International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 2 Article 3

11-3-2020

Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions

IJCIC Center for Cybercrime Investigation & Cybersecurity

Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions

Sinchul Back, PhD, The University of Scranton, U.S.A
Jennifer LaPrade*, Missouri State University, U.S.A

Keywords; Breadth of cybercrimes, Cybersecurity, Cyber-situational crime prevention

Abstract:

Academic institutions house enormous amounts of critical information from social security numbers of students to proprietary research data. Thus, maintaining up to date cybersecurity practices to protect academic institutions' information and facilities against cyber-perpetrators has become a top priority. The purpose of this study is to assess common cybersecurity measures through a situational crime prevention (SCP) theoretical framework. Using a national data set of academic institutions in the United States, this study investigates the link between common cybersecurity measures, crime prevention activities, and cybercrimes. By focusing on the conceptualization of cybersecurity measures as SCP techniques, this study also offers the SCP approach as a framework by which universities can seek to reduce incidents of cybercrime through the design, maintenance, and use of the built environment in the digital realm. Implications for theory, research and practice are discussed.

Introduction

The digital realm, or the connections between devices and the internet, is becoming increasingly important to modern society. From the growing significance of mobile devices to the availability of laptops and other small and portable devices, people are becoming ever-more connected to each other and reliant on the internet to conduct their daily activities. Specifically, within the context of the United States, the information era and competitive technological advances transitioned almost every aspect of U.S. society into a digital one. For example, food and water systems, health systems and emergency services, educational institutions, and banking and finance institutions are all heavily reliant on information systems and the internet to provide connectivity between critical infrastructure systems (Lewis, 2006; Skopik, Bleier, & Fiedler, 2012).

*Corresponding author

Jennifer LaPrade, Ph.D., Department of Criminology and Criminal Justice, Missouri State University, 901 S. National Ave., Springfield, MO, 65897, U.S.A.

Email: jlaprade@missouristate.edu

While such advances have made some aspects of life easier, it also creates a vulnerability to cyber threats that can threaten national security and economic vitality (Ten, Manimaran, & Liu, 2010). Additionally, major security incidents on cyber systems can cause substantial impacts to critical infrastructure. According to the U.S. Industrial Control System Cyber Emergency Response Team, if a cyberattack shuts down parts of the United States' critical infrastructure, it could cost approximately $1 trillion to the U.S. economy (Cohn, 2015).

One aspect of America's critical infrastructure that is particularly susceptible to cyberattacks are academic institutions. In this regard, academic institutions possess and use enormous amounts of critical information for faculty members, students, and third parties in order to implement their educational and research programs and operate their facilities. Considerable confidential information exists within many academic institutions since they cooperate with public and private sectors to conduct significant research projects for national security and economic systems. Recently, nine Iranian state-sponsored hackers were charged with conducting a massive theft of intellectual property and data – from 144 U.S. universities and 176 universities across 21 foreign countries, and U.S. government entities – which resulted in damages of approximately $3.4 billion USD (The United States Department of Justice [US DOJ], 2018). Given the magnitude of such attacks, designing effective cybersecurity systems to protect academic institutions' information and facilities against cyber-perpetrators is now a primary concern for both academic institutions and the nation as a whole.

Nevertheless, few theoretically informed studies have been conducted on the types of cybercrime commonly experienced among academic institutions. Further, questions remain about whether existing cybersecurity systems are appropriately implemented to protect their assets, and to what extent various security provisions are commonly used. Therefore, in order to fill these gaps, the purpose of this study is (1) to explore the use of cybersecurity measures by U.S. academic institutions through an application of the situational crime prevention (SCP) framework and (2) to diagnose the application of cyber-SCP techniques on coping with cybercrime among U.S. academic institutions. Drawing from SCP theory, the present study focuses on the conceptualization of cyber security measures as SCP techniques and empirically explores their use in the protection of U.S. academic institutions against cybercrimes. In particular, this study seeks to explore the associations between cyber-SCP activities and various cybercrime outcomes through a series of bivariate models, as well as examine whether there are links between the breadth of cybercrime types and the use of various cyber-SCP techniques through a series of multivariate models. While other studies have explored the potential connection theoretically, this is one of the first studies to empirically test the association between the SCP framework and cybercrime, making a significant contribution to the literature.

To answer these questions, this study is arranged as follows. In the first section, this study will review the background of research pertaining to cybercrime, cybersecurity, and situational crime prevention. In the second section, this study will outline the methodology and describe the results of the analyses. Lastly, the findings, policy implications, and limitations of the study will be discussed.

Background

Cybercrime and Cybersecurity

Based on the U.S. Computer Fraud and Abuse Act (1984) and the U.K. Computer Abuse Act (1990), cybercrime is defined as a criminal act that harms the reputation of the victim, causes physical or mental harm, or commits extortion to the victim directly or indirectly through using networks, computers, and mobile phones (Casey, Blitz, & Steuart, 2004; Choi, 2015; Thomas & Loader, 2000). In response to cybercrime, the main goals of cybersecurity systems include maintaining privacy, preserving data integrity, authenticating approved users of network resources, and enabling authorized users to connect securely to internal networks (Holden 2003). Figure 1 depicts the structure of common cybersecurity technologies.

To date, research on cybercrime prevention (cybersecurity) is limited and has been largely examined empirically by applying routine activities theory (e.g., Cohen & Felson, 1979; Choi, 2008; Bossler & Holt, 2009; Leukfeldt & Yar, 2016; Wilsem, 2011, 2013). Interestingly, these studies found mixed results. For example, Choi (2008) found that technical capable guardianship (e.g., anti-virus, anti-spyware) was associated with cybercrime victimization, whereas Bossler and Holt (2009), Leukfeldt and Yar (2016), and Marcum and associates (2010) found that technical capable guardianship was not related to cybercrime victimization. Along with the aforementioned studies, Testa and associates (2017) assessed the effects of situational deterring cues on cyber-trespassers' online behaviors. Testa et al. (2017) found that although the use of sanctioned threats in an attacked computer system is effective in mitigating the deviant activities of cybercriminals with a basic level of computer hacking skills, this strategy is ineffective in deterring cybercriminals who take over a stakeholder's network with high criminal efficacy (i.e., abusing administrative privileges).

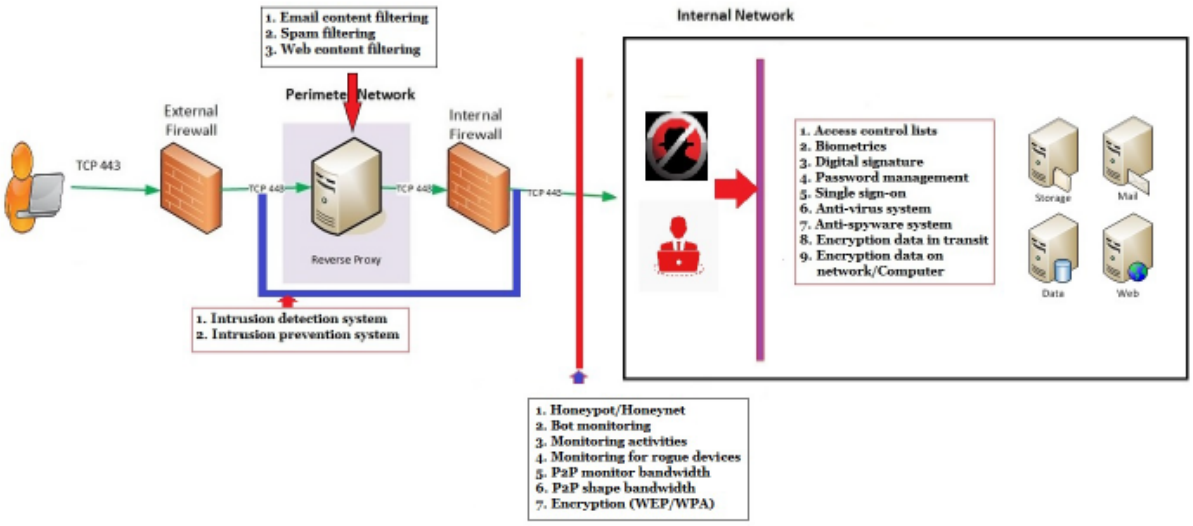

Figure 1. Diagram of Cybersecurity System Structure

Source. – Adapted from Ferrari (2005), Holden (2003), Stallings (2003).

In contrast, few studies in the criminological literature have utilized SCP theory to explain the effectiveness of cybercrime prevention. For example, Beebe and Rao (2005), and Hinduja and Kooi (2013) suggest that SCP theory could be useful to improve cybersecurity effectiveness by diminishing the perpetrator's expected rewards from the crime. Reyns (2010) concluded that SCP offers a critical framework to reduce criminal opportunities for cyberstalking. Also, Willison (2000; 2006) argued that situational crime prevention could explain the link between computer fraud opportunity and crime prevention. Unfortunately, the extant studies discussing the relevance of SCP theory were merely theoretical; these studies only conceptualized the framework and demonstrated that the concepts of SCP could be applied to the study of cybercrime and cybersecurity. Thus, the current study contributes to this literature by empirically examining the associations between cyber-SCP techniques and cybercrime incidents. Furthermore, there is an emerging body of literature that empirically explores cybervictimization among individuals (such as Wright & Li, 2013; Gini, Card, & Pozzoli, 2018), however, the literature examining cybervictimization among institutions is lacking.

Situational Crime Prevention

The situational crime prevention approach suggests that crime can be prevented by environmental settings that directly and indirectly impact criminals' perceptions of efforts, risks, rewards, provocations, and excuses (Cornish & Clarke, 2003; Welsh & Farrington, 2004). In recent years, the contemporary interest in applying situational crime prevention theory in criminal justice systems has arisen largely from academics and policy makers in the United Kingdom and the United States (Welsh & Farrington, 2004).

Clarke (1995; 1997), and Cornish and Clarke (2003) note that rational choice, routine activities, and crime pattern theories are found in situational crime prevention theory. First, rational choice theory (RCT) is grounded in the expected utility principle in which people will make rational choices based on the extent to which they anticipate their decisions to provide benefits and avoid losses. According to RCT, offenders will choose targets and determine the means to achieve their objectives in a manner that can be articulated (Cornish & Clarke, 2014). RCT provided a theoretical perspective to explain how SCP practices operate to prevent crime. Second, routine activity theory explains that crime events occur when three circumstances – motivated offender, suitable target, and the absence of capable guardian – converge (Cohen & Felson, 1979; Felson, 2017). In a related sense, the main proposition of RAT is that the more a person is motivated to commit a crime, the more the crime occurs when a suitable target exists and the formal/informal guardianships are absent (Akers, 2013; Cohen & Felson, 1979). RAT helps establish an SCP theoretical framework to explain how the roles of key actors, places, and suitable targets are related to the occurrence of the crime event. Third, according to crime pattern theory (CPT), criminals' routine movement patterns are associated with criminal behavior (Brantingham & Brantingham, 1993, 1995). For example, crime pattern theory explains that the distribution of offenders, targets, handlers, guardians, and managers over time and place are related to the patterns of crime events (Eck & Weisburd, 2015). Specifically, Eck and Weisburd (2015) contend that "interactions of offenders with their physical and social environment" impacts criminals' target selecting process. In this regard, the CPT theoretical framework has influenced SCP measures that are associated with explaining the clustering of crimes into hot spots (Brantingham & Brantingham, 1995; Smith & Clarke, 2012). In other words, the features of RCT, RAT, and CPT have assisted in the development of SCP classification schemes (Clarke, 1983, 1995, 1997; Clarke & Homel, 1997; Cornish & Clarke, 2003; Wortley, 2001, 2002).

Alongside these three theories, Clarke developed situational crime prevention (SCP) theory with 16 original opportunity-reducing techniques in 1980 (Clarke, 1980, 1983, 1997). Clarke defines "situational crime prevention as opportunity-reducing measures that: (1) are directed at highly specific forms of crime; (2) involve the management, design, or manipulation of the immediate environment in as systematic and permanent, a way as possible; (3) make crime more difficult and risky, or less rewarding and excusable as judged by a wide range of offenders" (Schneider, 2014, p. 45).

Critics including Wortley (2001), however, argued that the existing classification needs to be revised with four types of precipitator – prompts, pressures, permissions, and provocations – in order to reflect the relative neglect of other situational forces for criminal decision making and situational prevention (Cornish & Clarke, 2003). In line with that criticism, Cornish and Clarke (2003) revised and proposed a classification of 25 SCP techniques (see Table 1). The SCP theory consists of five major categories: (1) increasing the effort of the offender by target hardening; (2) increasing the risks to the offender; (3) reducing the rewards to the offender; (4) removing people's excuses to commit crimes; (5) reducing the provocations of the offender (Cornish & Clarke, 2003; Schneider, 2014).

Cyber-Situational Crime Prevention

As discussed above, SCP techniques can be extended to cyber settings to enhance cybercrime preventative framework. For example, automobiles with target hardening techniques (i.e., steering column locks) are less likely to be burglarized than those without its techniques (Schneider, 2014). In the virtual world, online users with cyber target hardening techniques (i.e., firewall systems) might be less likely to experience cyber-intrusions and unauthorized accesses. Firewall systems are hardware or software that 1) allows traffic for an established connection and 2) denies traffic for malicious packets containing false information so that it can protect a network from unauthorized access and malicious attacks (Holden, 2003). These examples provide support that situational crime prevention techniques cannot only be applied to reduce crime in the physical world but can also applied to reduce cybercrime. Specifically, higher education institutions can especially utilize situational crime prevention techniques to protect valuable and sensitive data with such tools such as firewalls, encryption, cybersecurity training of faculty, staff, and students, and strong password management systems.

It must be noted that scholars now utilize the 25 SCP techniques to explain criminal offending and crime prevention in the physical world, whereas the original 16 SCP techniques are still mainly applied and perhaps most relevant to conducting research on cybercrimes and crime prevention in cyberspace. According to Hinduja and Kooi (2013) who provided an application of 16 SCP to information security, although the 25 SCP techniques contribute more to identifying methods that explain situational precipitators and opportunity contributors, many of these elements were irrelevant for preventing cybercrime incidents. Also, because of the available variables, the data set analyzed in this study is more apt to the 16 SCP techniques than the 25 SCP techniques. As a result, the 16 SCP techniques (shaded in gray in Table 1 and 2) are utilized in this study to examine the relationships between cybercrime and cyber-SCP activities. In total, 46 cybercrime prevention measures were grouped according to 16 cyber-SCP techniques, with these 16 techniques divided according to one of the four categories of general means – increase the efforts, increase the risks, reduce rewards, and remove excuses.

Table 1. Twenty-Five Techniques of Situational Crime Prevention

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
1. Target hardening ▪ Steering column locks ▪ Anti-robbery screens ▪ Tamper-proof packaging	6. Extend guardianship ▪ Take routine precautions: go out in group at night, leave signs of occupancy, carry phone ▪ "Cocoon" neighborhood watch	11. Conceal targets ▪ Off-street parking ▪ Gender-neutral phone directories ▪ Unmarked bullion trucks	16. Reduce frustrations and stress ▪ Efficient queues and polite service ▪ Expand seating ▪ Soothing music/muted lights	21. Set rules ▪ Rental agreements ▪ Harassment codes ▪ Hotel registration
2. Control access to facilities ▪ Entry phones ▪ Electronic card access ▪ Baggage screening	7. Assist natural surveillance ▪ Improved street lighting ▪ Defensible space design ▪ Support whistleblowers	12. Remove targets ▪ Removable car radio ▪ Women's refuges ▪ Pre-paid cards for pay phones	17. Avoid disputes ▪ Separate enclosures for rival soccer fans ▪ Reduce crowding in pubs ▪ Fixed cab fares	22. Post instructions ▪ "No Parking" ▪ "Private Property" ▪ "Extinguish camp fires"
3. Screen exits ▪ Ticket needed for exit ▪ Export documents ▪ Electronic merchandise tags	8. Reduce anonymity ▪ Taxi drive IDs ▪ "How's my driving?" decals ▪ School uniforms	13. Identity property ▪ Property marking ▪ Vehicle licensing and parts marking ▪ Cattle branding	18. Reduce emotional arousal ▪ Controls on violent pornography ▪ Enforce good behavior on soccer field ▪ Prohibit racial slurs	23. Alert conscience ▪ Roadside speed display boards ▪ Signatures for customs declarations ▪ "Shoplifting is stealing"
4. Deflect offenders ▪ Street closures ▪ Separate bathrooms for women ▪ Disperse pubs	9. Utilize place managers ▪ CCTV for double-deck buses ▪ Two clerks for convenience stores	14. Disrupt markets ▪ Monitor pawn shops ▪ Controls on classified ads ▪ License street vendors	19. Neutralize peer pressure ▪ "Idiots drink and drive" ▪ "It's OK to say No" ▪ Disperse troublemakers at school	24. Assist compliance ▪ Easy library checkout ▪ Public lavatories ▪ Litter bins
5. Control tools/weapons ▪ "Smart" guns ▪ Disabling stolen cell phones ▪ Restrict spray paint sales to juveniles	10. Strengthen formal surveillance ▪ Red light cameras ▪ Burglar alarms ▪ Security guards	15. Deny benefits ▪ Ink merchandise tags ▪ Graffiti cleaning ▪ Speed humps	20. Discourage imitation ▪ Rapid repair of vandalism ▪ V-chips in TV's ▪ Censor details of modus operandi	25. Control drugs and alcohol ▪ Breathalyzers in pubs ▪ Server intervention ▪ Alcohol-free events

Source. – Adapted from Cornish and Clarke (2003)

Table 2. *Cyber-Situational Crime Prevention Techniques*

Opportunity-Reducing Strategies	Cyber-SCP Techniques	Cybercrime Prevention Measures
Increase Efforts	1. Target hardening	a) Firewall: perimeter, b) firewall: interior, c) internal firewall, d) patch computers
	2. Access control	a) Digital signatures, b) password management, c) single sign-on, d) access control list
	3. Deflecting offenders	a) Honeypot (i.e., identifying malicious hackers), b) honeynet (i.e., identifying bots/zombies)
	4. Controlling facilitators	a) Reference check, b) criminal background check, c) identity management, d) role-based access control
Increase Risks	5. Entry/exit screening	a) intrusion detection system, b) intrusion prevention system, c) anti-virus, d) anti-spyware, e) use content filtering, f) email content filtering, g) spam filtering, h) web content filtering
	6. Formal surveillance	a) bot monitoring, b) monitor activity, c) monitor for rogue devices
	7. Surveillance by employees	a) employees mandatory training, b) full-time IT officer
	8. Natural surveillance	a) peer-to-peer technology: monitor bandwidth, b) peer-to-peer technology: shape bandwidth
Reduce Rewards	9. Target removal	a) encryption data on hard drive, b) encryption backup data for off-site storage, c) monitor use of backup media (e.g., USB drives)
	10. Identifying property	a) information asset classification
	11. Reducing temptation	a) level of sensitive information sharing, b) physical separation
	12. Denying benefits	a) encryption (e.g., WEP, WPA), b) encryption data in transit (PKI, SSL, HTTPS), c) encryption data on network or computers
Remove Excuses	13. Rule setting	a) user agreement, b) acceptable use policy/laws
	14. Stimulating conscience	a) warning banners on website, b) codes of ethics
	15. Controlling disinhibitions	a) warning violators, b) suspension, c) dismissal, d) restricted access to network
	16. Facilitating compliance	a) cybersecurity education for staff, faculty, and students

Source, - Adapted from Clarke (1992; 1995; 1997), Cornish and Clarke (2003), Beebe and Rao (2005), and Hinduja and Kooi (2013)

The Current Study

The present study extends the SCP framework from existing research by providing cyber-SCP techniques. In this regard, this study particularly focuses on suggesting concrete concepts of cyber-SCP techniques based on SCP and other scholars' application of SCP to information security. Furthermore, this study demonstrates how these cyber-SCP techniques can be specifically applied to building cybercrime prevention strategies. With this reasoning, this study comprehensively measures four elements of opportunity-reducing techniques: increase effort, increase risks, reduce reward, and remove excuses. Thus, the following research questions are used to guide the analysis: (1) is there a relationship between the use of cyber-SCP techniques and cybercrime incidents?; and (2) is there a relationship between the use of cyber-SCP techniques and the breadth of cybercrime types?

To address these research questions, first, this study inductively hypothesizes there will be a positive or negative relationship between cyber-SCP techniques and cybercrime incidents. Additionally, this study hypothesizes higher education institutions with higher level applications of cyber-SCP will have experienced a lower breadth of cybercrime types. In correspondence with these empirical investigations, the application of SCP to cyber-security prevention efforts offers several potential benefits. First, this empirical exploration of cyber-SCP techniques can demonstrate how crime prevention frameworks can be extended to digital/cyber settings in addition to physical settings. Second, exploring the applicability of the cyber-SCP framework to cybercrimes can give us more insight into the nature of cybersecurity vulnerabilities and suitable tactics to protect academic institutions' assets against motivated cyber-adversaries. Lastly, identifying an effective cyber-SCP framework can help stakeholders – academia, law enforcement, policy makers, private sector, etc. – create a practical roadmap for improving cybersecurity strategies.

Many pilot-related global health public research efforts would involve going through all the phases, such as in the development of a mobile software application, or App, or hardware device. In this case, researchers would benefit from doing a risk or threat assessment in the respective phases documented in the proposal.

Data

This study uses data derived from "The Impact of Information Security in Academic Institutions on Public Safety and Security in the United States, 2005-2006 (ICPSR 21188)." In this original study, four data sets (quantitative field survey data, qualitative one-on-one interview data, subject 1 network analysis data, and subject 2 network analysis data) were collected to develop practical policies or cost-effective controls for critical information security in academic institutions. Six hundred higher education institutions in the United States were randomly selected from the Department of Education's National Center. These academic institutions were asked to participate in the quantitative survey by postcard, telephone, and email in 2005-2006. The quantitative survey data was collected from 72 universities (12 percent response rate). While the small sample size and age of the data are both limitations of this study, this data set may be the only existing data set that researchers can currently utilize for an empirical cybersecurity study on American higher eduction institutions (Holt 2015), therefore, the data is still valuable as a starting point to examine this topic.

Measures

Dependent variables. The experience of cybercrimes was created by asking the question: "Which of the following types of cybercrimes have your institution experienced within the past 12 months?" To answer the question, respondents chose from the following lists: 1) Denial of service, 2) web site defacement, 3) unauthorized access to information, systems, or networks, 4) exposure of private information, 5) theft of private information, 6) theft of intellectual property, 7) sabotage, 8) fraud, 9) bot hosting, and 10) copyright infringement. Also, the original responses were coded as a 1 if they experienced the type of cybercrime and a 0 if the cybercrime type was not experienced. In addition, the 10 items were put into an additive scale (Cronbach's Alpha = .72) that ranged from 0 to 8, with 8 indicating the university experienced all eight cybercrime incidents within the past 12 months.

Independent variables. To measure independent variables, participants were asked to respond to the following questions: "Please describe the cyber-SCP techniques that your academic institution has implemented or not implemented (Please select one response for each technique below – implemented [1], not implemented [0])."

1. Target hardening: firewall perimeter, firewall interior, internal firewall, and patching computer
2. Access control: digital signatures, password management, single sign-on, and access control list
3. Deflecting offenders: honeynet and honeypot
4. Controlling facilitators: reference/criminal background check, identity management, and role-based access control
5. Entry/exit screening: intrusion detection/prevention system, anti-virus/spyware, and email/spam/web content filtering
6. Formal surveillance: bot monitoring, monitoring activity, and monitoring for rogue devices
7. Surveillance by employees: employees mandatory cybersecurity training, and full-time IT officer
8. Natural surveillance: P2P monitor bandwidth and P2P shape bandwidth
9. Target removal: encryption data on hard drive, encryption backup data off-site storage, and using backup media
10. Identifying property: information asset classification
11. Reducing temptation: sharing sensitive information with federal agencies, and physical separation
12. Denying benefits: Encryption (e.g., WEP, WPA), encryption data in transit (PKI, SSL, HTTPS), and encryption data on network or computers
13. Rule setting: requesting user agreement for cybersecurity policy/laws

14. Stimulating conscience: warning banners on website, and login banner when users access
15. Controlling disinhibitions: warning violators, suspension, dismissal, and restricted access to network
16. Facilitating compliance: cybersecurity education for staff, faculty, and student

Control variables. Three control variables were included in the multivariate analysis: higher education institution's type of control, degree of urbanization, and highest degree, which could all possibly affect SCP framework capabilities and cyber victimization. Respondents were asked: "How would you characterize your institution's type of control?" The item for type of control is coded (0 = private, 1 = public). Respondents also were asked: "How would you characterize your institution's degree of urbanization?" The item for degree of urbanization is coded (1 = large town/small town/rural, 2 = mid-size city/urban fringe of mid-size city, 3 = large city/urban fringe of large city). Lastly, respondents were asked: "How would you characterize your institution's highest degree?" The item for highest degree is coded (1 = associates, 2 = bachelors, 3 = masters, 4 = doctoral, 5 = doctoral and first-professional).

Analytic Strategy

All models were estimated using SPSS 20. Two stages of analyses were applied in measuring the associations between cyber-SCP activities and cybercrime. First, Phi correlations were estimated to determine if any cyber-SCP techniques were significantly related with each of the cybercrime outcomes. The Phi coefficient was utilized to analyze the data because each variable not only has natural dichotomies but also for two-by-two crosstabulations (Williams, 2009). Second, this study explores the relationship between cyber-SCP techniques and the breadth of cybercrime types through Poisson regressions in order to formulate the best predictive model for the association between cyber-SCP techniques and cybercrime. The Poisson regression models are employed because the dependent variable for the breadth of cybercrime types is a count variable (Coxe, West, & Aiken, 2009). For the Poisson regression equations, 16 independent variables were derived from the previous Phi correlations matrix.

Results

Based on the original SCP and other scholars' application of SCP to information security, 46 cyber-SCP measures were initially established to transplant the concept SCP to cybercrime and cybersecurity. Next, these 46 cyber-SCP measures were utilized to explore the relationship between cyber-SCP techniques and the occurrence of cybercrime type. Accordingly, only 29 cyber-SCP measures, which were statistically significant in the Phi correlation analysis for cyber-SCP techniques and cybercrime types, were displayed in the descriptive statistics (Table 3) and Phi correlation matrix table (Table 4). Lastly, 16 cyber-SCP measures, which were the most significant measures from each of the 16 cyber-SCP techniques, were employed in the Poisson regression models in order to investigate the association between cyber-SCP techniques and the ten major cybercrime types. Descriptive analysis was performed to describe the sample characteristics and responses to the candidate variables. Table 3 provides the descriptive statistics (i.e., means, standard deviations, and number of sample) for each of the dependent variables and all other variables described below.

Table 3. *Descriptive Statistics*

Independent/Control Variables	Mean	SD	N
Internal firewall	.70	.45	68
Digital signature	.09	.29	65
Honeynet	.10	.30	68
Reference check-IT	.86	.33	69
Criminal check-IT	.60	.49	65
Identity management	.40	.49	66
Role-based access control	.55	.50	67
Intrusion prevention	.16	.37	65
Anti-virus	.97	.16	70
Spam filtering	.84	.36	71
Web content filtering	.10	.30	69
Bot monitoring	.26	.44	69
Monitoring rogue devices	.25	.44	70
Full-time IT staff	.43	.49	71
P2P monitor bandwidth	.75	.43	70
P2P shape bandwidth	.60	.49	70
Encryption data on hard drive	.09	.29	65
Encryption data for off-site	.23	.43	69
Information identity	.25	.43	72
US-CERT	.21	.40	72
US Department of Education	.65	.47	72
US Internal Revenue Service (IRS)	.57	.49	72
Physical separation	.46	.50	69
Encryption data in transit	.75	.43	69
Encryption data on network/computer	.27	.44	69
Student agree to cybersecurity policy	.46	.50	71
Affiliates agree cybersecurity policy	.25	.43	71
Warning banners	.65	.47	70
Restricted access to network	.66	.47	72
Cybersecurity education	.36	.48	72
Type of control	.50	.50	72
Urbanization	2.25	.83	72
Highest degree	3.2	1.4	72

Table 3. (Continued)

Dependent Variables	Mean	SD	N
DDOS attack	.50	.51	72
Website defacement	.22	.41	72
Unauthorized access	.38	.48	72
Exposure of private information	.21	.40	72
Theft of private information	.15	.36	72
Theft of intellectual property	.04	.20	72
Cyber-sabotage	.08	.27	72
Internet fraud	.07	.25	72
Bot hosting	.50	.51	72
Copyright infringement	.54	.50	72
Cybercrimes by count	2.69	2.16	72

Bivariate Associations

The analysis began by considering the relationships between each of the cyber-SCP techniques and each of the cybercrime types. This resulted in a series of 2*2 frequency tables that were examined using the Phi coefficient. The results of these equations are shown in Table 4, revealing some interesting patterns. First, different types of cyber-SCP techniques are associated with each of the cybercrimes. Second, overall, four cyber-SCP techniques (target hardening, controlling facilitators, entry/exit screening, and reducing temptation) were negatively related to the 10 types of cybercrime. Conversely, 10 cyber-SCP techniques (access control, formal surveillance, surveillance by employees, natural surveillance, target removal, denying benefits, rule setting, stimulating conscience, controlling disinhibitions, and facilitating compliance) were positively related to the 10 types of cybercrime.

Multivariate Models

More importantly, as a next step, the relationships between cyber-SCP techniques and the breadth of cybercrime types were assessed. This was considered with five Poisson regression equations. As Goodness of Fit Measures, Kolmogorov-Smirnov Test is not significant (Asymp. Sig: .208); thus, Poisson regression is deemed fit to analyze the dependent variable. Also, Pearson Chi-square value/df is close to 1, which indicates the model is a good fit for the data analysis. Finally, the omnibus test is statistically significant, which shows that the full model with all the independent variables is a major improvement over the intercept/baseline model.

Table 4. Phi Correlation Matrix for Cyber-SCP Techniques and Cybercrime Types

Cyber-SCP Techniques	Cybercrime Prevention Measures	1	2	3	4	5	6	7	8	9	10
Target hardening	Perimeter firewall		-.26*				-.26*				
	Internal firewall	-.27*	-.43***	-.24*	-.39**	-.41**				-.45***	-.28*
Access control	Digital signature						.55**				
Controlling facilitators	Reference check: IT staff									.28*	
	Criminal Background check: IT staff						-.29*				
	Identity management	-.31**								-.31**	
	Role-based access					-.39***				-.24*	
Entry/exit screening	Intrusion prevention							.28*			
	Anti-virus						-.38***				
	Spam filtering			-.24*		-.24*					
	Web content filtering									-.23*	
Formal surveillance	Bot monitoring									.25*	.33**
	Monitoring for rogue devices										.29*
Surveillance by employees	Full-time IT staff					.25*					.26*
Natural surveillance	P2P monitor bandwidth						-.37**			.23*	.28*
	P2P shape bandwidth									.29*	.30*

*** p < .05 (2-tailed); ** p < .01 (2-tailed); *** p < .001 (2-tailed); 1 = DDOS, 2 = Website defacement, 3 = Unauthorized access, 4 = Exposure of private information, 5 = Theft of private information, 6 = Theft of intellectual information, 7 = Cyber-sabotage, 8 = Internet fraud, 9 = Bot hosting, 10 = Copyright infringement.**

Table 4. (Continued)

Cyber-SCP Techniques	Cybercrime Prevention Measures	1	2	3	4	5	6	7	8	9	10
Target removal	Encryption data on hard drive			.330*				.421**			.304*
	Encryption backup data for off-site storage			.335*		314*		.341*			
Reducing temptation	US-CERT	-.239*					.235*				
	US Department of Education										-.320**
	IRS-Internal Revenue Service										-.237*
	Physical separation	-.344**			-.315**	-.317**			-.25*		-.455**
Denying benefits	Encryption data in transit										.278*
	Encryption data on network/comp	.283*				.263*			.32**	.283*	.248*
Rule setting	Student required to agree	.291*									
	Affiliates required to agree				.302*						
Stimulating conscience	Warning banners on the website									.316*	.336*
Controlling disinhibitions	Restricted access to network				.363**						.355**
Facilitating compliance	Cybersecurity education for student								.250*		

Table 5. Multivariate Models of Sixteen Cyber-SCP Techniques to Breadth of Cybercrime Types from Poisson Regressions

Opportunity-Reducing Strategies	Cyber-SCP Techniques	Cybercrime Prevention Measures	**Model 1** (N = 60)		**Model 2** (N = 69)		**Model 3** (N = 66)		**Model 4** (N = 69)		**Model 5** (N = 57)	
			EXP(B)	SE	*EXP*(B)	SE	*EXP*(B)	SE	*EXP*(B)	SE	*EXP*(B)	SE
Increase Efforts	*Target hardening*	Internal firewall	.44***	.16							.51**	.21
	Access control	Digital signature	1.18	.23							1.91*	.34
	Deflecting offender	Honeynet	.75	.26							.93	.32
	Controlling facilitators	Identity management	.72	.17							.91	.21
Increase Risks	*Entry/exit screen*	Spam filtering			.86	.20					.59*	.24
	Formal surveillance	Bot monitoring			1.33	.16					1.09	.23
	Surveillance by employ	Full-time IT staff			1.38*	.15					.91	.24
	Natural surveillance	P2P monitor bandwidth			1.03	.20					1.04	.31
Reduce Rewards	*Target Removal*	Encryption backup data for off-site					1.23	.18			1.37	.22
	Identifying property	Information identity					1.34	.16			1.33	.24
	Reducing temptation	Physical separation					.46***	.17			.74	.25
	Denying benefits	Encryption data on netw					1.39*	.16			.92	.23
Remove Excuses	*Rule setting*	Students agreed policy							.75	.16	.91	.20
	Stimulating conscience	Warning banners							1.41*	.16	1.60*	.23
	Controlling disinhibition	Restricted access to network							1.70**	.18	.82	.24
	Facilitating compliance	Cybersecurity education							1.13	.16	.90	.23
	Control Variables	Control by Pub/Pri/Mil									.75	.20
		Urbanization									.83	.13
		Highest degree									1.40***	.10
		Pearson x^2 value/df	1.32		1.68		1.36		1.64		1.06	
		Omnibus test sig.	.000		.024		.000		.005		.000	

*** p < .05 (2-tailed); ** p < .01 (2-tailed); *** p < .001 (2-tailed)**

The results for these equations are shown in Table 5. The variables for target hardening (internal firewall), entry/exit screening (spam filtering), and reducing temptation (physical separation) were statistically related to the breadth of cybercrime types. Specifically, target hardening (exp(B) = .51, $p < .01$), entry/exit screening (exp(B) = .59, $p < .05$), and reducing temptation (exp(B) = .46, $p < .001$) were negatively associated with the breadth of cybercrime types. In contrast, stimulating conscience (exp(B) = 1.60, $p < .05$) was positively associated with the breadth of cybercrime types. In sum, the evidence found throughout these analyses indicated that three cyber-SCP techniques – target hardening, entry/exit screening, and reducing temptation – may be the key components to preventing certain types of cybercrime activities or are at least the most commonly used.

Discussion

The malfunction or total loss of an information system from academic institutions can cause a tremendous amount of economic damage and is a massive security threat to the United States. Although scholars have begun to examine the applicability of the SCP theoretical framework in preventing cybercrime, no previous study has empirically assessed the relationships between SCP techniques and cybercrimes. In an effort to fill this gap in the literature, the present study addressed common cybersecurity measures and portrayed the concept of cyber-SCP techniques. In addition, this study explored the relationships between cyber-SCP activities and cybercrime types through bivariate analyses. Lastly, this study empirically investigated the applicability of 16 forms of cyber-SCP techniques in preventing cybercrime in the virtual world under the following categories: 1) increase effort, 2) increase risks, 3) reduce reward, and 4) remove excuses.

The findings of this study indicate that certain associations exist between cyber-SCP techniques and each of the cybercrime types. In fact, the results are mostly consistent with the existing literature (e.g., Clarke, 1992, 1997; Welsh & Farrington, 2004) pertaining to SCP theory – increasing a criminal's effort and risk, and removing the rewards of crimes – are substantially associated with crime preventions. Specifically, the results of this study lend support for the continued use of target hardening, entry/exit screening, and reducing temptation in directly or indirectly preventing crime in the online setting.

The results suggest that denying benefits (i.e., encryption data in transit, and encryption data on network or computer) measures were positively related to some types of cybercrime. Although existing literature argued that reducing the rewards (encryption data in transit, and encryption data on network or computer) can reduce cybercrime incidents, the findings do not confirm this prediction. The most likely explanation for this result is that encryption is easily hacked by interception tools for eavesdropping or impersonation of decryption methods (Holden, 2003). According to Holden (2003), transport method encryption cannot offer a high level of security against cyber-trespassing and eavesdropping. Consequently, one might expect a higher likelihood of cybercrime victimization experiences, instead of reducing the occurrence of the cybercrime. In short, these findings suggest that this prevention technique needs to be reexamined and improved to appropriately prevent cybercrime incidents in the future.

In line with the findings from Testa et al.'s (2017) study, these results demonstrate that a warning banner on websites did not deter cyber-perpetrators from committing crimes. In fact, the academic institutions who implemented warning banners on websites were more likely to experience cybercrime incidents (i.e., bot hosting and copyright infringement) than the academic institutions without it.

The current study was not able to reveal exactly why cyber-perpetrators committed cybercrimes against the academic institutions despite the displaying of warning banners. However, based on the studies of Testa et al. (2017) and Pogarsky (2002), this study can provide a possible explanation. In this regard, cybercriminals who have a high criminal efficacy and strong level of confidence can easily evade detection; therefore, they increasingly commit cybercriminal activities to achieve their goals, despite seeing sanction signs (Testa et al., 2017). In a broad sense, future research should consider uncovering the exact mechanisms that drive cybercriminals to continue their criminal behaviors in the presence of sanctioned threats in order to appropriately apply stimulating conscience strategies to the digital realm as an effective opportunity-reducing technique.

Policy Implications

With these thoughts in mind, it is important to discuss the policy implications of this study. Consistent with the application of SCP measures in physical environment, the continued use of (1) increasing the efforts (target hardening), (2) increasing the risks (entry/exit screening) of committing cybercrime, and (3) reducing the rewards (reducing temptation) can be effective ways to prevent cybercrime in online settings in higher education institutions. First, to increase the efforts of crime, target hardening techniques are represented as a feasible crime prevention strategy in most ordinary street crimes as well as cybercrimes (Crime analysis for problem solvers in 60 small steps, 2018). For example, target hardening (i.e., steering column locks) reduces burglary by making properties physically harder to break into. Likewise, firewall systems as a target hardening technique blocks access to the target or victim; thus, it can actively prevent cyber-intrusion and cyber-theft by making information systems and facilities among higher education institutions harder to penetrate. In other words, target hardening with firewall measures can lead cybercriminals to perceive crime opportunities (temptation) less attractive because the offender needs more effort to successfully break the law in the digital realm. Consequently, firewall systems provide strong digital guardianship; therefore, we must keep improving and executing this capstone of cybersecurity techniques for maximum efficacy in higher education institutions.

Second, offenders tend to worry more about the risks of being arrested than about the results if they are caught (Crime analysis for problem solvers in 60 small steps, 2018); therefore, increasing the risks of being apprehended, especially with entry/exit screening technique, may be effective to deal with crime in both the physical and online settings. Metal detectors and screeners are regarded as effective entry/exit screening techniques in that it allows only certain individuals admittance to the physical property of an organization (Hinduja & Kooi, 2013). In online settings, entry/exit screening systems such as spam filtering and intrusion detection systems can help to enhance the risks of being apprehended for cybercriminals. To better enhance the existing entry/exit screening systems in higher education institutions, artificial intelligence technology can be considered with the existing cyber-entry/exit screening systems. This is because artificial intelligence can enforce real-time detection or filtering, and then it is able to send quick alerts to cybersecurity staff and US-CERT team members using an artificial neural network and knowledge-based intrusion detection and filtering. Along with self-learning capabilities, artificial neural networks and knowledge-based intrusion techniques can be utilized to quickly identify suspicious and malicious behavioral patterns in cyberspace (Vieira, Schulter, Westphall, & Westphall, 2010).

In short, as explained above, increasing the risk of arrest can discourage cyber-perpetrators to commit cybercrime against higher education institutions since the cybercriminals will feel afraid of being caught via cutting-edge entry/exit screening systems. Thus, we can prudently pursue the application of artificial intelligence to improve the existing cybersecurity systems in order to effectively combat cyberattacks.

Third, offenders are always seeking the rewards of crimes; hence, if they do not see any benefit themselves by their crimes, they are less likely to commit crimes. To prevent street crimes, law enforcement officials advise people to hide their valuable assets so that criminals cannot see their properties as targets. Similar to crime prevention strategies for street crimes, removing temptation techniques (i.e., physical separation) for critical information and facilities in higher education institutions, might decrease the opportunities of perpetrators accessing these assets simply because they are not aware of whether or not valuable properties exist. Therefore, cybercrime can be discouraged when a potential offender does not perceive a situation as a criminal opportunity (the rewards of crimes) because they cannot see any attractive targets (values) through physical separation of critical information and facilities in higher education institutions.

In sum, the present study explores the applicability of ideas – cyber-SCP techniques – drawn from situation crime prevention theory to cybercrime. It is important to note that these policy implications will be both theoretical and practical benefits to create future cybercrime prevention strategies. Theoretically, research on criminal opportunities can lead to a better understanding of how and why cybercrime occur in particular cyber-environments. On the practical side, it can lead to a new approach of situational crime prevention to the cybercrime control. Particularly, this study provides further direction for cybercrime prevention strategies along with increasing the efforts, increasing the risks, and reducing the rewards of crimes.

Limitations

One of the issues that this study was not able to accurately explore was whether the experiences of cybercrime occurred before or after cyber-SCP techniques were implemented. The analysis could not establish correct temporal ordering – cybercrimes could have occurred before implementing cyber-SCP techniques among higher education institutions. This is because the analyses in this study were based on cross-sectional data collected at one point in time. To overcome this issue, future research should use longitudinal data to empirically examine the instantaneous and lagged relationship between cyber-SCP activities and the breadth of cybercrime incidents. Also, since this study utilized a small sample size data set (12 percent response rate), it is difficult to draw inferences about the generalizability of the findings. Furthermore, this data comes from 2005 – 2006 making the age of the data another limitation to this study. As a consequence, researchers should consider replicating this study in other academic institutions, as well as in the public and private sectors, so that more recent data and larger sample sizes can be explored. Nonetheless, the current study provides a valuable framework in which scholars, policy makers, and practitioners can apply cyber-SCP strategies to cybercrime prevention.

Conclusion

The present study explored and identified relationships between cyber-SCP techniques and several types of cybercrime. Furthermore, this study provides initial evidence that a diverse collection of cyber-SCP techniques might be effective in minimizing various types of cybercrime.

Most importantly, one of the major contributions of the present study is extending the focus of empirical applications of situational crime prevention techniques to criminal activities in the cyber world. This study demonstrated how situational crime prevention techniques might help stakeholders refine prevention efforts in cyber environments, which facilitate cybercrime through opportunity-reducing measures. Thus, consistent with previous research (e.g., Cornish & Clarke, 2003; Clarke, 1992, 1995, 1997; Guerette & Bowers, 2009; Shariati & Guerette, 2017), this study highlights the importance of SCP in preventing cybercrime and suggests the potential value of new scholarship in this emerging field.

Declaration of Interest Statement

The authors declare that they have no conflicts of interest.

References

Akers, R. L. (2013). *Criminological theories: Introduction and evaluation*. New York, NY: Routledge.

Beebe, N. L., & Rao, V. S. (2005, December). Using situational crime prevention theory to explain the effectiveness of information systems security. In *Proceedings of the 2005 SoftWars Conference, Las Vegas, NV* (pp. 1-18).

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.

Brantingham, P. L., & Brantingham, P. J. (1993). Nodes, paths and edges: Considerations on the complexity of crime and the physical environment. *Journal of Environmental Psychology*, *13*(1), 3-28.

Brantingham, P., & Brantingham, P. (1995). Criminality of place. *European Journal on Criminal Policy and Research*, *3*(3), 5-26.

Casey, E., Blitz, A., & Steuart, C. (2004). Digital evidence and computer crime. London: Academic Press.

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.* El Paso, TX: LFB Scholarly Publishing.

Clarke, R. V. (1980). "Situational" crime prevention: Theory and practice. *The British Journal of Criminology*, *20*(2), 136-147.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice*, *4*, 225-256.

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

Clarke, R. V. (1997). A revised classification of situational crime prevention techniques. *Crime Prevention at a Crossroads.* Cincinnati. OH: Anderson.

Clarke, R.V. & Homel, R. (1997). A revised classification of situational crime prevention techniques. In: Lab, S.P., ed. Crime prevention at the crossroads (pp. 17-27). Cincinnati, OH: Anderson

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

Cohn, C. (2015, July 8). Cyber attack on U.S. power grid could cost economy $1 trillion: report. *Reuters*. Retrieved from http://www.reuters.com/article/us-cyberattack-power-survey-idUSKCN0PI0XS20150708

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16,* 41-96.

Cornish, D. B., & Clarke, R. V. (2014). *The reasoning criminal: Rational choice perspectives on offending*. London: Transaction Publishers.

Coxe, S., West, S.G. & Aiken, S.L. (2009) The analysis of count data: A gentle introduction to Poisson regression and its alternatives. *Journal of Personality Assessment, 9*(2), 121-136.

Crime analysis for problem solvers in 60 small steps. (2018). In *Center for Problem-Oriented Policing*. Retrieved June 28, 2018, from http://www.popcenter.org/learning/60steps/index.cfm?stepNum=39

Eck, J. E., & Weisburd, D. L. (2015). Crime places in crime theory. In J. E. Eck & D. L. Weisburd (Ed.), *Crime and place,* (pp. 1-33). Monsey, NY: Criminal Justice Press.

Felson, M. (2017). Linking criminal choices, routine activities, informal control, and criminal outcomes. In D. B. Cornish & R. V. Clarke (Ed.), *The reasoning criminal: Rational choice perspectives on offending* (pp. 119-128). New Brunswick, NJ: Routledge.

Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief: Practical Theory for Crime Prevention. *Home Office Police Research Series, 98*, 1-36.

Ferrari, E. (Ed.). (2005). *Web and information security*. IGI Global.

Gini, G., Card, N. A., & Pozzoli, T. (2018). A meta-analysis of the differential relations of traditional and cyber-victimization with internalizing problems. *Aggressive Behavior*, *44*(2), 185-198.

Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention evaluations. *Criminology*, *47*(4), 1331-1368.

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, *26*(4), 383-402.

Holden, G. (2003). *Guide to network defense and countermeasures*. Boston, MA: Course Technology Press.

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

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

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

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.

Pogarsky, G. (2002). Identifying "deterrable" offenders: Implications for research on deterrence. *Justice Quarterly*, *19*(3), 431-452.

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.

Schneider, S. (2014). *Crime prevention: Theory and practice*. Boca Raton, FL: CRC Press.

Shariati, A., & Guerette, R. T. (2017). Situational Crime Prevention. In B. Teasdale & M.S. Bradley (Eds.) *Preventing Crime and Violence* (pp. 261-268). Cham, Switzerland: Springer.

Skopik, F., Bleier, T., & Fiedler, R. (2012). Information management and sharing for national cyber situational awareness. In H. Reimer, N. Pohlmann, & W. Schneider (Eds.) *ISSE 2012 Securing Electronic Business Processes* (pp. 217-227). Wiesbaden, Germany: Springer Vieweg.

Smith, M. J., & Clarke, R. V. (2012). Situational crime prevention: Classifying techniques using "good enough" theory. In D. Farrington & B.C. Welsh (Eds.) *The Oxford Handbook of Crime Prevention* (pp. 291-315). Oxford, England: Oxford University Press.

Stallings, W. (2003). *Cryptography and network security: principles and practice*. New Dehli, India: Pearson Education India.

State-sponsored cyber theft (2018, March 23). In The United States Department of Justice. Retrieved April 7, 2018, from https://www.fbi.gov/news/stories/nine-iranians-charged-in-hacking-scheme-032318.

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *40*(4), 853-865.

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers. *Criminology & Public Policy*, *16*(3), 689-726.

Thomas, D., & Loader, B. D. (2000). *Cybercrime. Law enforcement, security and surveillance in the Information Age*. London: Routledge.

Vieira, K., Schulter, A., Westphall, C., & Westphall, C. (2010). Intrusion detection for grid and cloud computing. *IT Professional*, *12*(4), 38-43.

Welsh, B. C., & Farrington, D. P. (2004). Surveillance for crime prevention in public space: Results and policy choices in Britain and America. *Criminology & Public Policy*, *3*(3), 497-526.

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

Willison, R. (2000). Understanding and addressing criminal opportunity: the application of situational crime prevention to IS security. *Journal of Financial Crime*, 7(3), 201-210.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organizational context. *Information and Organization*, 16(4), 304-324.

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.

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

Wright, M. F., & Li, Y. (2013). The association between cyber victimization and subsequent cyber aggression: The moderating effect of peer rejection. *Journal of Youth and Adolescence*, *42*(5), 662-674.

Appendix

Pearson r Correlation Matrix between Cyber-SCP Techniques and Breadth of Cybercrime Types

	CBC	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CBC	1																
1. IF	-.52**	1															
2. DS	.129	-.154	1														
3. HO	.049	-.030	.026	1													
4. IM	-.251*	.062	.083	-.039	1												
5. SF	-.082*	.005	-.011	.037	.161	1											
6. BM	.212	-.193	.052	.358**	-.129	-.037	1										
7. FIT	.253*	-.199	-.014	.079	.038	-.105	.121	1									
8. P2P	.121	-.130	-.221	.213	-.093	.150	.248*	.199	1								
9. EB	.288*	-.129	.142	.073	.035	-.067	.084	.141	.276*	1							
10. IC	.097	-.098	.052	.478**	-.114	.058	.120	.118	.010	-.098	1						
11. PS	-.45**	.409**	.026	-.003	.223	-.030	-.139	-.349**	.020	-.060	.109	1					
12. ED	.332**	-.024	-.082	-.050	-.288*	-.023	.221	.163	.202	.264*	-.05	-.167	1				
13. AA	.110	-.036	-.062	.075	-.052	.061	.115	.180	.093	.209	.107	-.136	.170	1			
14. WB	.138	-.192	.086	.114	.106	.029	.175	.208	.374**	.052	.156	-.093	.047	.159	1		
15. RA	.242*	-.34**	.014	.091	.024	-.059	.210	.206	.152	.189	.068	-.358**	-.027	.348**	.287*	1	
16. AP	.147	.004	.209	.156	-.048	-.010	.239*	.120	.214	.153	.167	.025	.210	.632**	.201	.286*	1

*** p < .05 (2-tailed); ** p < .01 (2-tailed); *** p < .001 (2-tailed);** CBC = Cybercrimes by Count, IF = Internal Firewall, DS = Digital Signature, HO = Honeynet, IM = Identity Management, SF = Spam Filtering, BM = Bot monitoring, FIT = Full-time IT Officer, P2P = P2P Monitor Bandwidth, EB = Encryption backup data for off-site storage, IC = Information Asset Classification, PS = Physical Separation, ED = Encryption Data on Network or Computers, AA = Affiliates Agree Cybersecurity Policy, WB = Warning Banners on Website, RA = Restricted Access to Network, AP = Affiliates Provided Cybersecurity Education.