (1 = administrative, 0 = otherwise), faculty (1 = faculty, 0 = otherwise), and executive service (1 = executive service, 0 = otherwise); Faculty is used as the reference.

Analytic Method. Over several decades, researchers have applied various tests (e.g., t-test, ANOVA, chi-square test, Mann-Whitney U-test, Mood's median test, Kruskal-Wallis test) of normality in order to choose statistically appropriate methods for parametric and non-parametric data (Wilcox, 2003, 2005; Zimmerman, 2011). In fact, when the dependent variable is normally distributed, the t-test is one of the most common methods to investigate potential differences between any two groups on a dependent variable; on the other hand, when the dependent variable is not normally distributed, the Mann-Whitney U-test can be suggested to examine potential differences between two groups on a dependent variable (William, 2009). In addition, when researchers suspect that the data is

non-normal distribution, both t-test and the Mann-Whitney U-test can be applied. As a result, the current study utilized the t-test and Mann-Whitney test to examine the differences between the treatment group (those who completed the cybersecurity awareness training) and the comparison group (those who did not complete the cybersecurity awareness training) on the dependent variable (i.e., status of response to phishing campaign).

Further, the Binary Logistic regression model was employed to examine associations between the dependent variable, cybersecurity awareness training, and sociodemographic background factors. According to Goodness-of-Fit in the logistic regression models, Pearson's Chi-square (i.e., 1.21; 1.20; 1.15) and Deviance measures are close to 1 — these logistic regression models (see Table 23) were fit to analyze the data. Also, Omnibus tests are statistically significant ($p < .001$). The full models with all the IV is a major improvement over the baseline model.

Table 18. Descriptive Statistics (N = 2000)

	Mean	SD	Min	Max
Response to phishing email				
Opened email	.41	.49	0	1
Clicked link	.19	.39	0	1
Submitted info	.04	.19	0	1
Cybersecurity training	.50	.50	0	1
Age	40.70	14.26	18	82
Gender (Male = 1)	.43	.49	0	1
Race				
White	.24	.42	0	1
Black	.15	.35	0	1
Latino/Hispanic	.53	.49	0	1
Asian	.08	.26	0	1
Education	5.09	1.68	1	7
Length of employment	6.72	6.93	1	47
Job category				
Temporary non-student worker	.18	.38	0	1
Work study	.02	.13	0	1
Student assistant	.06	.24	0	1
Graduate assistant	.04	.20	0	1
Staff	.13	.33	0	1
Administrative	.34	.47	0	1
Faculty	.22	.41	0	1
Executive service	.00	.04	0	1

Results

Descriptive Statistics. Tables 18 and 19 present the descriptive statistics for these data. These tables show mean, standard deviation, frequency and percent of responses to the phishing email, status of cybersecurity awareness training completion, and sociodemographic variables. In particular, Table 18 indicates the descriptive statistics of the dependent and independent variables. Also, Table 19 shows relative sequential percentages for the group responses to phishing campaign.

Table 19. Descriptive Statistics of the Group Responses to Phishing Campaign

	Cybersecurity Awareness Training			
	Not completed		***Completed***	
	Frequency	Relative Sequential Percentages	Frequency	Relative Sequential Percentages
Opened email	190		627	
Clicked link	83	44%	301	48%
Submitted data	22	27%	60	19%

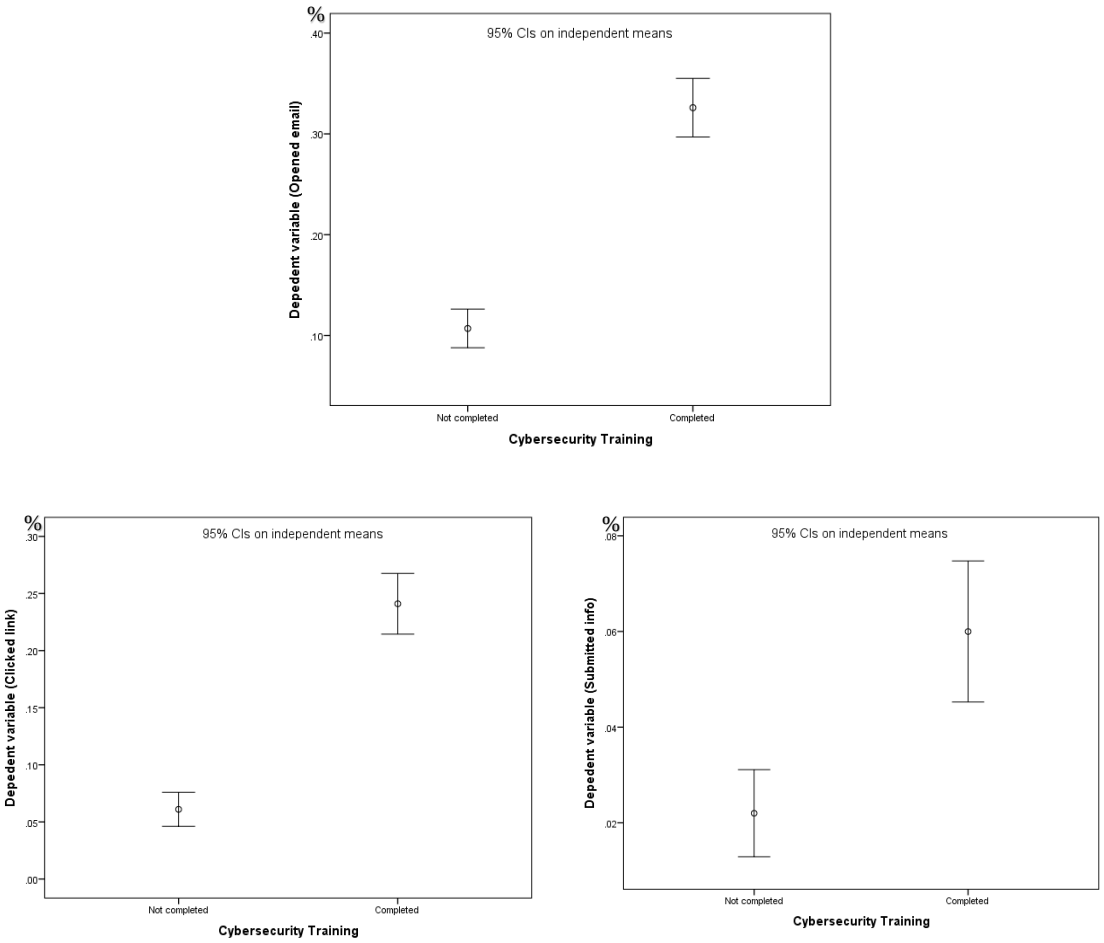


Figure 6. CI Bar Errors for Cybersecurity Training

Bivariate Relationships. First, Confidence Interval (CI) error bars were employed to scrutinize whether there are significant differences between the treated group and the comparison group for the dependent variables (i.e., the behaviors of opening email, clicking link, and submitting personal information). First, Figure 6 includes three error bars to further illustrate the differences revealed in the means tests (Cumming, Fidler, & Vaux, 2007). CI error bars do not overlap, which implies that there may be a significant difference between completing the cybersecurity awareness training and the phishing scam susceptibility. Since error bars provide clues about statistical significance, the statistical tests are therefore recommended to draw conclusions. As such, the t-test and Mann Whitney U-test were utilized to examine the relationships between these variables, as the following section will show.

Second, an observed correlation matrix is present in Table 20. Those correlations indicated that cybersecurity awareness training ($r = .28$, $p < .01$), age ($r = -.06$, $p < .01$), and Asian ($r = .05$, $p < .05$), were statistically correlated with the phishing campaign – the behavior of clicking the link. Also, it shows that cybersecurity awareness training ($r = .10$, $p < .01$), length of employment ($r = .06$, $p < .01$), temporary non-student worker ($r = -.11$, $p < .01$), staff ($r = .09$, $p < .01$), administrative ($r = .06$, $p < .01$), and faculty ($r = -.04$, $p < .05$) were statistically correlated with the phishing campaign – the behavior of submitting personal information. Lastly, cybersecurity awareness training ($r = .45$, $p < .01$), length of employment ($r = .16$, $p < .01$), temporary non-student worker ($r = -.24$, $p < .01$), staff ($r = .06$, $p < .01$), and administrative ($r = .18$, $p < .01$) were statistically correlated with the phishing campaign – the behavior of opening the email.

Table 20. Correlations of the Study Variables

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1. OE	1																			
2. CL	.58**	1																		
3. SI	.25**	.42**	1																	
4. Cyber-T	.45**	.28**	.10**	1																
5. Age	-.01	-.04	-.06**	-.01	1															
6. Gender	.03	.01	-.03	-.07**	.14**	1														
7. White	.04*	.01	.01	.03	.21**	.12**	1													
8. Black	-.06**	-.01	-.01	-.07*	-.01	-.08**	-.23**	1												
9. Hispanic	-.02	.01	-.02	.03	-.16*	-.09*	-.60**	-.44**	1											
10. Asian	.05*	.01	.05*	-.01	-.03	.07**	-.16**	-.11*	-.31**	1										
11. Education	.07**	-.01	-.02	-.04	.22**	.02	.21*	-.11*	-.17*	.13**	1									
12. LE	.16**	.06**	-.01	-.16*	.17**	.53**	.06*	.07**	-.06*	-.01	-.02	1								
13. TNS	-.24**	-.11*	-.03	-.28*	-.04*	-.01	-.10**	.24**	-.03	-.07**	-.21**	-.19**	1							
14. WS	-.02	.01	-.01	.02	-.17*	.01	-.07**	.03	.05*	-.02	-.19**	-.08*	-.06**	1						
15.SA	-.05*	.01	.03	-.03	-.31*	-.04	-.06**	.02	.04	.01	-.32**	-.18*	-.12*	-.03	1					
16.GA	.05*	-.02	.03	-.02	-.14*	.01	.04*	-.04*	-.12*	.20*	.04*	-.11*	-.09*	-.02	-.05*	1				
17. Staff	.06**	.09**	.04	.20**	.14**	.01	-.10**	-.01	.13**	-.05**	-.34**	.17**	-.18*	-.05*	-.09**	-.08**	1			

18.Admin	.18***	.06***	-.01	.28***	-.08**	-.13**	-.04**	-.09**	.15***	-.10***	.15**	.07***	-.34**	-.09***	-.18***	-.15**	-.27***	1		
19. Faculty	-.01	-.04**	-.03	-.17**	.32***	.17***	.27**	-.10**	-.24**	.14**	.52**	.14***	-.25**	-.07***	-.13***	-.11**	-.20**	-.38***	1	
20. Executive	.01	.03	-.01	.00	.05*	.02	.01	-.01	-.01	.02	.03	.01	-.02	-.01	-.01	-.01	-.01	-.03	.24	1

Note: Opened email (OE); Clicked link (CL); SI (Submitted information); Cybersecurity training (Cyber-T); Length of employment (LE); Temporary non-student employee (TNS); Work study (WS); Student assistant (SA); Graduate assistant (GA). *$p < .05$, **p < .01, ***$p < .001$

T-test Analysis. The independent *t*-tests were employed to determine if there were statistically significant variances of falling for the phishing campaign trial between these two groups. As shown in Table 21, surprisingly, the treated group had a higher probability of falling for the phishing campaign trial than the comparison group. The F-ratio under the "Levene Test" indicates a corresponding probability (sig.) of .000; therefore, the unequal variance *t*-test was accurate in this analysis. First, for opening the email, the t-test of rank scores were statistically different (t (1916.48) = 344.19, p < .001) between the treated group (M = .63, SD = .48) and the comparison group (M = .19, SD = .39). Second, for clicking the link, the t-test of rank scores were statistically different (t (1638.13) = 835.32, p < .001) between the treated group (M = .30, SD = .45) and the comparison group (M = .08, SD = .27). Last, for submitting personal information, the t-test of rank scores were statistically different (t (1664.38) = 76.77, p < .001) between the treated group (M = .06, SD = .23) and the comparisongroup (M = .02, SD = .14). Importantly, however, all these results were in the unpredicted (inverse) direction. It means that the treated group was more likely to fall for the phishing campaign trial rather than the comparison group. Thus, hypothesis 16 is not supported.

Table 21. The t-Test Information to Test a Hypothesis

	Cybersecurity training		t-Test for equality of means		
	Not completed	Completed			
	M (SD)	M (SD)	t	df	Sig. (2-tailed)
Response to phishing email					
Opened email	.19 (.39)	.63 (.48)	-22.18	1916.48	.000
Clicked link	.08(.27)	.30 (.45)	-12.87	1638.13	.000
Submitted info	.02 (.14)	.06 (.23)	-4.30	1664.38	.000

****p* < .001

Mann Whitney U-test Analysis. To compare whether there is a difference in the dependent variables (submitted information, clicked link, and opened email) for two independent groups, the Mann-Whitney U-test was applied (see Table 22). Interestingly, the Mann-Whitney U test indicated that the level of submitting data susceptibility was greater for individuals who completed cybersecurity awareness training (Mean = 10019.50) than for individuals that did not receive the cybersecurity awareness training (Mean = 981.50), U = 481000.00, p = .000; the level of clicking inserted link susceptibility was greater for individuals who did complete cybersecurity awareness training (Mean = 1090.50) than for individuals that did not receive the cybersecurity awareness training (Mean = 910.50), U = 410000.00, p = .000. For the Mann Whitney U-test model for the phishing campaigns, the effect size is 0.43, which means there was a moderate effect between the treatment and comparison groups, according to Cohen's classification of effect sizes (0.1 = small effect, 0.3 = moderate effect, and 0.5 and above = large effect). In other words, the FIU cybersecurity training for online users at FIU had a moderate effect on the online users' behaviors to engage in the phishing scam, but in the direction opposite to what was hypothesized.

Table 22. Mann Whitney U-test Information to Test a Hypothesis

Variable	Group	N	Mean rank	*U*	*P*
Opened email	***Not Completed***	190	782.00	281500.00	.000
	Completed	627	1219.00		
Clicked link	***Not Completed***	83	891.50	391000.00	.000
	Completed	301	1109.50		
Submitted information	***Not Completed***	22	981.50	481000.00	.000
	Completed	60	1019.50		

Logistic Regression Analysis. In Table 23, the phishing campaign measure was regressed on the independent variables. As the table illustrates, some independent variables included in the model are significant predictors of falling for the phishing campaign. Importantly, few variables (i.e., cybersecurity training, age, and Asian) were significantly associated with the falling for the phishing campaign: clicked link and submitted personal information in the logistic regression. Overall, the three models in Table 23 also indicate there were no statistically significant effects for gender, education, length of employment, and job category.

Model 1 indicates that FIU employees who completed the cybersecurity awareness training (b = 1.84, SE = .11, Exp(B) = 6.31, p < 001) had 6.31 times greater odds of opening the email than FIU employees who did not complete the training. In addition, male employees had greater odds of opening the email than female employees (b = .30, SE = .10, Exp(B) = 1.35, p < 01). Those employed longer had slightly greater odds of opening the email (b = .04, SE = .01, Exp(B) = 1.04, p < 001). The model also showed that those who were older had lower odds of opening the email (b = -.01, SE = .01, Exp(B) = .98, p < 001). Temporary non-student workers had lower odds of opening the email (b = -.96, SE = .23, Exp(B) = .38, p < 001).

Model 2 and 3 introduce the variables to test hypothesis 16 – An individual who completed the cybersecurity awareness training was more likely to fall for the phishing campaign trial than someone who did not complete the training. Model 2 and 3 failed to provide support for the hypothesis 16. Specifically, individuals who completed the cybersecurity awareness training had 4.35 times greater odds of clicking the inserted link (b = 1.47, SE = .14, Exp(B) = 4.35, p < 001). Also, the individuals who completed the

cybersecurity awareness training had 2.65 times greater odds of submitting personal information than individuals who did not complete the training (b = .97, SE = .27, Exp(B) = 2.65, p < 01). In sum, the treated group exhibited greater odds of submitting personal information or clicking a faked link and submitting personal data than the comparison group.

Table 23. Logistic Regression Results of Cybersecurity Training and Phishing Campaign

	Model 1: Opened email			Model 2: Clicked link			Model 3: Submitted Info		
Variables	Coefficient	*SE*	Exp (*B*)	Coefficient	*SE*	Exp (*B*)	Coefficient	*SE*	Exp (*B*)
Cybersecurity training	1.84***	.11	6.31	1.47***	.14	4.35	.97**	.27	2.65
Age	-.01***	.01	.98	-.01**	.01	.98	-.02*	.01	.97
Gender	.30**	.10	1.35	.21	.12	1.24	-.31	.24	.72
Race									
White	.11	.13	1.12	.05	.15	1.05	.40	.30	1.49
Black	.03	.16	1.03	.16	.18	1.18	.06	.36	1.06
Asian	.33	.20	1.39	.09	.23	1.09	.83*	.38	2.30
Education	.06	.04	1.06	.03	.05	1.03	.01	.09	1.00
Length of employment	.04***	.01	1.04	.02	.01	1.02	.01	.02	1.00
Job category									
Temporary	-.96***	.23	.38	-.38	.27	.68	.01	.52	1.00
Work study	-.40	.47	.66	.03	.52	1.03	-.44	.16	.64
Student assistant	-.48	.32	.61	.14	.36	1.15	.26	.65	1.30
Graduate assistant	.46	.28	1.59	-.09	.34	.91	.25	.56	1.29
Staff	-.17	.23	.83	.28	.26	1.32	.49	.50	1.64
Administrative	.02	.18	1.02	-.08	.19	.92	-.07	.39	.93
Executive	.36	.09	1.44	1.78	.05	5.98	-.42	.08	.00
Sig.	.000			.000			.001		
-2 Log Likelihood	2192.94			1772.67			646.69		
Nagelkerke R^2	.305			.141			.065		

Note: Entries are unstandardized coefficients; *p < .05, **p < .01, ***p < .001

As shown in Table 23, those who were older had lower odds of clicking the inserted link (b = -.01, SE = .01, Exp(B) = .98, p < 01) and the behavior of submitting personal information (b = -.02, SE = .01, Exp(B) = .97, p < 05). In terms of the race variable, Asians had 2.3 times greater odds of engaging in "falling for" behavior of submitting personal information than Hispanics. Most of the job position categories were not statistically associated with the behavior of submitting personal data and clicking the inserted link. In accordance with the results of the logistic regression, the sociodemographic variables (i.e., age and race) were significant predictors for the dependent variable (falling for the phishing campaign).

Discussion and Conclusion

This chapter examined whether place manager interventions suppress crime opportunities in the online domain. Previous research (e.g., Eck, 2002; Eck & Guerette, 2012; Mazerolle & Ransley, 2006; Roberts, 2007) provided strong support that changes in place management strategies had the potential to decrease crimes in the physical space. Kumaraguru et al. (2009), Sheng et al. (2007), and Nyeste and Mayhorn (2010) found that a phishing prevention training could assist online users in preventing themselves from phishing scam victimization. As such, this study hypothesized that a cybersecurity awareness program deters online users' risky behaviors, which could lead them to falling for a phishing campaign. In this final section, the findings and policy implications, the limitations of the study, and future research are discussed.

In alignment with the t-Test and Mann Whitney U-test analysis, the results of this study indicate that the FIU cybersecurity training for the employees had a moderate effect on the online users' behaviors to engage in the phishing campaign email, but in the

direction opposite to what was hypothesized. To supplement these findings derived from the -Test and Mann Whitney U-test, Logistic regression models were employed. To that end, these regression models show that the treated group was more likely to engage in clicking a faked link or submitting personal data than the comparison group. Currently, the FIU community, especially the Division of Information Technology in collaboration with the SANS institute and the U.S. Department of Homeland Security, or the U.S. National Cybersecurity Alliance, has put their efforts into combating cybercrime (e.g., phishing scam for online users at FIU). Despite their effort, the findings show that the cybersecurity awareness training did not help to prevent participants from engaging in "falling for" behaviors in the quasi-experimental phishing campaign derived from the FIU's DIT. As stated above, these results did not provide support that there is a link between the cyber place management (cybercrime prevention training) and the reduction of cybercrime incidents.

Unfortunately, this study was limited in explaining why the treated group was more likely to fall for phishing scams rather than the comparison group did use this phishing campaign data derived from the FIU's DIT. The body of literature (Choi, 2008; Holt & Bossler, 2009, 2013; Ngo & Paternoster, 2011; Reyns, 2013; Reyns & Henson, 2016) found that greater exposure (e.g., time spent online, including shopping, playing video games, emailing, using social networking media, using chat rooms, and instant messaging) to motivated cyber offenders increases online users' likelihood of being cybercrime victimization. According to the results in Table 23, the treated group who participated in the cybersecurity awareness program were 6 times more likely to open emails than the comparison group. One possible explanation for these results is that, as shown in Table 23,

the treated group might have been more likely to engage in online activities (i.e., emailing and using social networking sites), than the comparison group was, increasing the possibility of the treated group falling for the phishing campaign.

In spite of the conclusion of this study, the significance of cybersecurity awareness practice cannot be overlooked. This is considering that many cybersecurity experts and scholars assert that cybersecurity awareness education and training is one of the most significant aspects of an institution's security posture for individuals to effectively fight against cyber threats (Dodge, Carver, & Ferguson, 2007; Abawjy, Thatcher, & Kim, 2008). According to a European Cyber Security Perspective 2019 report, cutting-edge technology cannot be the only remedy to mitigate the cybercrime phenomenon. The human element is also a crucial component in the solution to disrupting cyber threats. As such, considering that human factors still play a significant role in the ongoing development of cybersecurity and protecting critical information infrastructures, it is important to note that cyber place management strategies along with implementing cybersecurity awareness training, and a resilient incident response system are all crucial means to effectively mitigating the likelihood of cybercrime victimization and minimization of losses in an online setting.

Next, the findings of this study revealed that some sociodemographic factors such as age, race, length of employment, and job category were associated with participants falling for phishing tests. This analysis explained that the older generation was more resistant to cyber deception than the younger generation; also, it suggested that individuals who were in a higher job position and a longer period of employment were more likely to engage in "falling for" behaviors during a phishing attack. In a broad sense, it seems reasonable to expect that employees can be influenced by their subculture and attitude

regarding cybercrime and cybersecurity issues in their work environment. Therefore, this suggests that cyber place managers not only need to be considerate about external cyber threats, but they also should concern themselves about whether employees are proactively engaging in preventing cybercrime victimization through daily life, or what sort of subculture in their community regarding cybersecurity and cybercrime exists in order to improve their perception and attitude about cybersecurity awareness training.

Inevitably, the online training platform at FIU might face disadvantages with the limited formatting of contents and the lack of interactivity. For example, the online training platform was limited to effectively deliver the cybersecurity awareness contents along with page-turning training and few videos. In accordance with the previous research (e.g., Holmberg, 2007; Kirtman, 2009; McCrory, Putnam, & Jansen, 2008; Menchaca, 2008), active learning and participation are keys to effective teaching and learning. Thus, it can be similarly applied to online teaching and learning to educate online users to effectively deal with crime in the online domain.

Policy Implications. Although the findings of this study did not directly add to a large body of evidence that cybersecurity awareness training is effective to proactively encourage online users to avoid cybercrime victimization, this study can provide significant implications for safer practices. With regard to practice, the findings suggest that higher education institutions may need to improve the existing training program as a pragmatic place management strategy so that it can actually help members of the university community improve their knowledge and skills to wisely deal with cybercrime. In particular, it is important to develop a tailored cybersecurity training program that can apply to the university community. For example, higher education institutions can utilize

a gaming platform for their cybersecurity awareness program. Cone, Irvine, Thompson, and Nguyen (2007) and Labuschagne, Burke, Veerasamy, and Eloff (2011) found that an interactive web-based game platform for cybersecurity awareness training was exponentially more effective in improving the cybersecurity efficacy of general computer users. It suggests that the use of gaming learning platforms can be successful in fully supporting cybersecurity awareness programs. In short, it is a crucial moment for the launching of a taskforce team from academia to the public and private sectors to develop the best practices (e.g., anti-phishing games) that can make our community and society more safe and secure from these risks.

Second, some of the sociodemographic factors were significant predictors for cybercrime prevention strategies; therefore, these aspects must be considered once cybersecurity managers implement their awareness program. Given this situation, establishing a cybersecurity awareness culture and environment may be a prerequisite condition in the enhancement of cybercrime prevention strategies. Online users' attitude and motivation towards cybersecurity guidelines, and the needs of cybersecurity awareness training can be enforced by providing the user community with regular updates on state-of-the-art cybercrime information and cybersecurity issues (Abawajy, Thatcher, & Kim, 2008). Current efforts (i.e., Ransomware Attacks Alert, Email Scams Alert, Security Alert: Update Your Zoom for Mac Application) derived from the FIU Division of Information Technology are good examples to build this cybersecurity awareness culture (see Appendix E). Thus, taken as a whole, this proactive and holistic approach can create an institutional environment where people encourage each other to have preventative actions and attitudes. In a broad sense, the tactics for phishing campaigns and cyber fraud have changed so

quickly and continuously. As a result, the more place managers and members in higher education are aware of the various and novel methods of phishing campaigns, the more online users in higher education can accurately disrupt cybercriminals' opportunities. Accordingly, cyber place managers (i.e., cybersecurity officers in universities) can develop or apply more agile real-time detection systems or behavioral-pattern threat detection systems for identifying the emerging phishing campaign or other types of cybercrime. Because the trends of cybercrime change and turn over so quickly, notification of a novel cybercrime is necessary for online users. Additionally, higher education institutions in collaboration with law enforcement agencies (e.g., FIU Police Department, the United States Computer Emergency Readiness Team [CERT], Cybersecurity and Infrastructure Security Agency [CISA] of the Department of Homeland Security), need to quickly disseminate this information to online users as soon as cybersecurity officers identify it.

Limitations. The present study also has several limitations. First, because the selection of the treatment group individuals was voluntary and not randomly assigned, it is possible that there are inherent differences between them and the comparison group. These differences could be what is responsible for the findings reported herein. However, because the multivariate logistic regression analyses revealed very few differences among the control variables overall, this seems less likely to be case. Nonetheless, it is possible that there exists an inherent difference between the treatment group individuals and comparison group individuals along with their online habits. For example, the treatment group might have been more likely to engage in online activities (i.e., using email and social media sites) than the comparison group. Consequently, their active online behaviors might facilitate the treatment group individuals to have greater chances for

opening the phishing email, clicking the inserted link, and submitting personal information than the comparison group individuals. Unfortunately, this study was limited in measuring the activeness of online activities for individuals in the treatment and comparison groups. In short, future studies can consider revealing whether there are relationships between cybersecurity awareness training, online behavior, and falling for phishing scams in order to enhance the validity of research design.

Second, similar to Caputo et al.'s (2014) study, this study was limited to observing the difference of "falling for phishing scams" among participants who completed the cybersecurity awareness program. This is because 2000 participants who completed the training were selected by the FIU's DIT staffs and there was no identifiable information to determine how long the training effect lasts. For example, someone who completed the training on November 1, 2018 as opposed to a participant who completed the training on April 25, 2019. Given this, there may be a gap for remaining effectiveness of the FIU's cybersecurity awareness training between those participants. Thus, this study was not able to clarify how much of an impact the training has lasted in enhancing participants' preventative behaviors during the phishing scam trial.

Third, this research was limited to accurately determine all the participants' click rates and submitted data rates because the rate of participants' response to the phishing campaign email was unexpectedly low. For example, the first 1000 phishing email trial had been executed to determine the participants' response between May 15 and 18, 2019; the second 1000 phishing email trial collected the participants' responses between May 17 and 21, 2019. In particular, even if all the participants received the phishing email trial, 1183

(59.2%) out of 2000 individuals did not open this email during the trial. Unfortunately, this study was unable to exactly point out why the participants' response to the phishing campaign emails in this study was low when compared to the existing studies (i.e., Kumaraguru et al., 2009). This raises the question of how Kumaraguru et al.'s study retained such high rate of participants' response to the phishing campaign emails in their study. In this case, Kumaraguru et al.'s (2009) study held a long-term retention period (i.e., 28 days), it might be a sufficient amount of time to determine all the participants' exact response rates. Specifically, Kumaraguru and colleagues designed it to send the 7 simulated phishing emails for 28 days. Moreover, the participants of the treated groups (343 out of 515) in Kumaraguru et al.'s study have received the phishing emails right before- or after- the phishing awareness training within 28 days. To that end, it might increase the participants' response rates to the phishing email.

As discussed above, lastly, the findings of this study were unable to reveal the explanation why the treated group was more likely to fall for the phishing campaign rather than the comparison group. In a study of "Online training: An evaluation of the effectiveness and efficiency of training law enforcement personnel over the Internet," Schmeekle (2003) found that no meaningful learning differences occurred between the online training group and the classroom training group. More importantly, the online training group reported lower motivation and positive feelings concerning their training course than did the classroom group. In line with Schmeeckle's findings, it is possible to explain that although the treated group have participated in the FIU's cybersecurity online training course, they might not pay attention to the training contents and materials so that its online training was not as effective an instructional method as classroom training.

Future research should attempt to accurately design and implement methods to reduce these weaknesses discussed above. Also, future studies can consider evaluating the effectiveness of cybersecurity awareness programs similar to that of Rezgui and Marks' (2008) study, through more diverse methods (e.g., survey-based questionnaire, observation, interview, and systematic document review). In addition, future studies can evaluate the effectiveness and efficiencies of online training as it compared to classroom training for cybersecurity awareness courses through the measuring of trainees' learning outcome, motivation, and attitudes.

CHAPTER 6

CONCLUSION: PROJECTION OF THE CYBERCRIME TRIANGLE

In the age of unprecedented information inundation, the global community is facing emerging challenges. Internet and information technology systems provide cybercriminals great opportunities to exploit online users all over the globe. In this sense, due to the global nature of crime, cyber adversaries attack suitable targets located in different real-world time zones without border controls. Therefore, global cyber threats trigger direct and indirect damages to the economic well-being and national/international security.

To effectively combat against these growing state-of-the-art cyber threats, it is important to apply a holistic framework as a cybercrime prevention strategy. Many criminologists (Madesen & Eck, 2013; Wilcox & Cullen, 2018) assert that if criminals are properly handled, suitable targets are protected, or places are well-guarded, crime can be discouraged. Although previous studies have focused on elaborating and empirically testing the crime triangle framework rooted in the notion of Routine Activity Theory (RAT) to establish crime control strategies, to date, there is no empirical study to apply the crime triangle concept to cybercrime prevention strategies. The main purpose of this dissertation was to fill this gap in the literature by empirically exploring and proposing the cybercrime triangle framework to help establish a solid blueprint of cybercrime prevention strategies.

This conclusion chapter is divided into four major areas. It begins with a layout of the dissertation, and then address the contributions of this dissertation. Also, this chapter examines the implications of the research approach in terms of design limitations and the

adequacy of the theoretical framework. Lastly, the future research in this area of study is discussed.

Layout of Dissertation

This dissertation sought to magnify the lens of the cybercrime triangle framework in order to understand why and how each element of cybercrime triangle dynamics (motivated offender, suitable target, and place) has connected each other in the virtual world. In order to answer this question, a quantitative research methodology was employed to provide more perspective linking cybercrime offenses to cybercrime victimization and place management strategies.

This dissertation was organized as follows. Chapter 2 reviewed the literature on the topic examined in this study. This was followed by a look into the overall trends in cybercrime over 18 years. It also included a review of the literature linking (1) routine activity theory to cybercrime and (2) crime triangle tenets to crime. Furthermore, a discussion of the theoretical background of routine activity and the crime triangle framework for cybercrime events was specifically reviewed. The second chapter concluded with the identification of gaps in the research literature and the importance of the application of the crime triangle to cybercrime.

In Chapter 3, this study explored the characteristics of cybercriminals via a criminal profiling method using criminal record documents (i.e., indictments/complaints) collected from the FIU Law School library website. This study used descriptive and regression models to provide answers to the questions of which, what, where, and how cybercrime offenders attacked suitable targets in the United States. After conducting a cybercriminal

profiling analysis, this study delineated the situational/opportunity factors, attack severity, geographic factors, and sociodemographic background factors.

In Chapter 4, the associations between cybercrime victims, digital capable guardians, perceived risk of cybercrime, and online activity were examined using Eurobarometer survey data. This phase used a cross-sectional design to reveal the nature of cybercrime victimization. The findings of the correlation and regression analyses were discussed. A discussion of the results, conclusions, and limitations of the study closed chapter 4.

In Chapter 5, the association between place management activities and cybercrime prevention was examined using "Phishing Campaign" and "Cybersecurity Awareness Training Program" related data derived from FIU's information technology division. This phase employed a quasi-experimental design. The data was analyzed by t-test, Mann Whitney U-test, logistic regression methods to evaluate the effectiveness of phishing prevention training program at FIU. The results of the effectiveness of the cybercrime prevention program were then presented.

Contributions and Implications

This section discusses the contributions of this dissertation. Importantly, the present study provides support for the theoretical, methodological, and practical extensions of criminological research to explain cybercrime phenomenon and cybercrime prevention. First, the RAT approach contributes significantly to the theoretical framework of the cybercrime triangle framework. The application of this concept provides some holistic insight into the cybercrime triangle mechanisms to effectively deal with cyber threats in

information era. RAT suggests that cyber offenses are influenced by situational factors and crime opportunity factors; moreover, cyber threats can be prevented by digital capable guardians and place management tactics. In other words, if appropriate prevention strategies executed by capable guardians and place managers were in the virtual world, cyber offenders are unable to obtain and use the crime opportunities for achieving their vicious purposes. Although the importance of criminological theory into cybercrime and cybersecurity fields have been considered, the lack of criminological theory has been rarely applied to devise an effective blueprint of cybercrime prevention strategies. Thus, one of the contributions of the current study is the importation and advocation of criminological theories (e.g., RAT, crime triangle framework) for cybercrime research.

Second, this research is grounded on new analytic models that reveal uncovered social contexts such as cyber offending and the perceived risk of cyber-threats. To date, there is no study to conduct on the associations between cybercrime offending, situational factors, and cybercrime opportunity factors through cybercriminal profiling analytic framework. As such, this dissertation contributes significantly to providing a solid analytic method to analyze cyber offending using the SSBACO Cybercriminal Profiling framework. In addition, a large body of literature was reviewed testing the direct effects of digital capable guardianship and online routine activity on cybercrime victimization. However, few studies have examined this relationship through perceived risk of cyber-threat for mediation effects. Given that situation, this study contributes to the existing literature via an application of a new statistical approach in order to analyze the relationships between cybercrime victimization and cyber offending, and human factor (i.e., perception of risk).

Third, the practical contributions of this study stem mainly from the theoretical importation of criminological theory into the cybercrime and cybersecurity fields. Specifically, this study provides explicit explanations how the cybercrime triangle perspective and framework lead to devise cybercrime preventions strategies in addressing new forms of crime opportunity and offending in the virtual world. For example, in line with the cybercrime triangle perspective, cyber place manager interventions and capable guardianship suppress crime opportunities in the online domain, albeit of the intangible variety (e.g., anonymity, collapse of spatial/temporal borders) of cyber environment. In this regard, practitioners and organizations can utilize these examples derived from criminology, such as a cyber place manager (i.e., information security official), enhancing digital capable guardians over their computer/network systems and proving tailored cybersecurity awareness trainings to improve individual online users' preventive capacities.

In summary, this research has contributed to the knowledge of the cybercrime prevention along with the theoretical, methodological, and practical extensions of criminological research. It has shown that (1) cyber offending are related with situational and crime opportunity factors; (2) increasing digital capable guardians and the use of strategic management of cyber place can mitigate cybercrime victimization; (3) human factor (perception of risk of cyber-threat) can enhance online users' efficiency and performance in preventing cybercrime victimization.

In alignment with these findings, this dissertation suggests three major policy implications in the following dimensions:

1. The cybercriminal profiling analysis results indicate that the 'SSBACO Cybercriminal Profiling Model' can be a scientific and useful method. This

suggests that it can be to help law enforcement establish new lines of scrutiny in cybercrime investigations.

2. The findings of this study provide significant implication of reinforcing the level of perceived risk of cyber-threat. In a related sense, disseminating efforts to improve the level of perceived risk of cybercrime (e.g., Cyber-Digital Task Force Report provided by the U.S. Department of Justice) are key practices to help online users to protect themselves against advanced cybercriminal typology.
3. Although the findings of this study did not directly add to a large body of evidence that cybersecurity awareness training is effective to proactively encourage online users to deal with cybercrime, the findings suggest that organizations may need to improve the existing training program as a pragmatic place management strategy. To that end, it can actually help online users improve their knowledge and skills to wisely deal with cybercrime.

Limitations and Future Research

Despite the contributions of this study, there are several issues that were pointed out as the limitations of this research. In this section, the limitations of this study and future research are discussed. There were theoretical and methodological issues in this study. First, this study relies primarily on a new integrated theoretical (cybercrime triangle) perspective so that the existing literature might be limited to directly provide enough suggestions and construct on the theoretical background of cybercrime triangle framework. The lack of conceptual sophistication is evidence when discussing the issue of cyber offending in Chapter 3. Second, this study used limited data (e.g., court record documents, cross-

sectional datasets, and dichotomized measure of survey items) to reveal causal factors of cyber offending and cybercrime victimization. For instance, a series of cross-sectional datasets utilized in this study were unable to reveal the time-ordering causal effects.

Future research should strive to properly design and implement research methods to reduce these weaknesses discussed above. First and foremost, further research should address the theoretical shortcomings of the cybercrime triangle model. Another area for future research should be to apply the relevant theoretical concepts and propositions to explain cyber offending and cyber place management. Finally, the current study concludes that the key strategy to combat cybercrime is that experts from government, law enforcement, private sector, and academia need to closely work together to discuss and coordinate strategies to reduce cyber threats. Through the application of the cybercrime triangle framework to cybercrime events, the findings of this study are expected to benefit the global community and strengthen efforts to effectively fight against malicious and state-of-the-art cybercriminals.

References

Abawajy, J., Thatcher, K., & Kim, T. H. (2008, April). Investigation of stakeholders' commitment to information security awareness programs. In *2008 International Conference on Information Security and Assurance (ISA 2008)* (pp. 472-476). IEEE.

Abdulhafedh, A. (2017). Incorporating the multinomial logistic regression in vehicle crash severity modeling: a detailed overview. *Journal of Transportation Technologies*, *7*(03), 279.

Akers, R. L., & Sellers, C. S. (2013). *Criminological theories: Introduction, evaluation, and application*. New York, NY: Oxford University Press.

Albanese, J. S. (2011). *Transnational crime and the 21st century: Criminal enterprise, corruption, and opportunity*. New York, NY: Oxford University Press.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, *26*(4), 276-289.

Al-Nemrat, A., Jahankhani, H., & Preston, D. S. (2010, September). Cybercrime victimisations/criminalisation and punishment. In *International Conference on Global Security, Safety, and Sustainability* (pp. 55-62). Springer, Berlin, Heidelberg.

Anastas, J. W. (1999). *Research design for social work and the human services*. Columbia University Press.

Andresen, M. A., & Felson, M. (2009). The impact of co-offending. *The British Journal of Criminology*, *50*(1), 66-81.

Andrews, F. M. (1984). Construct validity and error components of survey measures: A structural modeling approach. *Public opinion quarterly*, *48*(2), 409-442.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Ariyapperuma, S., & Minhas, A. (2005, October). Internet security games as a pedagogic tool for teaching network security. In *Proceedings Frontiers in Education 35th Annual Conference* (pp. S2D-1). IEEE.

Awareness Training. (2019). In *Florida International University*. Retrieved from https://security.fiu.edu/awareness_training

Back, S. (2016). Empirical assessment of cyber harassment victimization via cyber-routine activities theory.

Back, S., & LaPrade, J. (2019). The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 1-4.

Back, S., LaPrade, J., Shehadeh, L., & Kim, M. (2019, June). Youth hackers and adult hackers in South Korea: An application of cybercriminal profiling. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 410-413). IEEE.

Back, S., LaPrade, J., & Soor, S. (2018). Spatial and Temporal Patterns of Cyberattacks: Effective CYBERCRIME Prevention Strategies around the Globe. *International journal of protection, security & investigation*, *3*, 7-13.

Back, S., Soor, S., & LaPrade, J. (2018). Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 40-55.

Back, S., Sung, Y., & LaPrade, J. (2017). The effect of terrorism risk perception and agency's interaction on police homeland security preparedness. *International Journal of Police & Policing*, *2*(1), 7-13.

Baker, T., & Wolfer, L. (2003). The crime triangle: Alcohol, drug use, and vandalism. *Police practice and Research*, *4*(1), 47-61.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Macmillan.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *Mis Quarterly*, 31-60.

Bartol, C. R. (1996). Police psychology: Then, now, and beyond. *Criminal Justice and Behavior*, *23*(1), 70-89.

Beauregard, E., & Busina, I. (2013). Journey "during" crime: Predicting criminal mobility patterns in sexual assaults. *Journal of interpersonal violence*, *28*(10), 2052-2067.

Beauregard, E., Lussier, P., & Proulx, J. (2005). The role of sexual interests and situational factors on rapists' modus operandi: Implications for offender profiling. *Legal and Criminological Psychology*, *10*(2), 265-278.

Beauregard, E., Lussier, P., & Proulx, J. (2008). Criminal propensity and criminal opportunity. In *Criminal Profiling* (pp. 89-113). Humana Press.

Bennell, C., & Corey, S. (2008). Geographic profiling of terrorist attacks. In *Criminal profiling* (pp. 189-203). Humana Press.

Berk, R. A., & de Leeuw, J. (1999). An evaluation of California's inmate classification system using a generalized regression discontinuity design. *Journal of the American Statistical Association*, *94*(448), 1045-1052.

Berk, R. A., & Rauma, D. (1983). Capitalizing on nonrandom assignment to treatments: A regression-discontinuity evaluation of a crime-control program. *Journal of the American Statistical Association*, *78*(381), 21-27.

Bernasco, W. (2010). A sentimental journey to crime: Effects of residential history on crime location choice. *Criminology*, *48*(2), 389-416.

Bernasco, W., & Nieuwbeerta, P. (2004). How do residential burglars select target areas? A new approach to the analysis of criminal location choice. *British Journal of Criminology*, *45*(3), 296-315.

Bernburg, J. G., & Thorlindsson, T. (2001). Routine activities in social context: A closer look at the role of opportunity in deviant behavior. *Justice Quarterly*, *18*(3), 543-567.

Birkbeck, C., & LaFree, G. (1993). The situational analysis of crime and deviance. *Annual review of sociology*, *19*(1), 113-137.

Blanchette, K. (2002, January). Classifying female offenders for effective intervention: Application of the case-based principles of risk and need. In *Forum on Corrections Research* (Vol. 14, No. 1, pp. 31-35). CORRECTIONAL SERVICE OF CANADA.

Block, R., & Bernasco, W. (2009). Finding a serial burglar's home using distance decay and conditional origin–destination patterns: a test of empirical Bayes journey-to-crime estimation in the Hague. *Journal of Investigative Psychology and Offender Profiling*, *6*(3), 187-211.

Block, R., Galary, A., & Brice, D. (2007). The journey to crime: Victims and offenders converge in violent index offences in Chicago. *Security Journal*, *20*(2), 123-137.

Block, R. L., & Block, C. R. (1995). Space, place and crime: Hot spot areas and hot places of liquor-related crime. *Crime and place*, *4*(2), 145-184.

Bonk, C. J. (2002). *Online training in an online world*. Bloomington, IN: CourseShare. com.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, *44*(4), 500-523.Boudreaux, M. C., Lord, W. D., & Jarvis, J. P. (2001). Behavioral perspectives on child homicide: The role of access, vulnerability, and routine activities theory. *Trauma, Violence, & Abuse*, *2*(1), 56-78.

Braga, A. A., & Clarke, R. V. (2014). Explaining high-risk concentrations of crime in the city: Social disorganization, crime opportunities, and important next steps. *Journal of Research in Crime and Delinquency*, *51*(4), 480-498.

Brantingham, P. L., & Brantingham, P. J. (1981). Environmental criminology. Beverly Hills, CA: Sage.

Brantingham, P. L., & Brantingham, P. J. (1990). Situational crime prevention in practice. *Canadian J. Criminology*, *32*, 17.

Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. Santa Barbara, CA: ABC-CLIO.

Britz, T. M. (2010). *Terrorism and technology: Operationailzing cyberterrorism and identifying concepts*. Durham, NC: Carolina Academy Press.

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and Cybercrime Risks in a University Student Community. *Available at SSRN 3176319*.

Brody, R. G., Gonzales, K., & Oldham, D. (2013). Wi-fi hotspots: secure or ripe for fraud. *Journal of Forensic Investigative Accounting*, *5*(2), 27-47.

Burruss, G. W., Giblin, M. J., & Schafer, J. A. (2010). Threatened globally, acting locally: Modeling law enforcement homeland security practices. *Justice Quarterly*, *27*(1), 77-101.

Campbell, D. T., & Stanley, J. C. (2015). *Experimental and quasi-experimental designs for research*. Ravenio Books.

Canter, D. V., & Gregory, A. (1994). Identifying the residential location of rapists. *Journal of the Forensic Science Society*, *34*(3), 169-175.

Canter, D., & Hammond, L. (2006). A comparison of the efficacy of different decay functions in geographical profiling for a sample of US serial killers. *Journal of Investigative Psychology and Offender Profiling*, *3*(2), 91-103.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28-38.

Casey, E. (2012). Cyberpatterns: Criminal behavior on the Internet. In *Criminal Profiling: An Introduction to Behavioral Evidence Analysis.* (pp. 361-378). Burlington, MA: Elsevier Ltd.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2009). Information security control resources in organizations: A multidimensional view and their key drivers. *working paper, Sauder School of Business, University of British Columbia*.

Chan, H. C., Heide, K. M., & Beauregard, E. (2011). What propels sexual murderers: A proposed integrated theory of social learning and routine activities

theories. *International Journal of Offender Therapy and Comparative Criminology*, *55*(2), 228-250.

Chang, L. Y. (2013). Formal and informal modalities for policing cybercrime across the Taiwan Strait. *Policing and Society*, *23*(4), 540-555.

Charoen, D., Raman, M., & Olfman, L. (2008). Improving end user behavior in password utilization: An action research initiative. *Systemic Practice and Action Research*, *21*(1), 55-72.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning & Performance Journal*, *24*(1).

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

Choi, K. S. (2015). *Cybercriminology and digital investigation* (p. 340). El Paso, TX: LFB Scholarly Publishing.

Choi, K. S., Choo, K., & Sung, Y. E. (2016). Demographic variables and risk factors in computer-crime: an empirical assessment. *Cluster Computing*, *19*(1), 369-377.

Choi, K. S., Scott, T. M., & LeClair, D. P. (2016). Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *International Journal of Forensic Science & Pathology*.

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402.

Clarke, R. V. (1995). Situational crime prevention. *Crime and justice*, *19*, 91-150.

Clarke, R. V. G. (Ed.). (1997). *Situational crime prevention* (pp. 225-256). Monsey, NY: Criminal Justice Press.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and justice*, *6*, 147-185.

Clarke, R. V. and Cornish, D. B. (2001). Rational choice. In R. Paternoster & R. Bachman (Eds.), Explaining criminals and crime: Essays in contemporary criminological theory (pp. 23–42). New York, NY: Oxford University Press.

Clarke, R. V., & Eck, J. E. (2005). Crime analysis for problem solvers. *Washington, DC: Center for Problem Oriented Policing*.

Clarke, R. V. G., & Felson, M. (Eds.). (1993). *Routine activity and rational choice* (Vol. 5). Transaction publishers.

Cockbain, E., & Laycock, G. (2017). Crime science. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*.

Cohen, J. (1992). A power primer. *Psychological bulletin*, *112*(1), 155.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*. *44,* 588-608.

Cohen, L. E., & Felson, M. (2016). Social Change and Crime Rate Trends: A Routine Activity Approach (1979). In *Classics in Environmental Criminology* (pp. 203-232). Boca Raton, FL: CRC Press.

Cohen, L. E., Felson, M., & Land, K. C. (1980). Property crime rates in the United States: A macrodynamic analysis, 1947-1977; with ex ante forecasts for the mid-1980s. *American journal of Sociology*, *86*(1), 90-118.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, 505-524.

Computer misuse act 1990 (2018, July 5). In *Legislation.gov.uk*. Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/contents

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security*, *26*(1), 63-72.

Cornish, D. B. (1993). Theories of action in criminology: Learning theory and rational choice approaches. *Routine activity and rational choice*, *5*, 351-382.Cornish, D., & Clarke, R., (2002). Analyzing organized crimes. In: Piquero, Alexis, Tibbetts, Stephen (Eds.), Rational Choice and Criminal Behavior. London: Routledge.

Cornish, D., & Clarke, R. (2008). The rational choice perspective. *Environmental criminology and crime analysis*, *21*, 21-47.

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology*, *44*(2), 431-464.

Cozens, P., & Grieve, S. (2014). Situational crime prevention at nightclub entrances in Perth, Western Australia: Exploring micro-level crime precipitators. *Crime prevention and community safety*, *16*(1), 54-70.

Cromwell, P. F., & Olson, J. N. (2004). *Breaking and entering: Burglars on burglary*. Thomson: Wadsworth.

Cumming, G., Fidler, F., & Vaux, D. L. (2007). Error bars in experimental biology. *The Journal of cell biology*, *177*(1), 7-11. Curran, P. J., & Hussong, A. M. (2009). Integrative data analysis: The simultaneous analysis of multiple data sets. *Psychological methods*, *14*(2), 81.

Danner, T. A. (2003). Violent times: a case study of the Ybor City Historic District. *Criminal Justice Policy Review*, *14*(1), 3-29.

Dasgupta, D., Ferebee, D. M., & Michalewicz, Z. (2013, October). Applying puzzle-based learning to cyber-security education. In *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference* (p. 20). ACM.

Davies, A., Wittebrood, K., & Jackson, J. L. (1998). *Predicting the criminal record of a stranger rapist*. London, UK: Home Office, Policing and Reducing Crime Unit.

De Coster, S., Estes, S. B., & Mueller, C. W. (1999). Routine activities and sexual harassment in the workplace. *Work and Occupations*, *26*(1), 21-49.

Dlamini, Z., & Modise, M. (2013). Cyber security awareness initiatives in South Africa: a synergy approach. *Case Stud. Inf. Warf. Secur. Res. Teach. Stud*, *1*.

Denning, D. E. R. (1999). *Information warfare and security* (Vol. 4). Reading, MA: Addison-Wesley.

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013, November). Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 915-928). ACM.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *computers & security*, *26*(1), 73-80.

Douglas, J. E., & Burgess, A. E. (1986). Criminal profiling: A viable investigative tool against violent crime. *FBI L. Enforcement Bull.*, *55*, 9.

Douglas, J. E., Ressler, R. K., Burgess, A. W., & Hartman, C. R. (1986). Criminal profiling from crime scene analysis. *Behavioral Sciences & the Law*, *4*(4), 401-421.

Dowden, C., Bennell, C., & Bloomfield, S. (2007). Advances in offender profiling: A systematic review of the profiling literature published over the past three decades. *Journal of Police and Criminal Psychology*, *22*(1), 44.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, *26*(1), 36-43.

Earls, C. M., & Marshall, W. L. (1983). The current state of technology in the laboratory assessment of sexual arousal patterns. *The sexual aggressor: Current perspectives on treatment*, 336-362.

Eastin, M. S., & LaRose, R. (2000). Internet self-efficacy and the psychology of the digital divide. *Journal of computer-mediated communication*, *6*(1), JCMC611.

Eck, J. E. (1994). Drug markets and drug places. *Unpublished PhD dissertation, University of Maryland, College Park, MD.*

Eck, J.E. (2002). Preventing crime at places. In Sherman, Farrington, Welsh, & MacKenzie (Eds.), Evidence-Based crime prevention. (pp. 241-94).

Eck, J. E., & Guerette, R. T. (2012). Place-based crime prevention: Theory, evidence, and policy. *The Oxford handbook of crime prevention*, (pp. 354-383). New York, NY: Oxford University Press.

Eck, J. E., & Weisburd, D. L. (2015). Crime places in crime theory. In Crime and Place, eds. Monsey, NY: Criminal Justice Press.

Economic espionage (2016). In U.S. Department of Justice. Retrieved from https://www.justice.gov/usam/usam-9-59000-economic-espionage

Ellis, P. D. (2010). *The essential guide to effect sizes: Statistical power, meta-analysis, and the interpretation of research results*. Cambridge University Press.

Emig, M. N., Heck, R. O., & Kravitz, M. (1980). Crime analysis--A selected bibliography. *Washington, DC: US National Criminal Justice Reference Service*.

Engel, M. S., de Vasconcelos Segundo, E. H., & Zannin, P. H. T. (2014). Statistical analysis of a combination of objective and subjective environmental noise data using factor analysis and multinomial logistic regression. *Stochastic environmental research and risk assessment*, *28*(2), 393-399.

Farrington, D. P., & Lambert, S. (1997). Predicting offender profiles from victim and witness descriptions.

Federal Bureau of Investigation. (1995). *Crime in the United States, 1994: Uniform crime reports*. Washington, DC: Department of Justice.

Felson, M. (1986). Routine activities, social controls, rational decisions and criminal outcomes. *The reasoning criminal*, 302-327.

Felson, M. (1987). Routine activities and crime prevention in the developing metro polis. *Criminology*, *25*(4), 911-932.

Felson, M. (1995). Those who discourage crime. *Crime and place*, *4*, 53-66.

Felson, M. (1998). Crime and everyday life: Insight and implications for society. Thousand Oaks, CA: Pine Forge Press.

Felson, M. (2017). Linking criminal choices, routine activities, informal control, and criminal outcomes. In *The reasoning criminal* (pp. 119-128). Routledge.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. *Police research series, paper*, *98*, 1-36.

Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk.* Albany, NY: SUNY press.

Flatt, C., & Jacobs, R. L. (2019). Principle Assumptions of Regression Analysis: Testing, Techniques, and Statistical Reporting of Imperfect Data Sets. *Advances in Developing Human Resources*, *21*(4), 484-502.

Foltz, B. C. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, 12, 154-166.

Foreman, J. (2004). Game-based learning: How to delight and instruct in the 21st century. *Educause Review*, *39*(5).

Furnell, S. M., Clarke, N., von Solms, R., Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*.

Geers, K. (2010). Cyber weapons convention. *Computer law & security review*, *26*(5), 547-551.

Gilmour, N. (2016). Understanding the practices behind money laundering–A rational choice interpretation. *International Journal of Law, Crime and Justice*, *44*, 1-13.

Godwin, M. (2002). Reliability, validity, and utility of criminal profiling typologies. *Journal of Police and Criminal Psychology*, *17*(1), 1.

Goetting, A. (1995). *Homicide in families and other special populations*. Springer Publishing Co.

Gondree M., Peterson Z. N., and Denning T., "Security through play," Secur. Priv. IEEE, vol. 11, no. 3, pp. 64–67, 2013.

Goulet, J. A. S., & Tardif, M. (2018). Exploring sexuality profiles of adolescents who have engaged in sexual abuse and their link to delinquency and offense characteristics. *Child abuse & neglect*, *82*, 112-123.

Grabosky, P. (2015). Keynotes in criminology and criminal justice series: Cybercrime. New York, NY: Oxford University Press.

Grabosky, P. N., & Smith, R. G. (2001). Digital crime in the twenty-first century. *Journal of information ethics*, *10*(1), 8.

Graney, D. J., & Arrigo, B. A. (2002). The power serial rapist. *Springfield, Illinois*.

Habibi, A., Mukminin, A., Riyanto, Y., Prasojo, L. D., Sulistiyo, U., Sofwan, M., & SAUDAGAR, F. (2018). Building an online community: Student teachers' perceptions on the advantages of using social networking services in a teacher education program. *Turkish Online Journal of Distance Education*, *19*(1), 46-61.

Hadzhidimova, L. I., & Payne, B. K. (2019). The profile of the international cyber offender in the US. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(1), 40-55.

Hagen, J., Albrechtsen, E., & Ole Johnsen, S. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security*, *19*(3), 140-154.

Halibozek, E., & Kovacich, G. L. (2017). *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann.

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford Publications.

Haynes, M. R., & Giblin, M. J. (2014). Homeland security risk and preparedness in police agencies: The insignificance of actual risk factors. *Police Quarterly*, *17*(1), 30-53.

Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology*, *7*(2), 155.

Hazelwood, R. R., & Warren, J. I. (2004). Linkage analysis: Modus operandi, ritual, and signature in serial sexual crime. Aggression and Violent Behavior, 9, 307–318.

Hicks, S. J., & Sales, B. D. (2006). *Criminal profiling: Developing an effective science and practice*. American Psychological Association.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant behavior*, *29*(2), 129-156.

Hirschfield, A. (2017). Analysis for intervention. In *Handbook of crime prevention and community safety*. New York, NY: Routledge.

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety*, *15*(1), 65-79.

Holmberg, B. (2007). A theory of teaching-learning conversations. *Handbook of distance education*, *2*, 69-88.

Holmes, R. M., & Holmes, S. T. (2008). *Profiling violent crimes: An investigative tool*. Sage.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*(2), 165-177.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1-25.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436.

Holt, T. J., Burruss, G. W., & Bossler, A. (2015). *Policing cybercrime and cyberterror*. Durham, NC: Carolina Academic Press.

Holt, T. J., Lee, J. R., Liggett, R., Holt, K. M., & Bossler, A. (2019). Examining perceptions of online harassment among constables in England and Wales. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(1), 24-39.

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Internet-based radicalization as enculturation to violent deviant subcultures. *Deviant behavior*, *38*(8), 855-869.

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime & Delinquency*, *58*(5), 798-822.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-22Hough M. (1987). Offenders' choice of target: Findings from victim surveys. *Journal of Quantitative Criminology*, *3*(4), 355-369.

Hsu, M. H., & Chiu, C. M. (2004). Internet self-efficacy and electronic service acceptance. *Decision support systems*, *38*(3), 369-381.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'Net'?. *Current Issues in Criminal Justice*, *20*(3), 433-452.

Internet Crime Complaint Center. 2001. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2001_IC3Report.pdf

Internet Crime Complaint Center. 2002. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2002_IC3Report.pdf

Internet Crime Complaint Center. 2003. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2003_IC3Report.pdf

Internet Crime Complaint Center. 2004. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2004_IC3Report.pdf

Internet Crime Complaint Center. 2005. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2005_IC3Report.pdf

Internet Crime Complaint Center. 2006. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2006_IC3Report.pdf

Internet Crime Complaint Center. 2007. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2007_IC3Report.pdf

Internet Crime Complaint Center. 2008. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2008_IC3Report.pdf

Internet Crime Complaint Center. 2009. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2009_IC3Report.pdf

Internet Crime Complaint Center. 2010. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2010_IC3Report.pdf

Internet Crime Complaint Center. 2011. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2011_IC3Report.pdf

Internet Crime Complaint Center. 2012. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2012_IC3Report.pdf

Internet Crime Complaint Center. 2013. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2013_IC3Report.pdf

Internet Crime Complaint Center. 2014. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2014_IC3Report.pdf

Internet Crime Complaint Center. 2015. Internet Crime Report. Retrieved June 27, 2016, from https://pdf.ic3.gov/2015_IC3Report.pdf

Internet Crime Complaint Center. 2016. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf

Internet Crime Complaint Center. 2017. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

Internet Crime Complaint Center. 2018. Internet Crime Report. Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf

Internet Security Threat Report (2015). In *Symantec Corporation*. Retrieved from https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Irvine, C. E., & Thompson, M. (2003). *Teaching objectives of a simulation game for computer security*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Jackson, J. L., van den Eshof, P., & de Kleuver, E. E. (1997). A research approach to offender profiling.

Jacobs, J. (1961). 1 961, The Death and Life of Great American Cities. *New York: Vintage*.

Jahankhani, H., & Al-Nemrat, A. (2012). Examination of cyber-criminal behaviour. *International Journal of Information Science and Management (IJISM)*, 41-48.

James, G. (2002). Advantages and disadvantages of online learning. *Retrieved July*, *1*, 2006.

Jansen, R., & Van Koppen, P. (1998). The road to robbery. *Br J Criminol*, *38*(2), 230-246.

Jeffery, C. R. (1971). *Crime prevention through environmental design* (Vol. 91). Beverly Hills, CA: Sage Publications.

Junger, M., Laycock, G., Hartel, P., & Ratcliffe, J. (2012). Crime science: editorial statement. *Crime Science*, *1*(1), 1-3.

Kayali, F., Wallner, G., Kriglstein, S., Bauer, G., Martinek, D., Hlavacs, H., ... & Wölfle, R. (2014, April). A case study of a learning game about the Internet. In *International Conference on Serious Games* (pp. 47-58). Springer, Cham.

Kennedy, L. W., Caplan, J. M., & Piza, E. (2011). Risk clusters, hotspots, and spatial intelligence: risk terrain modeling as an algorithm for police resource allocation strategies. *Journal of Quantitative Criminology*, *27*(3), 339-362.

Kennedy, L. W., & Forde, D. R. (1990). Routine activities and crime: An analysis of victimization in Canada. *Criminology*, *28*(1), 137-152.

Kim, E. B. (2013). Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective*, *22*(4), 171-179.

Kirtman, L. (2009). Online versus in-class courses: An examination of differences in learning outcomes. *Issues in Teacher Education*, *18*(2), 103-116.

Kirwan, G. (Ed.). (2011). *The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles*. Igi Global.

Kirwan, G., & Power, A. (2011). The psychology of cybercrime. *Pennsylvania: IGI Global Press. Crossref*.

Kirwan, G., & Power, A. (2013). Cybercrime: Psychology of cybercrime. *Dublin: Dun Laoghaire Institute of Art, Design and Technology*.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840-847.

Kubic, T. (2001). The FBI's perspective on the cybercrime problems. *Before the House Committee on the Judiciary, Subcommittee on Crime of the Federal Bureau of Investigation*. Retrieved from https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish: A Real-Word Evaluation of Anti-Phishing Training (Cmu-Cylab-09-002).

Kwan, L., Ray, P., & Stephens, G. (2008, January). Towards a methodology for profiling cyber criminals. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 264-264). IEEE.

Labuschagne, W. A., Burke, I., Veerasamy, N., & Eloff, M. M. (2011, August). Design of cyber security awareness game utilizing a social media framework. In *2011 Information Security for South Africa* (pp. 1-9). IEEE. Lalumiere, M. L., & Quinsey, V. L. (1996). Sexual deviance, antisociality, mating effort, and the use of sexually coercive behaviors. *Personality and Individual differences*, *21*(1), 33-48.

Leclerc, B., Wortley, R., & Dowling, C. (2016). Situational precipitators and interactive forces in sexual crime events involving adult offenders. *Criminal justice and behavior*, *43*(11), 1600-1618.

Lee, S. S., Choi, K. S., Choi, S., & Englander, E. (2019). A Test of Structural Model for Fear of Crime in Social Networking Sites. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 5-22.

Lee, J. R., & Downing, S. (2019). An Exploratory Perception Analysis of Consensual and Nonconsensual Image Sharing. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 23-43.

Lesik, S. A. (2008). Studying the effectiveness of programs and initiatives in higher education using the regression-discontinuity design. In *Higher Education* (pp. 277-297). Springer, Dordrecht.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. L. (2016). The implications of economic cybercrime for policing.

Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies.*

Lewis, J. A. (2018, February 21). Economic impact of cybercrime: No slowing down. In *Center for Strategic & International Studies*. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime

Lewis-Beck, M., Bryman, A. E., & Liao, T. F. (2003). *The Sage encyclopedia of social science research methods*. Sage Publications.

Lussier, P., Proulx, J., & LeBlanc, M. (2005). Criminal propensity, deviant sexual interests and criminal activity of sexual aggressors against women: A comparison of explanatory models. *Criminology*, *43*(1), 249-282.

Madensen, T. D. (2007). *Bar management and crime: Toward a dynamic theory of place management and crime hotspots* (Doctoral dissertation, University of Cincinnati).

Madensen, T. D., & Eck, J. E. (2013). Crime places and place management. In *The Oxford handbook of criminological theory.* New York, NY: Oxford University Press.

Madero-Hernandez, A., & Fisher, B. S. (2012). Routine activity theory. In *The Oxford handbook of criminological theory*.

Malamuth, N. M. (1998). The confluence model as an organizing framework for research on sexually aggressive men: Risk moderators, imagined aggression, and pornography consumption. In *Human aggression* (pp. 229-245). Academic Press.

Maness, R., Valeriano, B., & Jensen, B. (2019). The dyadic cyber incident and campaign (DCID) dataset, version 1.5. Retrieved from http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf

Mani, D., Raymond Choo, K. K., & Mubarak, S. (2014). Information security in the South Australian real estate industry: A study of 40 real estate organizations. *Information Management & Computer Security*, *22*(1), 24-41.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cyber crime. *International Journal of Police Science & Management*, *12*(4), 516-525.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal justice review*, *35*(4), 412-437.

Marshall, W. L. (1988). The use of sexually explicit stimuli by rapists, child molesters, and nonoffenders. *Journal of Sex Research*, *25*(2), 267-288.

Marshall, W. L., & Barbaree, H. E. (1990). An integrated theory of the etiology of sexual offending. In *Handbook of sexual assault* (pp. 257-275). Springer, Boston, MA.

Massey, J. L., Krohn, M. D., & Bonati, L. M. (1989). Property crime and the routine activities of individuals. *Journal of Research in Crime and Delinquency*, *26*(4), 378-400.Maxwell, S. E. (2004). The persistence of underpowered studies in psychological research: causes, consequences, and remedies. *Psychological methods*, *9*(2), 147.

Mazerolle, L. G., Kadleck, C., & Roehl, J. (1998). Controlling drug and disorder problems: The role of place managers. *Criminology*, *36*(2), 371-404.

Mazerolle, L., & Ransley, J. (2006). *Third party policing*. New York, NY: Cambridge University Press.

Mazerolle, L. G., & Roehl, J. (1998). *Civil remedies and crime prevention* (Vol. 9). Monsey, NY: Criminal Justice Press.

McCrory, R., Putnam, R., & Jansen, A. (2008). Interaction in online courses for teacher education: Subject matter and pedagogy. *Journal of Technology and Teacher Education*, *16*(2), 155-180.

McGrath, M. G., & Casey, E. (2002). Forensic psychiatry and the internet: practical perspectives on sexual predators and obsessional harassers in cyberspace. *Journal of the American Academy of Psychiatry and the Law Online*, *30*(1), 81-94.

Meldrum, R. C., Boman, J. H., & Back, S. (2019). Low Self-Control, Social Learning, and Texting while Driving. *American Journal of Criminal Justice*, *44*(2), 191-210.

Menchaca, M. P., & Bekele, T. A. (2008). Learner and instructor identified success factors in distance education. *Distance education*, *29*(3), 231-252.

Messner, S. F., & Tardiff, K. (1985). The social ecology of urban homicide: An application of the "routine activities" approach. *Criminology*, *23*(2), 241-267.

Mieczkowski, T., & Beauregard, E. (2010). Lethal outcome in sexual assault events: A conjunctive analysis. *Justice Quarterly*, *27*(3), 332-361.

Miethe, T. D., & McDowall, D. (1993). Contextual effects in models of criminal victimization. *Social Forces*, *71*(3), 741-759.

Miethe, T. D., Stafford, M. C., & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/lifestyle theories. *American Sociological Review*, 184-194.

Mokros, A., & Alison, L. J. (2002). Is offender profiling possible? Testing the predicted homology of crime scene actions and background characteristics in a sample of rapists. *Legal and Criminological Psychology, 7*(1), 25-43.

Monyai, S., Lesaoana, M., Darikwa, T., & Nyamugure, P. (2016). Application of multinomial logistic regression to educational factors of the 2009 General Household Survey in South Africa. *Journal of Applied Statistics*, *43*(1), 128-139.

Moreto, W. D. (2019). Provoked poachers? Applying a situational precipitator framework to examine the nexus between human-wildlife conflict, retaliatory killings, and poaching. *Criminal Justice Studies*, *32*(2), 63-80.

Morgan, R., Maguire, M., & Reiner, R. (Eds.). (2012). *The Oxford handbook of criminology*. Oxford University Press.

Morselli, C., & Royer, M. N. (2008). Criminal mobility and criminal achievement. *Journal of Research in Crime and Delinquency*, *45*(1), 4-21.

Moteff, J., & Parfomak, P. (2004, October). Critical infrastructure and key assets: definition and identification. Library of Congress Washington DC Congressional Research Service.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology, 36*(4), 829-858.

Nachreiner, C. (2015). Signature antivirus' dirty little secret. *HelpNet Security*.

Newman, O., & National Institute of Law Enforcement and Criminal Justice. (1973). *Architectural design for crime prevention* (pp. 2700-00161). Washington, DC: National Institute of Law Enforcement and Criminal Justice.

Newman, G. R. and Clarke, R. V. (2003). Superhighway Robbery: Preventing E-Commerce Crime. Devon, UK: Willan Publishing.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1).

Nyeste, P. G., & Mayhorn, C. B. (2010, September). Training users to counteract phishing. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 54, No. 23, pp. 1956-1960). Sage CA: Los Angeles, CA: SAGE Publications.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Review*, *21*(5), 408-414.

Osgood, D. W., Wilson, J. K., O'malley, P. M., Bachman, J. G., & Johnston, L. D. (1996). Routine activities and individual deviant behavior. *American Sociological Review*, 635-655.

Ouimet, M., & Proulx, J. (1994, November). Spatial and temporal behavior of pedophiles: Their clinical usefulness as to the relapse prevention model. In *46th Annual Conference of the American Society of Criminology, Miami, FL*.

Overview of Florida International University (2019). In *US News*. Retrieved from https://www.usnews.com/best-colleges/fiu-9635

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, *22*(4), 334-345.

Pastor, V., Díaz, G., & Castro, M. (2010, April). State-of-the-art simulation systems for information security education, training and awareness. In *IEEE EDUCON 2010 Conference* (pp. 1907-1916). IEEE.Piazza, P. (2006). Security goes to school. *Security Management*, *50*(12), 46-51.

Pelfrey Jr, W. V. (2007). Local law enforcement terrorism prevention efforts: A state level case study. *Journal of Criminal Justice*, *35*(3), 313-321.

Peng, C. Y. J., & Nichols, R. N. (2003). Using multinomial logistic models to predict adolescent behavioral risk. *Journal of Modern Applied Statistical Methods*, *2*(1), 16.

Piazza, P. (2006). Security goes to school. *Security Management*, *50*(12), 46-51.

Pires, S. F., Guerette, R. T., & Stubbert, C. H. (2014). The crime triangle of kidnapping for ransom incidents in Colombia, South America: A 'Litmus' test for situational crime prevention. *British Journal of Criminology*, *54*(5), 784-808.

Pollitt, M. M. (1998). Cyberterrorism—fact or fancy?. *Computer Fraud & Security*, *1998*(2), 8-10.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Prentky, R. A., Burgess, A. W., Rokous, F., Lee, A., Hartman, C., Ressler, R., & Douglas, J. (1989). The presumptive role of fantasy in serial sexual homicide. *American journal of Psychiatry*, *146*(7), 887-891.

Pyle, G. F., Hanten, E. W., Williams, P. G., Pearson, A., & Doyle, J. G. (1974). *The spatial dynamics of crime* (Vol. 159). Chicago, IL: University of Chicago, Department of Geography.

Pyrooz, D. C., Decker, S. H., & Moule Jr, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, *32*(3), 471-499.

Rader, N. E., May, D. C., & Goodrum, S. (2007). An empirical assessment of the "threat of victimization:" Considering fear of crime, perceived risk, avoidance, and defensive behaviors. *Sociological Spectrum*, *27*(5), 475-505.

Randol, B. M. (2012). The organizational correlates of terrorism response preparedness in local police departments. *Criminal justice policy review*, *23*(3), 304-326.

Randolph, J. J., Falbe, K., Manuel, A. K., & Balloun, J. L. (2009). Practical assessment, research & evaluation. *Practical Assessment, Research, & Evaluations*, *14*(13), 1-13.

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, *21*(6), 328-345.

Rauma, D., & Berk, R. A. (1987). Remuneration and recidivism: The long-term impact of unemployment compensation on ex-offenders. *Journal of Quantitative Criminology*, *3*(1), 3-27.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior*, *36*(4), 369-384.

Rengert, G. F., Piquero, A. R., & Jones, P. R. (1999). Distance decay reexamined. *Criminology*, *37*(2), 427-446.

Rengifo, A. F., & Bolton, A. (2012). Routine activities and fear of crimes: Specifying individual-level mechanisms. *European Journal of Criminology*, *9*(2), 99-119.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), 99-118.

Report of the Attorney General's Cyber Digital Task Force (2018, July 2). In *U.S. Department of Justice*. Retrieved from https://www.justice.gov/ag/page/file/1076696/download

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396-411.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine

activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior*, *38*(11), 1149-1169.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7-8), 241-253.

Riegg, S. K. (2008). Causal inference and omitted variable bias in financial aid research: Assessing solutions. *The Review of Higher Education*, *31*(3), 329-354.

Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261-273.

Rhodes, W. M., & Conly, C. (1981). *Analysis of federal sentencing*. Department of Justice.

Roberts, J. C. (2007). Barroom aggression in Hoboken, New Jersey: don't blame the bouncers!. *Journal of Drug Education*, *37*(4), 429-445.

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security*, *22*(4), 292-298.

Roncek, D. W., & Maier, P. A. (1991). Bars, blocks, and crimes revisited: Linking the theory of routine activities to the empiricism of "hot spots". *Criminology*, *29*(4), 725-753.

Rossmo, D. K., & Velarde, L. (2008). Geographic profiling analysis: principles, methods and applications. *Crime mapping case studies: Practice and research*, 35-43.

Rountree, P. W., & Land, K. C. (1996). Burglary victimization, perceptions of crime risk, and routine activities: A multilevel analysis across Seattle neighborhoods and census tracts. *Journal of research in crime and delinquency*, *33*(2), 147-180.

Ryan, J. (2007). Information security awareness: an evaluation among business students with regard to computer self-efficacy and personal innovation. *AMCIS 2007 Proceedings*, 251.

Safarik, M. E., Jarvis, J., & Nussbaum, K. (2000). Elderly female serial sexual homicide: A limited empirical test of criminal investigative analysis. *Homicide Studies*, *4*(3), 294-307.

Salfati, C. G. (2000). The nature of expressiveness and instrumentality in homicide: Implications for offender profiling. *Homicide Studies*, *4*(3), 265-293.

Salkind, N. J. and Rasmussen, K. (2007). Encyclopedia of Measurement and Statistics. 1, London: SAGE Publications, Inc.

Sarangi, S., & Youngs, D. (2006). Spatial patterns of Indian serial burglars with relevance to geographical profiling. *Journal of Investigative Psychology and Offender Profiling*, *3*(2), 105-115.

Scams and safety (2016). In *Federal Bureau of Investigation*. Retrieved from https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud

Schafer, J. A., Huebner, B. M., & Bynum, T. S. (2006). Fear of crime and criminal victimization: Gender-based contrasts. *Journal of Criminal Justice*, *34*(3), 285-301.

Schmeeckle, J. M. (2003). Online training: An evaluation of the effectiveness and efficiency of training law enforcement personnel over the internet. *Journal of Science Education and Technology*, *12*(3), 205-260.

Schweitzer, D., & Brown, W. (2009). Using visualization to teach security. *Journal of Computing Sciences in Colleges*, *24*(5), 143-150.

Scott, M., Eck, J., Knutsson, J., & Goldstein, H. (2008). 12. Problem-oriented policing and environmental criminology. In *Environmental criminology and crime analysis*, UK: Willian Publishing, pp. 221-246.

Scott, D., Lambie, I., Henwood, D., & Lamb, R. (2006). Profiling stranger rapists: Linking offence behaviour to previous criminal histories using a regression model. *Journal of sexual aggression*, *12*(3), 265-275.

Shannon, D. (2008). Online sexual grooming in Sweden—Online and offline sex offences against children as described in Swedish police data. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *9*(2), 160-180.

Shaw, E. D. (2006). The role of behavioral research and profiling in malicious cyber insider investigations. *Digital investigation*, *3*(1), 20-31.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99). ACM.

Sherman, L. W. (1995). Hot spots of crime and criminal careers of places. *Crime and place*, *4*, 35-52.

Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology*, *27*(1), 27-56.

Shinder, D. L., & Cross, M. (2008). *Scene of the Cybercrime*. Elsevier.

Simon, T. (2017). Chapter seven: Critical infrastructure and the internet of things. *Cyber Security in a Volatile World*, *93*.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3-26.

Snook, B., Eastwood, J., Gendreau, P., Goggin, C., & Cullen, R. M. (2007). Taking stock of criminal profiling: A narrative review and meta-analysis. *Criminal Justice and Behavior*, *34*(4), 437-453.

Spelman, W., & Eck, J. E. (1989). *Sitting ducks, ravenous wolves and helping hands: New approaches to urban policing*. Austin, TX: Lyndon B. Johnson School of Public Affairs, University of Texas at Austin.

Stajkovic, A. D., & Luthans, F. (1998). Social cognitive theory and self-efficacy: Goin beyond traditional motivational and behavioral approaches. *Organizational dynamics*, *26*(4), 62-74.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, February). An analysis of information security awareness within home and work environments. In *2010 International Conference on Availability, Reliability and Security* (pp. 196-203). IEEE.

Taylor, R. W., Fritsch, E. J., Liederbach, J., Saylor, M. R., & Tafoya, W. L. (2019). *Cybercrime and cyber terrorism.* New York, NY: Pearson.

Tennakoon, H (2011). The need for a comprehensive methodology for profiling cyber-criminals. New Security Learning. Retrieved www. newsecuritylearning.com

Thyer, B. A. (2012). *Quasi-experimental research designs*. New York: Oxford University Press.

Tilley, N., & Sidebottom, A. (2017). *Handbook of crime prevention and community safety*. New York, NY: Routledge.

Torkzadeh, R., Pflughoeft, K., & Hall, L. (1999). Computer self-efficacy, training effectiveness and user attitudes: An empirical study. *Behaviour & Information Technology*, *18*(4), 299-309.

Trochim, W. (2001). Regression-discontinuity design. *International encyclopedia of the social and behavioral sciences*, *19*, 12940-12945.

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology*, *44*(1), 66-91.

Turvey, B. (1999). Criminal profiling: An introduction to behavioral evidence analysis. San Diego, CA: Academic Press.

Turvey, B. E. (Ed.). (2011). *Criminal profiling: An introduction to behavioral evidence analysis*. Academic press.

Ullman, S. E. (2007). A 10-year update of "Review and critique of empirical studies of rape avoidance". *Criminal justice and behavior*, *34*(3), 411-429.

Van Koppen, P. J., & De Keijser, J. W. (1997). Desisting distance decay: On the aggregation of individual crime trips. *Criminology*, *35*(3), 505-515.

Van Patten, I. T., & Delhauer, P. Q. (2007). Sexual homicide: A spatial analysis of 25 years of deaths in Los Angeles. *Journal of forensic sciences*, *52*(5), 1129-1141.

Walker, J. T., & Maddan, S. (2019). *Statistics in criminology and criminal justice*. Jones & Bartlett Learning.

Wall, D. (2001). S. Cybercrimes and the Internet. *WALL, David. S.(Ed.). Crime and the Internet. London: Routledge*, 1-17.

Warikoo, A. (2014). Proposed methodology for cybercriminal profiling. *Information Security Journal: A Global Perspective*, *23*(4-6), 172-178.

Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. *Criminal justice*, *4*(4), 451-489.

Warr, M. (2001). Crime and opportunity: A theoretical essay. *The process and structure of crime: Criminal events and crime analysis*, *9*, 65-94.

Weerman, F. M. (2003). Co-offending as Social Exchange. Explaining Characteristics of Co-offending. *British journal of criminology*, *43*(2), 398-416.

Weisburd, D. (1997). *Reorienting crime prevention research and policy: From the causes of criminality to the context of crime*. US Department of Justice, Office of Justice Programs, National Institute of Justice.

Welsh, B. C., & Farrington, D. P. (2014). *The Oxford handbook of crime prevention*. Oxford University Press.

Wilcox, R. R. (2003). *Applying contemporary statistical techniques*. Elsevier.

Wilcox, R. R. (2005). Trimmed means. Encyclopedia of statistics in behavioral science. Hoboken.

Wilcox, P., & Cullen, F. T. (2018). Situational Opportunity Theories of Crime. *Annual Review of Criminology*, *1*, 123-148.

Wilcox, P., Land, K. C., & Hunt, S. A. (2003). *Criminal circumstance: A dynamic multi-contextual criminal opportunity theory*. New York, NY: Aldine de Gruyter.

Wilcox, P., May, D. C., & Roberts, S. D. (2006). Student weapon possession and the "fear and victimization hypothesis": Unraveling the temporal order. *Justice Quarterly, 23*(4), 502-529.

Williams, F. P. (2009). *Statistical concepts for criminal justice and criminology*. Upper Saddle River, NJ: Pearson Prentice Hall.

Williams, M. L. (2016). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21-48.

Williams, M., & Levi, M. (2015). Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors. *Security Journal*, *28*(3), 252-271.

Wilsem, J. V. (2011). 'Bought it, but never got it's assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168-178.

Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437-453.Wittebrood, K., & Nieuwbeerta, P. (2000). Criminal victimization during one's life course: The effects of previous victimization and patterns of routine activities. *Journal of research in crime and delinquency*, *37*(1), 91-122.

Wood, E. (1961). Housing design: A social theory. *Ekistics*, *12*(74), 383-392.

Woodhams, J., & Toye, K. (2007). An empirical test of the assumptions of case linkage and offender profiling with serial commercial robberies. *Psychology, Public Policy, and Law*, *13*(1), 59.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings*, 31.

Wolfe, S. E., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2016). Routine cell phone activity and exposure to sext messages: Extending the generality of routine activity theory and exploring the etiology of a risky teenage behavior. *Crime & Delinquency*, *62*(5), 614-644.

Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal*, *14*(4), 63-82.

Wortley, R., Sidebottom, A., Tilley, N., & Laycock, G. (2018). *Routledge Handbook of Crime Science*. Routledge.

Wortley, R., & Townsley, M. (Eds.). (2016). *Environmental criminology and crime analysis*. Taylor & Francis.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.

Yu, S. (2013). Behavioral evidence analysis on Facebook: A test of cyber-profiling. *Defendologija, 16*(33), 19-30.

Zegiorgis, S. (2002). Writing Information Security Policies. *Technical Communication*, *49*(3), 357.

Zimmerman, D. W. (2011). Inheritance of properties of normal and non-normal distributions after transformation of scores to ranks. *Psicológica*, *32*(1), 65-85.

Zimmerman, G. M., & Vasquez, B. E. (2011). Decomposing the peer effect on adolescent substance use: Mediation, nonlinearity, and differential nonlinearity. *Criminology*, *49*(4), 1235-1273.

Note

1. Definitions of Key Terms for Cybercrime Typology

To better understand cybercrime typology, the top 10 types of cybercrime utilized over the 17 years need to be briefly discussed as the followings: 1) auction fraud, 2) non-delivery fraud, 3) Nigerian letter fraud, 4) credit/debit card fraud, 5) identity theft, 6) financial institution fraud, 7) FBI scams, 8) romance scams, 9) real estate fraud, and 10) ransomware scams.

"Auction fraud" is defined as "a fraudulent transaction or exchange that occurs in the context of an online auction site" (IC3, 2009, p. 17). "Non-delivery fraud" can be defined as an incident in which customers purchase goods in online markets, but they never receive it. "Nigerian letter fraud" is defined as an act in which Nigerian criminals send an unsolicited email message, in which the criminals give the recipient guarantee to obtain a vast amount of money. At the same time, the criminals request the recipient to transmit "an advance fee or offer identity, credit card or bank account information" (IC3, 2007, p.19). "Credit/debit card fraud" is defined as a fraudulent act that purposes to achieve anything of monetary gain via any unauthorized use of a credit/debit card. "Identity theft" is defined as an illicit behavior that steals some individual's identifying information: name, birth date, social security number, credit/debit card number, etc. (IC3, 2007). "Financial institution fraud" is defined as deviant behavior that is to defraud someone "to induce a business, an organization through misrepresentation of the truth or concealment of a material fact" (IC3, 2007, p. 19). As discussed previously, "FBI scams" is defined as a fraudulent act that is to request individual's money, identity information, etc. by criminals who exploit the FBI or government agents' name (IC3, 2007). "Romance scams" is defined as an act in which

perpetrators search individual targets on chat rooms, dating sites, and social networking sites, and these criminals request victims to transmit money for helping their severe hardships after a building-up relationship or companionship (IC3, 2013). “Real estate fraud” is defined as a fraudulent act in which perpetrators exploit information from legal ads and post this information on online advertising sites to attract potential victims; then these criminals usually ask victims to send money overseas for purchasing houses (IC3, 2013). “Ransomware scams” is defined as an act in which perpetrators send the virus to encrypt computer database and files, and after encrypting these, they extort funds from victims by intimidating them (IC3, 2013).

Appendix A

Studies of Criminological Theories and Cybercrime

Authors/Theory	Variables	Design/Data	Conclusion	Authors/Theory	Variables	Design/Data	Conclusion
Al-Nemrat (2010)/Routine activity theory (RAT)	DVs: Cybercrime victimization (multiple types) IVs: Digital guardian (formal/informal social control/target hardening/awareness); Online exposure	Quantitative research approach; Confirmatory factor analysis;	Formal social control and awareness (impact); Online exposure (+) → Victim (+);	Choi (2008)/ Lifestyle-routine activity theory (L-RAT)	DVs: Computer-crime victimization IVs: Digital guardian; Online lifestyle	Cross-sectional research design; Structural equation model; Student population	Digital guardian (+) → Victim (-); Adequate online lifestyle (+) → Victim (-)
Arntfield (2015)/ RAT	DVs: Cyberbullying victimization IVs: Social media environment; Capable guardian	Exploratory study	Conceptualization	Choi & Lee (2017)/Cyber-routine activity theory (Cyber-RAT)	DVs: Cyber-interpersonal violence victimization IVs: Digital guardian; Online lifestyle	Cross-sectional research design; Logistic regression; Student population	Digital guardian (-) → Victim (+); Risky online behavior (+) → Victim (+)
Back (2016)/ RAT	DVs: Cyber-harassment victimization IVs:	Cross-sectional research design; Population	Digital guardian (-) → Victim (+); Risky online behavior (+) → Victim (+)	Choi et al. (2016)/Cyber-RAT	DVs: Ransomware victimization IVs:	Exploratory study; Ordinary least squares (OLS) regression;	Digital guardian (+) → Victim (-); Adequate online

	Digital guardian (target hardening); Risky online behavior	(aged 15 and older)	
Bossler & Holt (2009)/ RAT	DVs: Malware victimization IVs: Digital guardian (target hardening); Risky online behavior; Online exposure	Cross-sectional research design; Logistic regression; Student population	Digital guardian (no impact); Risky online behavior (+) → Victim (+); Online exposure (+) → Victim (+)

	Digital guardian; Online lifestyle	Police agencies	lifestyle (+) → Victim (-)
Holt & Bossler (2009)/L-RAT	DVs: Cyber-harassment victimization IVs: Digital guardian (physical guardian; social guardian); Risky online behavior	Cross-sectional research design; Logistic regression; Student population	Social guardian (-) → Victim (+); Physical guardian (no impact); Risky online behavior (+) → Victim (+); Online exposure (no impact)

Continued

Authors/Theory	Variables	Design/Data	Conclusion	Authors/Theory	Variables	Design/Data	Conclusion
Holt & Bossler (2013)/RAT	DVs: Malware victimization IVs: Digital guardian (target hardening); Risky online behavior; Online exposure	Cross-sectional research design; Logistic regression; Student population	Digital guardian (mixed results); Risky online behavior (+) → Victim (+); Online exposure (no impact)	Leukfeldt (2014)/RAT	DVs: Phishing victimization IVs: Financial characteristics; Online exposure; Antivirus software; Computer knowledge; Online risk perception	Cross-sectional research design; Structural equation model	Financial characteristics (no impact); Online exposure (no impact); Antivirus software (no impact); Computer knowledge/Online risk perception (no impact)
Holtfreter et al. (2008)/L-RAT; Self-control	DVs: Fraud victimization IVs: Remote purchasing; Low self-control	Cross-sectional research design; Logistic regression	Remote purchasing (+) → Victim (+); Low self-control (no impact)	Leukfeldt & Yar (2016)/RAT	DVs: 6 types of cybercrime victimization IVs: Value; Visibility; Technical guardian; Personal guardian	Cross-sectional research design; Multivariate analysis; Sample (21,800 citizens aged 15 years and older)	Value (+) → Malware victim (+); Visibility (+) → Hacking/malware/stalking victim (+); Technical guardian (no impact); Personal guardian (+) → Hacking (-)
Hutchings & Hayes (2008)/RAT	DVs: Phishing victimization	Cross-sectional research design;	Email filters (+) → Victim (-); Internet use (no impact); Internet	Marcum et al. (2010)/RAT	DVs:	Cross-sectional research design;	Online exposure (+) → Victim (+);

	IVs: Email filters; Internet use; Internet banking	Logistic regression;	banking (+) → Victim (+)		Cyber-harassment victimization IVs: Online exposure; Target suitability; Protective software	Logistic regression; Sample (744 college students)	Target suitability (+) → Victim (+); Protective software (no impact)
Kigerl (2012)/RAT	DVs: Spam rate; Phishing rate IVs: Percent Internet users; Unemployment ; GDP per capita	Exploratory study; Negative binomial regression	Internet users (+) → Spam/phishing (no impact); Unemployment (no impact on spam/phishing victim) GDP (+)→Spam/phishing victim (-)	Marcum et al. (2010)/RAT	DVs: Cyberbullying victimization IVs: Online exposure; Parental mediation	Cross-sectional research design; Logistic regression; Sample (935 teens ages 12-17 years)	Online exposure (+) → Victim (+); Parental mediation (mixed results)

Continued

Authors/Theory	Variables	Design/Data	Conclusion	Authors/Theory	Variables	Design/Data	Conclusion
Navarro & Jasinski (2012)/RAT	DVs: Cybercrime victimization (multiple types) IVs: Digital guardian (formal/informal/social control/target hardening/awareness); Online exposure	Quantitative research approach; Confirmatory factor analysis	Formal social control and awareness (impact); Online exposure (+) → Victim (+)	Reyns (2015)/RAT	DVs: Phishing/hacking/malware victimization IVs: Online guardian; Online exposure; Online target suitability	Cross-sectional research design; Logistic regression; Sample (19,422 households)	Online exposure (+) → Victim (+); Online guardian/online target suitability (mixed results)
Pratt et al. (2010)/RAT	DVs: Internet fraud victimization IVs: Routine online activities; Personal characteristics	Cross-sectional research design; Logistic regression; Sample (922 adults)	Routine online activities (+) → Victim (+); Personal characteristics (no impact)	Reyns & Henson (2016)/RAT	DVs: Identity theft victimization IVs: Online exposure; Online proximity; Online target suitability; Online guardian (target harderning)	Cross-sectional research design; Logistic regression; Sample (19,422 citizens aged 15 years or older)	Online exposure (+) → Victim (+); Online proximity (+) → Victim (+); Online target suitability (+) → Victim (+); Digital guardian (-) → Victim (+)
Pyrooz et al. (2015)/RAT	DVs: Crime and deviance online IVs:	Cross-sectional research design; Logistic regression; Sample (418	Internet use (impact); Social network use (impact);	Reyns et al. (2011)/ Cyber lifestyle-RAT	DVs: Cyberstalking victimization IVs:	Exploratory study; Logistic regression; Sample (974	Online exposure/proximity (weakest effect) Online target suitability/guar

	Internet use; Social network use; Technological capacity	current and former gang members)	Technological capacity (no impact)		Online exposure; Online proximity; Online target suitability; Online guardian; Online deviance	college students)	dian (moderate effect) Online deviance (strongest effect)
Reyns (2013)/RAT	DVs: ID theft victimization IVs: Online routine activities; Individual characteristics; perceived risk of victimization on identity theft	Cross-sectional research design; Logistic regression; Sample (5,985 citizens)	Online routine activities (+) → Victim (+); Individual characteristics (impact); Perceived risk of victim (+) → Victim (+)	Reyns et al. (2016)/RAT	DVs: Cyberstalking victimization IVs: Guardianship (offline and online); Online target hardening	Cross-sectional research design; Logistic regression; Sample (850 college students)	Offline/online guardian (no impact); Online target hardening (+) → Victim (-)

Continued

Authors/Theory	Variables	Design/Data	Conclusion	Authors/Theory	Variables	Design/Data	Conclusion
Navarro & Jasinski (2012)/RAT	DVs: Cybercrime victimization (multiple types) IVs:	Quantitative research approach; Confirmatory factor analysis	Formal social control and awareness (impact); Online exposure	Reyns (2015)/RAT	DVs: Phishing/hacking/malware victimization IVs:	Cross-sectional research design; Logistic regression; Sample	Online exposure (+) → Victim (+); Online guardian/online target

	Digital guardian (formal/informal/social control/target hardening/awareness); Online exposure		(+) → Victim (+)		Online guardian; Online exposure; Online target suitability	(19,422 households)	suitability (mixed results)
Pratt et al. (2010)/RAT	DVs: Internet fraud victimization IVs: Routine online activities; Personal characteristics	Cross-sectional research design; Logistic regression; Sample (922 adults)	Routine online activities (+) → Victim (+); Personal characteristics (no impact)	Reyns & Henson (2016)/RAT	DVs: Identity theft victimization IVs: Online exposure; Online proximity; Online target suitability; Online guardian (target harderning)	Cross-sectional research design; Logistic regression; Sample (19,422 citizens aged 15 years or older)	Online exposure (+) → Victim (+); Online proximity (+) → Victim (+); Online target suitability (+) → Victim (+); Digital guardian (-) → Victim (+)
Pyrooz et al. (2015)/RAT	DVs: Crime and deviance online IVs: Internet use; Social network use; Technological capacity	Cross-sectional research design; Logistic regression; Sample (418 current and former gang members)	Internet use (impact); Social network use (impact); Technological capacity (no impact)	Reyns et al. (2011)/ Cyberlifestyle-RAT	DVs: Cyberstalking victimization IVs: Online exposure; Online proximity; Online target suitability; Online guardian; Online deviance	Cross-sectional research design; Logistic regression; Sample (974 college students)	exposure/proximity (weakest effect) Online target suitability/guardian (moderate effect) Online deviance (strongest effect)

Reyns (2013)/RAT	DVs: ID theft victimization IVs: Online routine activities; Individual characteristics; perceived risk of victimization on identity theft	Cross-sectional research design; Logistic regression; Sample (5,985 citizens)	Online routine activities (+) → Victim (+); Individual characteristics (impact); Perceived risk of victim (+) → Victim (+)	Holt & Bossler (2009)/L-RAT	DVs: Cyber-threat victimization IVs: Offline routine activities; Digital routine activities; Low self-control; Online deviance	Cross-sectional research design; Multilevel multinomial regression; Sample (6,896 citizens aged 16 years or older)	Offline routine activities and digital routine activities (no impact); Low self-control (+) → Victim (+); Online deviance (+) → Victim (+)

Continued

Authors/Theory	Variables	Design/Data	Conclusion	Authors/Theory	Variables	Design/Data	Conclusion
Williams (2015)/RAT	DVs: Identity theft victimization IVs: Online routine activities; Capable guardianship; Physical guardianship	Cross-sectional research design; Multilevel Poisson regression; Sample (26,593 citizens)	Capable guardian (mixed findings); Physical guardian (+) → Victim (-); Online routine activities (+) → Victim (+)	Yar (2005)/ RAT	Value; Inertia; Visibility; Accessibility; Convergence in space and time of cyberspace	Exploratory study	Conceptualization
Wolfe et al. (2016)/RAT	DVs: Sexting victimization	Cross-sectional research design;	Exposure-based routine cell phone activities (+) → Victim				

<u>IVs:</u> Exposure-based routine cell phone activities; Supervision-based routine cell phone activities	Logistic regression; Sample (800 teenagers aged 12-17)	(+); Supervision-based routine cell phone activities (+) → Victim (+)

Appendix B

Studies of Cybersecurity Awareness Program

Authors	Type	Methods	Findings	Authors	Type	Methods	Findings
Kruger & Kearney (2006)	Web-based review/ brochures & company magazine/ posters	Vocabulary test	Effective	Kritzinger & von Solms (2010)	Conceptualization for information security awareness model	E-learning	Not applicable
Chen et al. (2006)	In-person lecture/ Online lecture	Pre-& post-experimental study	Mixed	Hagen et al. (2010)	E-learning	Pre-& post-experimental study/ survey-based questionnaire	Effective, but a need for repeated training for long-term effects
Drevin et al. (2007)	Value focused	Interview	Effective	Bulgurcu et al. (2010)	No cybersecurity awareness training	Survey-based questionnaire	Exploring users' attitude, normative beliefs, and self-efficacy for cybersecurity programs
Furnell et al. (2007)	Web-based training modules	Survey-based questionnaire	Ineffective	Labuschagne et al. (2011)	Interactive game hosted by social networking sites	Game tool	Development of a conceptual prototype
Albrechtsen (2007)	Mass-media based awareness campaigns/ user-involving approach	Interview	Mixed	Rantos et al. (2012)	No cybersecurity awareness training	Descriptive study	Development of a conceptual framework for cybersecurity awareness evaluations

Cone et al. (2007)	Interactive video game (CyberCIEGE)	Game evaluation tool	Effective	Furman et al. (2012)	No cybersecurity awareness training	Interview	Users' perceived risk of cyber-threats, attitude and awareness to cybersecurity
Charoen et al. (2007)	Focus group training	Survey-based questionnaire/ Interview	Effective	Kim (2013)	No cybersecurity awareness training	Kruskal-Wallis test	Users' perceived risk of cyber-threats, attitude and awareness to cybersecurity
Power (2007)	Web-based training modules	Survey-based questionnaire	Not available	Mani et al. (2013)	No cybersecurity awareness training	Survey-based questionnaire/ interview	Users' perceived risk of cyber-threats, attitude and awareness to cybersecurity
Rezgui & Marks (2008)	No cybersecurity awareness training	Survey-based questionnaire/ Observation/ Interview/ Document review	Recommend cybersecurity awareness program	Parsons et al. (2013)	No cybersecurity awareness training	Survey-based questionnaire	Users' perceived risk of cyber-threats, attitude and awareness to cybersecurity
Furnell et al. (2008)	No cybersecurity awareness training	Interview	Recommend cybersecurity awareness program	Caputo et al. (2014) Computer Science	Anti-Phishing Web-based training	Clicking on the phishing link	Ineffective
Kruger et al. (2010)	Web-based review/ 44	Vocabulary test	Effective	Kumaraguru et al. (2009)	Anti-Phishing Web-based training	Clicking on the phishing link	Effective

	university students			Computer Science			
Talib et al. (2010)	Web-based review/ brochures & company magazine/ posters	Survey-based questionnaire	Effective	Slusky & Navid (2012)	No cybersecurity awareness training	Survey-based questionnaire	Users' perceived risk of cyber-threats, attitude and awareness to cybersecurity

Studies on Evaluations of Gamification for Cybersecurity Awareness

Authors	Type	Methods	Findings	Authors	Type	Methods	Findings
Arachchilage & Love (2013) Computer Science	No cybersecurity awareness training	Pilot study/ Usability questionnaire	Effective	Gondree et al. (2013)	Mobile board game	Multi-player assessment (group study)	Effective, but need for more evaluation
Arachchilage & Love (2014)	No cybersecurity awareness training	Pilot study/ Usability questionnaire	Effective	Dasgupta et al. (2013)	Mobile puzzle game	Assessment based on Puzzles	Effective
Nyeste & Mayhorn (2010) Psychology	Anti-Phishing mobile gaming application: Training for links (URL) safety	Pre-& post-experimental study	Effective	Denning et al. (2013)	Web based review	Survey of teachers	Effective
Ariyapperuma & Minhas (2005)	Web based gaming applications	Review	Effective	Geers (2010)	Training exercise with virtual attackers and defenders	Review	Recommendations for improved IT infrastructure

Kayali et al. (2014)	Puzzle game	Experimental study	Effective	Pastor et al. (2010)	Multiple games	Review	Recommended developing and using more tools in games
Irvine & Thompson (2003)	Web based review	Review	Positive impacts of games with recommendations	Schweitzer & Brown (2009)	Visual presentation	Presentation (Education) case study	Positive experience of users in using interactive visualization
Sheng et al. (2007) Computer science	Anti-Phishing Training (game, reading online training)	Pre-& post-experimental study	Effective	Ryan (2007)	No cybersecurity awareness training	Survey-based questionnaire	Users' perceived risk of cyber-threats, attitude and awareness to cybersecurity

Appendix C

Cyber Criminal Profiles

Cybercriminal profiles	Motive	Structure	Motivation level	Skill level	Attack severity	Crime (or attack) method
Cyberstalking/Cyberbullying perpetrators	Entertainment/ personality disorder/ extortion	Unorganized	Low to high	Basic to intermediate	Low to medium	SNS/ hacking tools
Online sexual perpetrators	Entertainment/Personality disorder/ extortion	Unorganized	Medium to high	Basic to intermediate	Low to high	Child porn/ sexual solicitation
Online illegal trader	Monetary gain	Unorganized with some level of collaboration	Medium to high	Intermediate	Medium	Dark/ Crypto currency/ Hacking tools
Cybercrime syndicates	Monetary gain	Organized/ Well-funded	High	Intermediate to advanced	Medium to high	Phishing/ Spamming/ Malware
Hackers	Monetary gain/ Entertainment/	Unorganized with some level of collaboration	Medium	Highly advanced	Medium to high	Malware/ Botnet/ /DDoS/ Ransomware
Cyber spices	Espionage/ IP theft	State sponsored/ Highly organized/ Well-funded	High	Highly advanced	Critical	Customized codes/ Zero-day attacks/ Spyware
Cyber terrorists	Monetary gain/ Entertainment/ Political hacktivism	State sponsored/ Organized/ Well-funded/ Work in small modules	High	Highly advanced	Critical	Botnet/ Stuxnet/ DDoS/ Ransomware

Codebook Instructions for Cybercriminal Profiling

1.	Offender name	**e.g., Charles Edward**
2.	Offender sex	**If 0 = female, 1 = male**
3.	Offender age	Age of apprehension/trial **(e.g., 28)**
4.	Offender type	0 = individual cybercriminal 1 = hacking group (i.e., Anonymous group) 2 = organized cybercriminals (i.e., Mafia, Drug cartels, etc.) 3 = state-sponsored cybercriminals (i.e., hackers sponsored by Russian government or Chinese government, or North Korean government)
5.	Offender geo location/nationality	*City **(i.e., Maimi)** and state **(i.e., FL)** or Nationality **(i.e., Nigeria):*** **If 0 = USA; 1 = Argentina; 2 = Australia; 3 = Bangladesh; 4 = Belgium; 5 = Brazil; 6 = Cameron; 7 = Canada; 8 = Chez Republic; 9 = China; 10 = Croatia; 11 = Estonia; 12 = Finland; 13 = France; 14 = Georgia; 15 = Germany; 16 = Hungary; 17 = India; 18 = Iran; 19 = Ireland; 20 = Israel; 21 = Italy; 22 = Japan; 23 = Kosovo; 24 = Lithuania; 25 = Malaysia; 26 = Mexico; 27 = Moldova; 28 = Netherland; 29 = Nigeria; 30 = North Korea; 31 = Pakistan; 32 = Poland; 33 = Philippine; 34 = Romania; 35 = Russia; 36 = Saudi Arabia; 37 = South Africa; 38 = South Korea; 39 = Spain; 40 = Sweden; 41 = Taiwan; 42 = Thailand; 43 = Turkey; 44 = UK; 45 = Ukraine; 46 = Vietnam; 47 = Colombia ; 48 = Venezuela; 49 = Ecuador; 50 = Algeria; 51 = Morocco; 52 = Uruguay; 53 = Latvia; 54 = Lebanon; 55 = Belarus; 56 = Dominican Republic; 57 = Egypt; 58 = Kazakhstan; 59 = Greece; 60 = Macedonia;**
6.	The type of target	**If 1 = private** **2 = business sector (e.g., company, bank, news media company, etc.)**

3 = government/military

7. Cybercrime method utilized

If 0 = Vandalism (i.e., defacement; sabotage),

1 = Denial of Service

(i.e., DDoS; zombies; botnets)

2 = Intrusion

(i.e., unauthorized access; ransomware scams; Trojans; trapdoors; backdoors; identity theft; intellectual property theft; cyber-espionage)

3 = Infiltration

(i.e., worms; virus; sniffers; logic bombs; and keystroke loggings)

4 = Extortion and Exploitation

(i.e., sex solicitation; intent of purchasing sex; harassing with constant messages or sexual images/videos; sexting; revenge pornography; spreading rumors; stalking social networking accounts; cyberbullying; cyber-harassment)

5 = Deception

(i.e., phishing; spear-phishing; social engineering scams; financial institution scheme; investment scheme; internet confidence scheme; online auction scheme; online dating scheme; the Nigerian 419 scheme).

6 = Online illegal trade

(i.e., drug trafficking; organ trafficking; illegal weapon/counterfeit trades; stolen personal information trade)

7 = Cyberterrorism

(i.e., using encrypted communication technology for terrorism; using cyber-resources for terrorist recruitment and propaganda; using cyberspace to financial support for terrorist group)

8. Offender motivation	**If 0 = revenge** **1 = exposure** **2 = hacktivism (cyberterrorism): due to political or ideological or religious reasons** **3 = ego** **4 = monetary gain** **5 = entertainment** **6 = personality disorder** **7 = extortion and exploitation** **8 = blackmail** **9 = sabotage** **10 = espionage** **11 = information warfare** **12 = Mixed motivations (Revenge + Exposure)** **13 = Mixed motivations (Revenge + Hacktivism/Cyberterrorism)** **14 = Mixed motivations (Revenge + Ego)** **15 = Mixed motivations (Revenge + Monetary gain)** **16 = Mixed motivations (Revenge + Entertainment)** **17 = Mixed motivations (Revenge + Personality disorder)** **18 = Mixed motivations (Revenge + Extortion/Exploitation)** **19 = Mixed motivations (Revenge + Blackmail)** **20 = Mixed motivations (Revenge + Sabotage)** **21 = Mixed motivations (Revenge + Espionage)**

22 = Mixed motivations (Revenge + Information warfare)

23 = Mixed motivations (Exposure + Hacktivism)

24 = Mixed motivations (Exposure + Ego)

25 = Mixed motivations (Exposure + Monetary gain)

26 = Mixed motivations (Exposure + Entertainment)

27 = Mixed motivations (Exposure + Personality disorder)

28 = Mixed motivations (Exposure + Extortion/Exploitation)

29 = Mixed motivations (Exposure + Blackmail)

30 = Mixed motivations (Exposure + Sabotage)

31 = Mixed motivations (Exposure + Espionage)

32 = Mixed motivations (Exposure + Information warfare)

32 = Mixed motivations (Hacktivism + Ego)

33 = Mixed motivations (Hacktivism + Monetary gain)

34 = Mixed motivations (Hacktivism + Entertainment)

35 = Mixed motivations (Hacktivism + Personality disorder)

36 = Mixed motivations (Hacktivism +Extortion/exploitation)

37 = Mixed motivations (Hacktivism + Blackmail)

38 = Mixed motivations (Hacktivism + Sabotage)

39 = Mixed motivations (Hacktivism + Espionage)

40 = Mixed motivations (Hacktivism + Information warfare)

41 = Mixed motivations (Ego + Monetary gain)

42 = Mixed motivations (Ego + Entertainment)

42 = Mixed motivations (Ego + Personality disorder)

43 = Mixed motivations (Ego + Extortion/Exploitation)

44 = Mixed motivations (Ego + Blackmail)

45 = Mixed motivations (Ego + Sabotage)

46 = Mixed motivations (Ego + Espionage)

47 = Mixed motivations (Ego + Information warfare)

48 = Mixed motivations (Monetary gain + Entertainment)

49 = Mixed motivations (Monetary gain + Personality disorder)

50 = Mixed motivations (Monetary gain + Extortion/Exploitation)

51 = Mixed motivations (Monetary gain + Blackmail)

52 = Mixed motivations (Monetary gain + Sabotage)

53 = Mixed motivations (Monetary gain + Espionage)

54 = Mixed motivations (Monetary gain + Information warfare)

55 = Mixed motivations (Entertainment + Personality disorder)

56 = Mixed motivations (Entertainment + Extortion/Exploitation)

57 = Mixed motivations (Entertainment + Blackmail)

58 = Mixed motivations (Entertainment + Sabotage)

59 = Mixed motivations (Entertainment + Espionage)

60 = Mixed motivations (Entertainment + Information warfare)

61 = Mixed motivations (Personality disorder + Extortion/Exploitation)

62 = Mixed motivations (Personality disorder + Blackmail)

63 = Mixed motivations (Personality disorder + Sabotage)

64 = Mixed motivations (Personality disorder + Espionage)

65 = Mixed motivations (Personality disorder + Information warfare)

66 = Mixed motivations (Extortion/Exploitation + Blackmail)

67 = Mixed motivations (Extortion/Exploitation + Sabotage)

68 = Mixed motivations (Extortion/Exploitation + Espionage)

69 = Mixed motivations (Extortion/Exploitation + Information warfare)

70 = Mixed motivations (Blackmail + Sabotage)

71 = Mixed motivations (Blackmail + Espionage)

72 = Mixed motivations (Blackmail + Information warfare)

73 = Mixed motivations (Sabotage + Espionage)

74 = Mixed motivations (Sabotage + Information warfare)

	75 = Mixed motivations (Espionage + Information warfare)
	76 = Mixed motivations (more three motivations on the list above)
9. Offender's distance level from target	**If 1 = Intra-city**
	2 = Inter-city
	3 = Inter-state
	4 = International
10. Accomplice (Y/N)	**If 0 = no, 1 = yes**
11. Damage or monetary loss	**If 0 = none**
	1 = infrastructure damage
	2= individual or business property damage (including monetary loss)
	3 = sexual abuse
	4 = psychological harm/physical harm/death
	5 = mixed damages (infrastructure + individual/business)
	6 = mixed damages (infrastructure + sexual abuse)
	7 = mixed damages (infrastructure + psychological/physical harm/death)
	8 = mixed damages (individual/business + sexual abuse)
	9 = mixed damages (individual/business + psychological/physical)
	10 = mixed damages (sexual abuse + psychological/physical/death)

12. Severity scale of damage

5 = Critical network and infrastructure destruction

Example - power grid hack, hydroelectric dams shut down, indirect death

Notes - For this measure to be coded, a state's critical infrastructure must be breached and the network manipulated so that widespread functionality is disrupted for a significant period of time. These efforts have to be massive, impactful, and clearly intentional.

4 = Widespread government, economic, military, or critical private sector theft of information

Example - (US OPM hack, DoD employee records stolen, IRS hack)

Notes –Phishing and intrusion espionage campaigns that successfully steal large troves of critical information, such as the OPM hack.

3 = Stealing targeted critical information

Example - (Chinese targeted espionage, government-sanctioned cybercrime, Sony Hack)

Notes - This involves the use of intruding upon a secure network and stealing sensitive or secret information. The theft of Lockheed Martin's F-35 jet plans or the U.S. Department of Defense's strategy in the Far East are examples or if the target was critical to national security or the objective of the attack had national security implications. The piggy-back method is another example of this severity type. The United States' NSA was able to piggy back on China's Byzantine Series undetected and spy on the targets that the original espionage was spying upon.

2 = Harassment, propaganda, nuisance disruption

Example - (Propagandist messages in Ukraine, Vandalism, DDoS in Georgia, Bronze Soldier dispute)

Notes–Mainly vandalism or DDoS campaigns, this measure is coded when pockets of government or private networks are disrupted for periods of time and normal day to day online life is difficult, but recoverable.

1 = Probing without kinetic cyber

Example - (US NSA dormant infiltrations)

Notes - Using cyber methods to breach networks but not utilize any malicious actions beyond that. Hacking a power grid but not shutting it down, planting surveillance technology within networks, and unsophisticated probing methods are examples of this severity level.

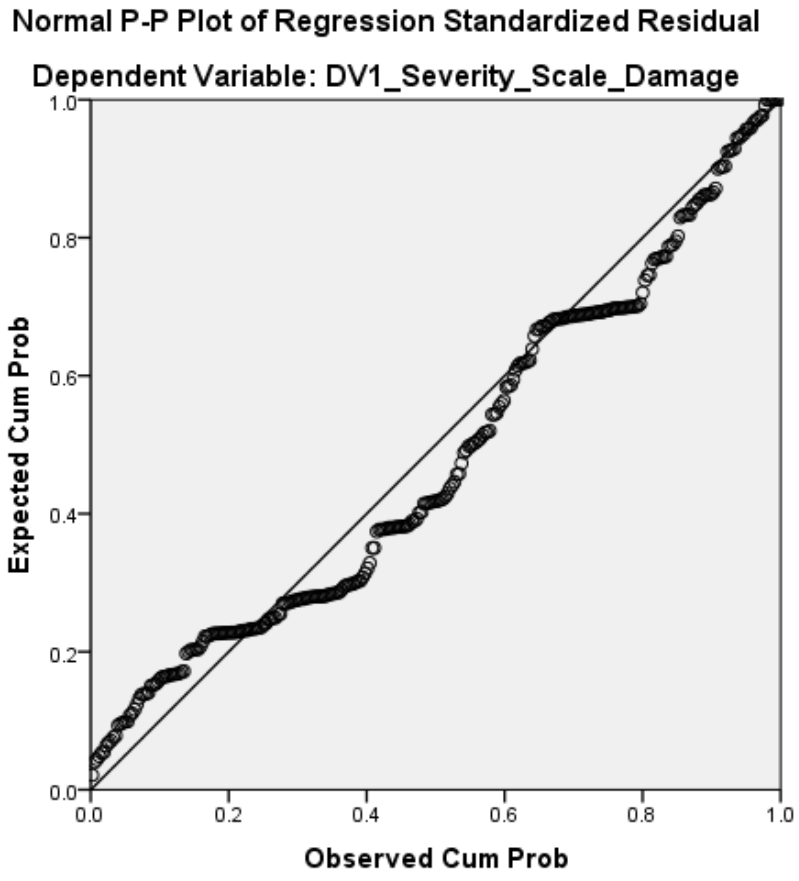
13. Damage type

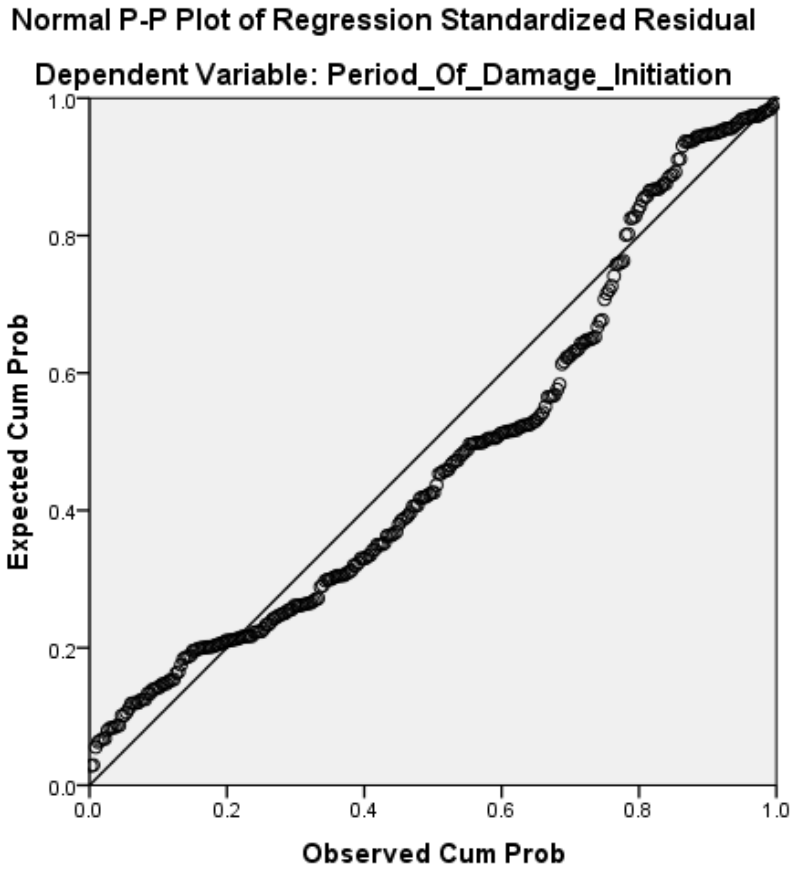
1. Indirect and delayed. If intellectual property is stolen by an initiator and it becomes publicly available, this may result in improved competition for states or private companies that did not have this technology or advantage prior. China stole the American company's F-35 jet plans, and if it gave these plans to Russia, the effects of this cyber incident would be indirect, and the costs would be felt at a future point in time.

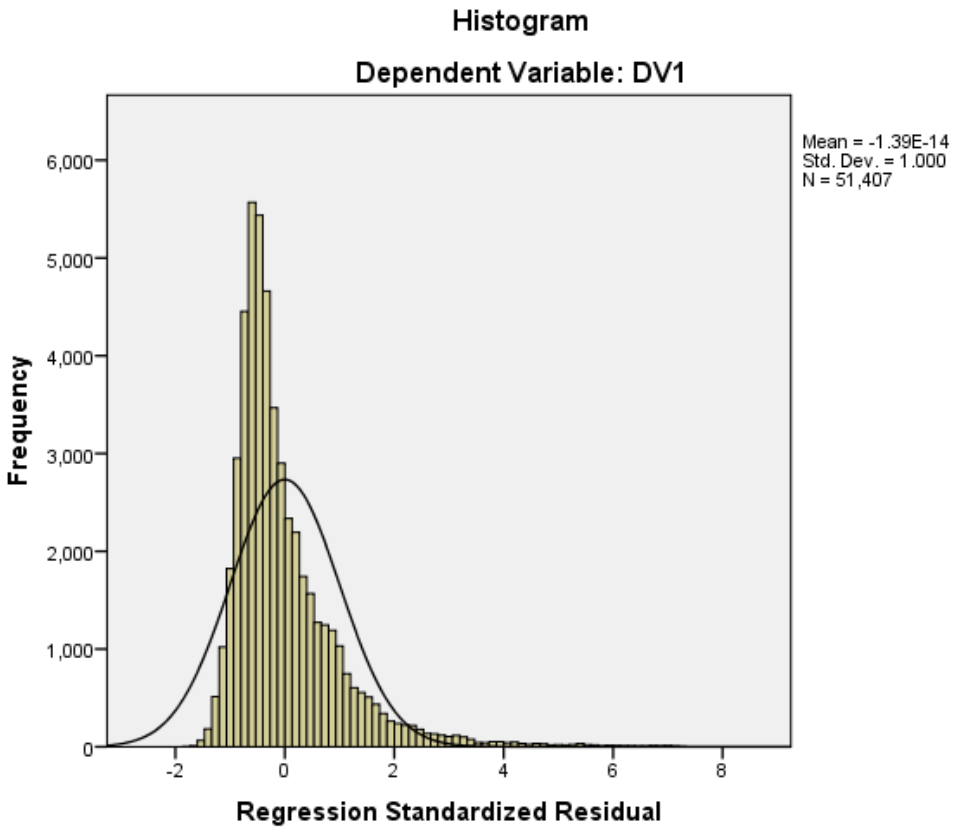
2. Indirect and immediate. Indirect in this context means that the damage done by the cyber incident was not the original intent of the initiator. The stealing of confidential information from a bank or a breach in the Wall Street system is an example of this. The costs of these incidents are felt immediately. Reputational damage or loss of confidentiality

	is what to look for when coding this damage. 3. Direct and delayed. Stuxnet was intended to disrupt Iran's nuclear program by damaging the centrifuges at the Natanz plant, and it succeeded. The impact of this attack took a number of months if not years to slowly disrupt and damage these centrifuges through code manipulation. 4. Direct and immediate: The term direct in this context means that the damage done by the cyber incident was what was intended by the initiator and the costs of the cyber incident are felt immediately. The Russian DDoS attacks on Estonia's government and private networks in 2007 is an example, as the effective shutdowns cost millions of dollars in lost revenue for the Baltic country.
14. Random violence	0 = randomly attack to victim/target 1 = intended attack to victim/target,
15. Victim age	*Age when he/she was victimized **(e.g., 36)***
16. Victim sex	**If 0 = female,** **1 = male**
17. Victim geographic location	City **(i.e., Maimi)** and state **(i.e., FL)**

Appendix D

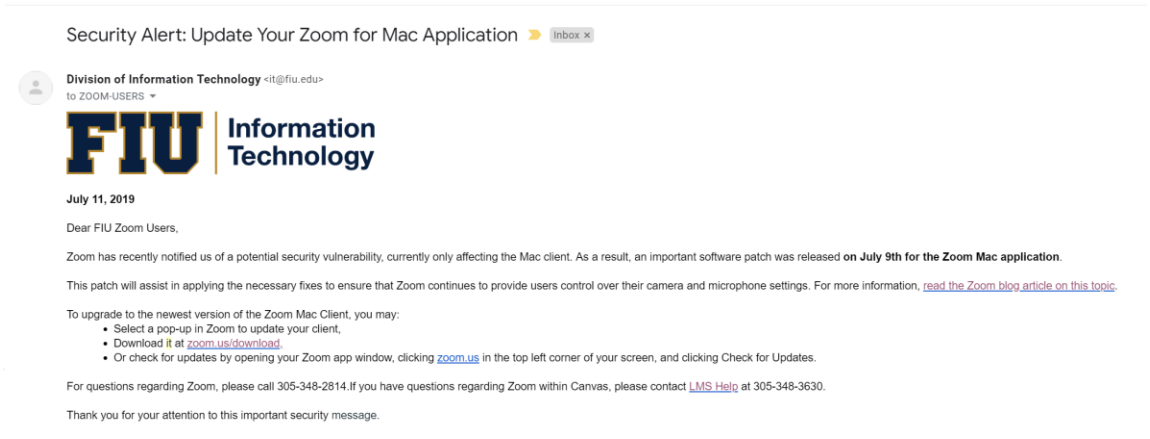

Normal P-P Plot of Regression Standardized Residual
Dependent Variable: DV1_Severity_Scale_Damage
Expected Cum Prob
Observed Cum Prob
0.0
0.2
0.4
0.6
0.8
1.0


Normal P-P Plot of Regression Standardized Residual
Dependent Variable: Period_Of_Damage_Initiation
Expected Cum Prob
Observed Cum Prob
0.0
0.2
0.4
0.6
0.8
1.0



Regression Standardized Residual for Cybercrime Victimization

Appendix E



Security Alert: Update Your Zoom for Mac Application

Division of Information Technology <it@fiu.edu>
to ZOOM-USERS

FIU Information Technology

July 11, 2019

Dear FIU Zoom Users,

Zoom has recently notified us of a potential security vulnerability, currently only affecting the Mac client. As a result, an important software patch was released **on July 9th for the Zoom Mac application**.

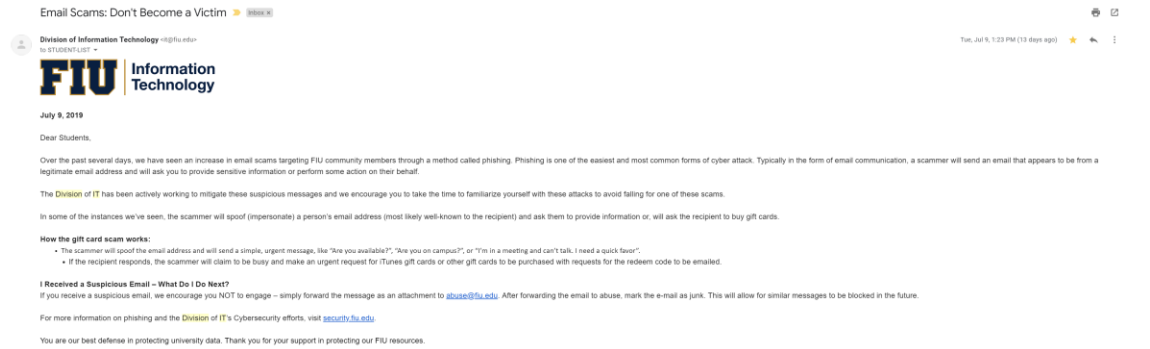
This patch will assist in applying the necessary fixes to ensure that Zoom continues to provide users control over their camera and microphone settings. For more information, read the Zoom blog article on this topic.

To upgrade to the newest version of the Zoom Mac Client, you may:

- Select a pop-up in Zoom to update your client,
- Download it at zoom.us/download.
- Or check for updates by opening your Zoom app window, clicking zoom.us in the top left corner of your screen, and clicking Check for Updates.

For questions regarding Zoom, please call 305-348-2814.If you have questions regarding Zoom within Canvas, please contact LMS Help at 305-348-3630.

Thank you for your attention to this important security message.



Email Scams: Don't Become a Victim

Division of Information Technology <it@fiu.edu>
to STUDENT-LIST

FIU Information Technology

July 9, 2019

Dear Students,

Over the past several days, we have seen an increase in email scams targeting FIU community members through a method called phishing. Phishing is one of the easiest and most common forms of cyber attack. Typically in the form of email communication, a scammer will send an email that appears to be from a legitimate email address and will ask you to provide sensitive information or perform some action on their behalf.

The Division of IT has been actively working to mitigate these suspicious messages and we encourage you to take the time to familiarize yourself with these attacks to avoid falling for one of these scams.

In some of the instances we've seen, the scammer will spoof (impersonate) a person's email address (most likely well-known to the recipient) and ask them to provide information or, will ask the recipient to buy gift cards.

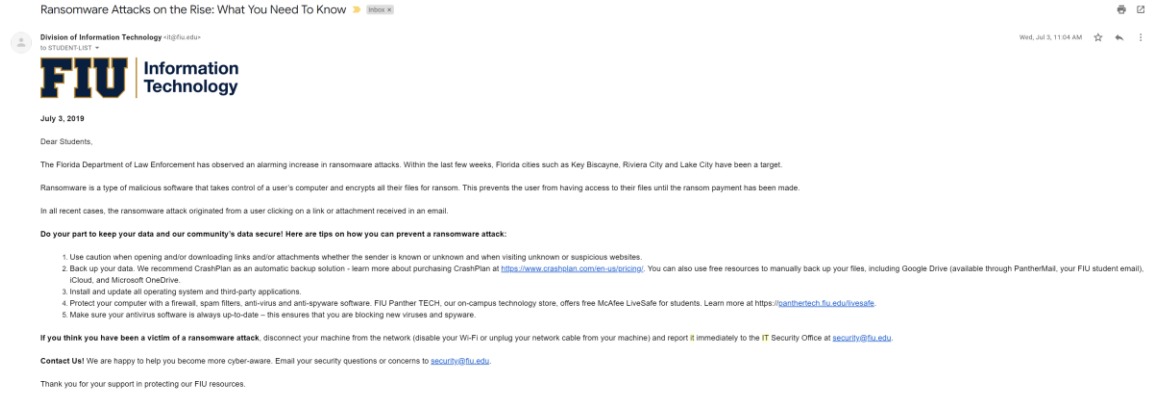
How the gift card scam works:

- The scammer will spoof the email address and will send a simple, urgent message, like "Are you available?", "Are you on campus?", or "I'm in a meeting and can't talk. I need a quick favor".
- If the recipient responds, the scammer will claim to be busy and make an urgent request for iTunes gift cards or other gift cards to be purchased with requests for the redeem code to be emailed.

I Received a Suspicious Email – What Do I Do Next?
If you receive a suspicious email, we encourage you NOT to engage – simply forward the message as an attachment to abuse@fiu.edu. After forwarding the email to abuse, mark the e-mail as junk. This will allow for similar messages to be blocked in the future.

For more information on phishing and the Division of IT's Cybersecurity efforts, visit security.fiu.edu.

You are our best defense in protecting university data. Thank you for your support in protecting our FIU resources.



Ransomware Attacks on the Rise: What You Need To Know

Division of Information Technology <it@fiu.edu>
to STUDENT-LIST

FIU Information Technology

July 3, 2019

Dear Students,

The Florida Department of Law Enforcement has observed an alarming increase in ransomware attacks. Within the last few weeks, Florida cities such as Key Biscayne, Riviera City and Lake City have been a target.

Ransomware is a type of malicious software that takes control of a user's computer and encrypts all their files for ransom. This prevents the user from having access to their files until the ransom payment has been made.

In all recent cases, the ransomware attack originated from a user clicking on a link or attachment received in an email.

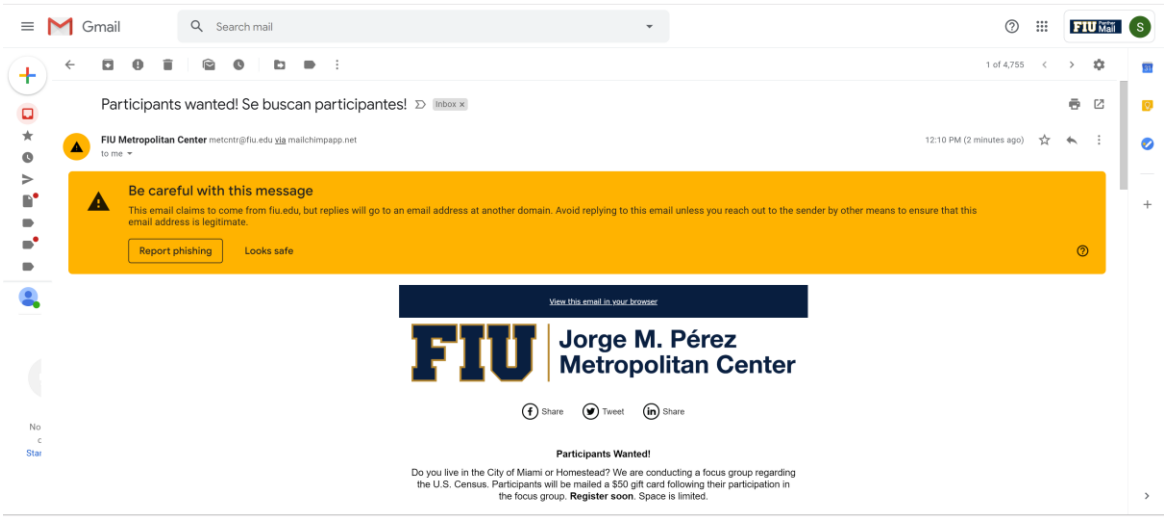
Do your part to keep your data and our community's data secure! Here are tips on how you can prevent a ransomware attack:

1. Use caution when opening and/or downloading links and/or attachments whether the sender is known or unknown and when visiting unknown or suspicious websites.
2. Back up your data. We recommend CrashPlan as an automatic backup solution - learn more about purchasing CrashPlan at https://www.crashplan.com/en-us/pricing/. You can also use free resources to manually back up your files, including Google Drive (available through PantherMail, your FIU student email), iCloud, and Microsoft OneDrive.
3. Install and update all operating system and third-party applications.
4. Protect your computer with a firewall, spam filters, anti-virus and anti-spyware software. FIU Panther TECH, our on-campus technology store, offers free McAfee LiveSafe for students. Learn more at https://panthertech.fiu.edu/livesafe.
5. Make sure your antivirus software is always up-to-date – this ensures that you are blocking new viruses and spyware.

If you think you have been a victim of a ransomware attack, disconnect your machine from the network (disable your Wi-Fi or unplug your network cable from your machine) and report it immediately to the IT Security Office at security@fiu.edu.

Contact Us! We are happy to help you become more cyber-aware. Email your security questions or concerns to security@fiu.edu.

Thank you for your support in protecting our FIU resources.


Gmail
Search mail
FIU Mail
Participants wanted! Se buscan participantes!
Inbox ×
1 of 4,755
FIU Metropolitan Center metcntr@fiu.edu via mailchimpapp.net
to me
12:10 PM (2 minutes ago)
Be careful with this message
This email claims to come from fiu.edu, but replies will go to an email address at another domain. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.
Report phishing
Looks safe
View this email in your browser
FIU
Jorge M. Pérez
Metropolitan Center
Share
Tweet
Share
Participants Wanted!
Do you live in the City of Miami or Homestead? We are conducting a focus group regarding the U.S. Census. Participants will be mailed a $50 gift card following their participation in the focus group. Register soon. Space is limited.

VITA

SINCHUL BACK

Born, Jinju, South Korea

2012	B.S., Leadership Northeastern University Boston, Massachusetts
2016	M.S., Criminal Justice Bridgewater State University Bridgewater, Massachusetts
2019	Doctoral Candidate Florida International University Miami, Florida
2019 -2020	Assistant Professor University of Scranton Scranton, Pennsylvania

PUBLICATIONS

Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 1-4.

Back, S., LaPrade, J., Shehadeh, L., & Kim, M. (2019). Youth hackers and adult hackers in South Korea: An application of cybercriminal profiling. *IEEE on Security and Privacy*, 2019, pp. 410-413.

Meldrum, R. C., Boman, J. H., & Back, S. (2018). Low Self-Control, Social Learning, and Texting while Driving. *American Journal of Criminal Justice*, 1-20.

Back, S., Soor, S., & LaPrade, J. (2018). Juvenile hackers: An empirical test of self-control theory and social bonding theory. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 40-55.

Back, S., LaPrade, J., & Soor, S. (2018). Spatial and temporal patterns of cyberattacks: Effective prevention strategies around the globe. *International Journal of Protection, Security & Investigation*, *3*, 7-13.

Back, S., Sung, Y., & Cruz, E. (2017). Capable guardianship and crisis of identity theft in the United States: Expanding cyber-routine activities theory. *International Journal of Crisis & Safety, 2*(1), 16-24.

Back, S., Sung, Y., & LaPrade, J. (2017). The effect of terrorism risk perception and agency's interaction on police homeland preparedness. *International Journal of Police & Policing, 2*, 7-13.

Back, S., Sung, Y., & Morales, A. (2017). Impact of a refugee crisis on the increase of terrorist incidents. *International Journal of Protection, Security & Investigation, 2 (1),* 1-8.

Scott, T., Back, S., & Choi, K. (2015). Emotional literacy program and its effectiveness: Potential policy implication in South Korea. *Korean Criminal Psychology Review, 11*(3), 274-293.