Computers in Human Behavior 73 (2017) 394–402

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory

Kyung-Shick Choi [a], [b], [*], Jin Ree Lee [c]

[a] Department of Criminal Justice, Bridgewater State University, USA
[b] Department of Applied Social Sciences, Boston University, USA
[c] School of Criminal Justice, Michigan State University, USA

ARTICLE INFO

Article history:
Received 26 November 2016
Received in revised form
28 March 2017
Accepted 29 March 2017
Available online 31 March 2017

Keywords:
Cybercrime
Cyber-interpersonal violence
Cyber-routine activities theory
Lifestyle-routine activity theory
Victim-offender overlap

ABSTRACT

The current study provides an empirical testing of the victim-offender overlap in online platforms due to the scarcity of studies examining this overlapping victim-offending dynamic. Two types of cyber-interpersonal violence are examined: Cyber-harassment (including cyber-sexual harassment) and cyber-impersonation. Using Choi's (2008) integrated theory of Cyber-Routine Activities Theory, a sample of 272 college students at a Massachusetts university are examined. Three major findings are revealed: (1) Respondents who engage in risky online leisure activities are more likely to experience interpersonal violence in cyberspace, (2) poor online security management can contribute to the likelihood of being victimized by interpersonal violence on social networking sites (SNS), and (3) respondents who engage in risky social networking site activities are likely to commit cyber-interpersonal violence. For the two types of cyber-interpersonal violence examined in this study, it could also be predicted that females are more likely to have higher levels of victimization. Cybersecurity management and sex had no significant effects on cyber-interpersonal violence offending. The hope is that education on the potential hazards of the Internet and of cyber-interpersonal violence will induce more responsible online activity and engagement.

1. Introduction

The Internet, social networking sites (SNS), and online communications have all changed the way individuals communicate and interact worldwide. While many benefits have developed from such technological advancements, various hazards have also been documented to accompany this wave of digital progressivism. One of the more notable risks is the inception of cyber-interpersonal violence (e.g., Dredge, Gleeson, & de la Piedad Garcia, 2014; Fenaughty & Harre, 2013; Pereira, Spitzberg, & Matos, 2016). Using social media usage as an example, many routinely service these platforms to release personal information and pictures online without being cognizant of the fact that their actions may increase their vulnerability to cyber-harassment and identity theft (Shin, 2010). Though advancements in technology and online communications have made life unequivocally easier in many aspects, the ease by which potential offenders can access personal information online is a strong reason for concern and calls for more research to be done on the subject of cyber-interpersonal violence victimization and offending.

In an attempt to understand the potential consequences of online interpersonal activity, an earlier study conducted by Spitzberg and Hoobler (2002) found that 31% of undergraduate participants experienced some kind of personal online victimization. In a similar study conducted in 2011, 42% of social network users reported experiencing some form of interpersonal victimization online (Henson, Reyns, & Fisher, 2011). A more recent study conducted by Pereira et al. (2016) found that 69.9% of adolescents reported some level of cyber-harassment victimization in the past. Of that total, 60.8% reported being victims of repeated acts of cyber-harassment. The interesting element unique to online behaviors is that, unlike physical activities, cyber-acts bear the potential to affect all those who use the Internet, regardless of their usage capacity. In our heavily reliant and technologically-dependent society, this means that the vast majority of people are at risk. The widely-mistaken assumption that only risky online activities have the ability to propel one's status as a potential cyber-victim is simply inaccurate.

[*] Corresponding author. Department of Criminal Justice, 10 Shaw Road, Bridgewater State University, Bridgewater, MA 02325, USA.
E-mail address: kchoi@bridgew.edu (K.-S. Choi).

http://dx.doi.org/10.1016/j.chb.2017.03.061
0747-5632/Published by Elsevier Ltd.

Another characteristic unique to online behaviors is its lack of a concrete criminal jurisdiction in monitoring cyber-offenders. That is, investigating and prosecuting cybercriminals are often difficult because the behaviors take place over the Internet instead of in identifiable spatial locations (Choi, 2015). The absence of a specific location makes it very challenging for law enforcement authorities and policy makers to identify who the bearers of enforcing legal penalties are and what those penalties should be.

For the purpose of this study, the online behaviors that will be examined are computer-assisted forms of cyber-interpersonal violence. The two types of cyber-interpersonal violence that will be analyzed in this study are: Cyber-harassment (consisting of verbally harassing someone online, including the spreading of rumors, unwanted sexual photos without consent, and/or threatening individuals with or without sexual content), and cyber-impersonation (also known as 'catfishing', which involves individuals using other people's personal information and images in order to pose as someone they are not while being online). Although there are other notable types of cyber-interpersonal violence, only the two described here will be analyzed within the current study. The aim is to highlight the cyber-interpersonal violence most frequented among college populations. The reason for targeting the college population is due to the fact that young people represent a disproportionately high number of criminal activity and victimization in both online and offline settings (Cops & Pleysier, 2014).

As the scientific community begins to explore online behavior in greater detail, it will become increasingly helpful to both theorize and understand the possible factors that increase the likelihood of cyber-victimization and cyber-offending. This study thus serves to determine whether or not risky online lifestyle factors and cyber-security management influence cyber-interpersonal violence against individuals. An analysis identifying the possible factors that increase the likelihood of cyber-interpersonal victimization and offending will be conducted. It is hypothesized that those who engage in risky online lifestyle behaviors and do not effectively manage online security settings on social networking sites are more likely to engage in both cyber-interpersonal violence and experience cyber-interpersonal violence victimization. The theory used to conduct this analysis will be Choi's (2008) Cyber-Routine Activities Theory – an integrated theory based on the cores values of Cohen, Kluegel, and Land's (1981) Lifestyle-Routine Activity Theory. This theory will be applied to the examination of surveys completed by a sample of college students at a Massachusetts university. A theoretical application of the results will also be provided in offering suggestions for future research and possible policy implications.

2. Theoretical framework

2.1. Lifestyle-routine activity theory (LRAT)

Before discussing and engaging with Choi's (2008) Cyber-Routine Activities Theory, an understanding of its integrated theoretical roots must first be had. This brings us to a discussion on Cohen, Kluegel, and Land's (1981) Lifestyle-Routine Activity Theory (LRAT). The theory can be understood as proposing the idea that individual lifestyles and routine activities put people in risky situations that create criminal opportunities conducive to criminal victimization (Cohen, Felson, & Land, 1980, 1981; Miethe & Meier, 1994). As an integrated theory itself, LRAT stresses the idea that individuals encounter criminal events based on the types of places (settings) they spend their free time, the people with which they occupy their free time, and the kind of activities they engage in during their free time (Svensson & Pauwels, 2010). Ultimately, LRAT proposes that an individual's routine behaviors and lifestyle choices are what makes one a suitable target for criminal victimization (Cohen et al., 1981).

An interesting aspect of LRAT is that, while the theory was initially introduced as strictly a victimization theory (Chen, 2009; Cohen et al., 1981), there have been many successful attempts at empirically testing the theory to also explain for criminal offending behaviors (e.g., Miller, 2013; Nofziger & Kurtz, 2005; Pauwels & Svensson, 2011). However, despite the increasing number of studies using LRAT principles to explain for individual offending behaviors, empirical research on the victim-offending overlap is still relatively scarce (Cops & Pleysier, 2014; Pauwels & Svensson, 2011). That is, while many studies have identified offenders and victims of criminal events as sharing similar lifestyle characteristics and behavioral patterns (e.g., Chen, 2009; Gottfredson, 1984; Hindelang, Gottfredson, & Garofalo, 1978), very few have empirically tested the overlapping victim-offender dynamic in terms of whether or not one is influenced by the other.

Another notable aspect of LRAT is that, while the theory is mostly used to account for physical crimes, there are instances where components of the theory can be applied to online behaviors – that is, individuals can end up in places and times where they become suitable targets for victimization both in the online realm and in the physical world. An example of this is when a person posts information and/or indicators of their vacation plans online through social networking sites such as Facebook. By posting such information online about a specific place before leaving on vacation, these individuals have potentially opened themselves up to becoming victimized in not only the digital world, but also in the physical world. Therefore, while LRAT has been predominantly used to assess physical crimes and offline criminal behaviors, there have been attempts at using LRAT principles to also examine behaviors that account for online patterns and lifestyles (e.g., Holt & Bossler, 2009; Holtfreter, Reisig, & Pratt, 2008; Reyns, 2013).

2.2. Cyber-routine activities theory (Cyber-RAT)

While the aforementioned integrated theory accounts for criminality when potential offenders and victims come together within the same physical environment without the presence of a capable guardian, it does not adequately address victimization and offending that take place in non-physical terrains. This is because the theory values the physical convergence of space and time between the victim and offender. Given the rise of digital technology, the physical convergence of potential offenders and victims in time and space are no longer quintessential elements to engender victimization (Eck & Clarke, 2003; Holtfreter et al., 2008; Pratt, Holtfreter, & Reisig, 2010). Therefore, despite LRAT holding the capacity to explain various segments of victimization that occur at a distance, generating a revised conceptualization of the integrated theory to address online behaviors specifically is integral. The main benefit of a cyber-focused theory is that it would bring more accuracy and precision towards studies investigating online behaviors. In response to this need for a cyber-focused explanation to online behavior, Choi (2008) proposed an integrated theory reflecting the concepts of LRAT to individual victimizations of computer crimes called Cyber-Routine Activities Theory. Choi (2008) selectively conceptualized two causal factors that contribute to computer crime victimization: (1) The concept of digital guardianship such as cyber-security and (2) online vocational and leisure activities. While the theory's focus is primarily on computer hacking, the theory posits that it may also be used to account for other cybercrimes. Essentially, Choi's (2008) theory argues that online lifestyles and digital guardianship substantially contribute to computer-crime victimization.

It must be noted that while the principles of LRAT have been used to test for both victimization and offending patterns in the physical world, very few studies have tested for this victim-offender overlap for online behaviors (e.g., Pereira et al., 2016). That is, while studies individually examining online victimization (e.g., Chen, Beaudoin, & Hong, 2017; Dredge et al., 2014; Fenaughty & Harre, 2013) and offending (e.g., Patton et al., 2014) have been conducted, studies analyzing the online victim-offending overlap have been rather limited. Given that Choi's (2008) theory roots its basic tenants in LRAT principles (with modifications to adjust for the online elements), the research endeavor should not come off as being unconventional and irrational – especially since related tests have been conducted using similar core principles but on physical crimes. Stated differently, the present research attempts to do what studies have done on physical crimes, but to the digital realm. This study will, therefore, analyze cyber-interpersonal violence victimization and offending using Cyber-RAT's three quintessential components: A potential offender, a potential target, and a virtual network (Eck & Clarke, 2003; Tillyer & Eck, 2009, pp. 279–287).

For the purposes of this research, risky online lifestyles of social networking sites and online security management will be examined. To briefly explain these variables: Social networking sites are websites that connect people by allowing them to share interests and activities with friends, family, colleagues, and others with similar interests (Shin, 2010). Some examples of social networking sites are: Facebook, Instagram, Twitter, Tumblr, and Snapchat. While social networking sites might differ in their function, they all share the same motive in allowing users to interact with others instantaneously using digital profiles and online messaging. Risky online behaviors, on the other hand, are activities that take place online and can be, but are not limited to, behaviors considered outside the norm of society. Since this study's focus is on cyber-interpersonal violence, risky online behaviors will be conceptualized as social networking, vocational, and leisure activities performed online. Digital capable guardianship, the last variable within this study, is conceptualized as online privacy settings on personal networking sites. There are two main types of security management available to social network users: User controls and profile controls. User controls are functions that allow users to decide who has access to their social media profiles, whereas profile controls allow individuals to control what aspects of their online profiles are made accessible to their friends. Digital capable guardianship will be measured by conceptualizing the varying levels of online security management used within social networking site platforms. A further explanation of the measurements and definitions will be discussed in the methodology sections of this study.

3. Methodology

3.1. Data and sample

Data was collected from self-report surveys given to a random sample of college students from a Massachusetts university in the spring of 2014. In order to reflect the entire university population, stratified-cluster random sampling was used. First, the full list of liberal studies classes that were available during the spring 2014 semester were entered into the Statistical Package for the Social Sciences (SPSS). These liberal studies classes are breadth requirement modules required for all students, regardless of their major. That is, although students have the option to choose which classes to enroll in, classes from this list are required in order to fulfill the university's degree requirement. Once the class list was entered into SPSS, it was stratified by class level (e.g., freshman/100 level classes, sophomore/200 level classes, and upperclassmen/300 and 400 level classes). A proportionate sub-sample of classes were then randomly selected using SPSS. In essence, a list of the university's entire liberal studies breadth requirement classes available during the spring 2014 semester were entered into SPSS. From this list, the SPSS random number generator randomly selected 10 classes based on their class level for inclusion in the sample.

With regards to class selection, 39 initial classes were randomly selected using SPSS to fulfill the requirement of a 10-class minimum. However, only four of the randomly selected classes agreed to be surveyed. This was due to the survey being administered at the end of the semester nearing the institution's final exam period. As a result, additional classes had to be generated from the SPSS random generator list. In the end, an additional 11 elective classes from the SPSS random generator list were gained, bringing the total number of classes surveyed to 15. A total of 272 respondents participated in the study, meaning a sample of 272 surveys were analyzed for this project.

The current study used the survey instrument to assess cyber-interpersonal violence among the college population. There are advantages in using university students as the target sample for the proposed study. First, university students are expected to be literate and familiar with self-report surveys. Second, university students are expected to be regular users of computers because of both its low cost and its frequent usage in classroom settings. Furthermore, university students are also noted to frequently use the Internet and their computers for entertainment purposes, thereby underscoring their familiarity with the platform. Finally, younger generations have been using computers for most of their lives and are more likely to see them as a necessity than an auxiliary.

Table 1 below presents four specific demographic items (age, sex, race, and class) that highlight comparisons between the population and the sample. Even though this sample cannot be considered representative of the holistic population on the basis of the compared sample and population demographic, the composition of the sample is not a major concern in this study. This is because the study is more concerned with victimization rates and instances of risky online behavior than with who participated in the study.

3.2. Properties of measures: cyber interpersonal violence and abuse

As previously mentioned, the current study will focus on two cyber-interpersonal violence behaviors that are committed against individuals. Yar (2005) categorizes cyber-interpersonal offenses as: (a) cyber-violence, (b) cyber-deceptions, and (c) cyber-pornography. The two cyber-interpersonal violence behaviors were thus chosen based on Yar's (2005) conceptualization of these actions. All variables used within this analysis are described in Table 2.

Given Yar's (2005) proposed definitions, the definition of cyber-interpersonal violence victimization in this study was operationalized consisting of five different types of self-report survey questions asking whether or not: (1) “Your private photos spread over the Internet in the past 12 months”; (2) you have “received illegal sexual contents through the Internet without consent in the past 12 months”; (3) you have “been verbally harassed on the Internet in the past 12 months”; (4) you have had “rumors spread about you over the Internet in the past 12 months; ” and (5) if you had “been threatened over the Internet in the past 12 months.” Using a binary scale, these items were summed to create one variable and then recorded with “yes” as 1 and “no” as 0. The possible range for cyber-interpersonal violence victimization was between 0 and 5, with greater numbers representing a higher number of victimization. The mean of the cyber-interpersonal violence victimization score for this sample was .31, with a standard deviation of .80, a skewness of 2.96, and a kurtosis of 9.10. Cyber-interpersonal violence

Table 1
Comparison of sample and population on available demographic characteristics.

Demographic characteristic	A undergraduate student population (N = 9684)	Study Sample (N = 272)
Age		
Mean Age	22	21.32
Sex		
Female	58% (n = 5635)	49.6% (n = 135)
Male	42% (n = 4049)	50.4% (n = 137)
Race		
White	83% (n = 8065)	83.4% (n = 226)
Non-White	17% (n = 1619)	16.6% (n = 46)
Class		
Freshman	19% (n = 1826)	7% (n = 19)
Sophomore	21% (n = 2074)	31.6% (n = 86)
Junior	27% (n = 2594)	31.3% (n = 85)
Senior	32% (n = 3057)	29.8% (n = 81)
Other	1% (n = 133)	0.4% (n = 1)

Table 2
Measures for the analysis of cyber interpersonal violence & Abuse. Model.

Variable	Label	Scale	Mean (s.d.)
Endogenous Variables			
Cyber Interpersonal Violence Victimization (observed variable consisting of …)	CIV_V	Range: 0–1	.31 (.80)
Have your private photos spread over the Internet in the past 12 months	CIV1_V	0 – no	.02 (.14)
Received illegal sexual contents through the Internet without consent in the past 12 months	CIV2_V	1 – yes	.03 (.18)
Been verbally harassed on the Internet in the past 12 months	CIV3_V		.11 (.32)
Have rumors spread about you over the Internet in the past 12 months	CIV4_V		.08 (.28)
Been threatened over the Internet in the past 12 months	CIV5_V		.06 (.24)
Cyber Interpersonal Violence Offense	CIV_O	Range: 0–1	.60 (6.37)
Verbally harassed someone on the Internet	CIV1_O	0 – no	.07 (.26)
Impersonated someone online	CIV2_O	1 – yes	.02 (.15)
Spread rumors online	CIV3_O		.04 (.19)
Threatened someone online	CIV4_O		.02 (.13)
Exogenous Variables: Risky Online Lifestyle Factors			
Sex	SEX	0 = female	.50 (.50)
		1 = male	
Cyber Risky Social Networking Site (SNS) Activities (factor consisting of …)	CR_SNS	Range: 1–5	
Share most of my life events through SNS	CR_SNS1	1 = strongly disagree	2.96 (1.21)
Express my opinions and feelings through SNS	CR_SNS2	2 = disagree	2.88 (1.16)
Offer a lot of personal information through SNS	CR_SNS3	3 = neutral	1.90 (.84)
Frequently write about my life on SNS	CR_SNS4	4 = agree	2.23 (1.11)
Express my opinions with honesty on SNS	CR_SNS5	5 = strongly agree	3.12 (1.17)
Express my feelings on SNS	CR_SNS6		2.51 (1.20)
Express myself on sensitive issues through SNS	CR_SNS7		2.02 (.96)
Cyber Risky Leisure Activities (factor consisting of …)	CR_L	Range:1–5	
Downloaded free games	CR_L1	1 = strongly disagree	2.11 (1.02)
Downloaded free music	CR_L2	2 = disagree	2.56 (1.27)
Downloaded free movies	CR_L3	3 = neutral	2.21 (1.14)
		4 = agree	
		5 = strongly agree	
Cyber Risky Vocational Activities (factor consisting of …)	CR_VC	Range: 1–5	
Opened any email attachments	CRL_VC1	1 = strongly disagree	2.90 (1.28)
Opened any files sent via instant messaging	CRL_VC2	2 = disagree	2.55 (1.20)
Clicked on any website links	CRL_VC3	3 = neutral	2.53 (1.23)
Clicked on any pop ups	CRL_VC4	4 = agree	1.82 (.87)
		5 = strongly agree	
Social Networking Site Security(CG_Security)	CG_SCT	Range:1–5	3.91 (1.06)

victimization was labeled as “CIV_V,” as shown in Table 2.

The second response variable was cyber-interpersonal violence offending, consisting of: (1) “Verbally harassed someone on the Internet”; (2) “impersonated someone online”; (3) “spread rumors online; ” and (4) “threatened someone online.” These items were also summed using a binary scale to create one variable and then recorded with “yes” as 1 and “no” as 0. The possible range for cyber-interpersonal violence offending was between 0 and 4, with greater scores representing a higher number of offending. The mean of the cyber-interpersonal violence offending score for this sample was .15, with a standard deviation of .56, a skewness of 4.69, and a kurtosis of 24.17. Cyber interpersonal violence offending was labeled as “CIV_O.” It is worth noting that the measures of cyber-interpersonal violence victimization and offending were designed to capture the constructs prescribed by Yar's (2005) description of what constitutes an act of cyber-interpersonal violence (see also studies conducted by Reyns, Henson, & Fisher, 2015; Pereira et al., 2016 for the use of these constructs and variables).

3.3. Properties of measures: cyber-routine activities theory (Cyber-RAT)

Framed within a re-conceptualized modification of LRAT, the major predictors in this study involved the following risky online lifestyles: (1) Cyber risky social networking site activities; (2) cyber risky leisure activities; and (3) cyber risky vocational activities – as shown in Table 2. Through these measures, it is assumed that instances of cyber-interpersonal violence happen by way of network interaction rather than a convergence in time and place between the potential offender and victim. In other words, cyber-interpersonal violence can be explained using the following three components: A potential offender, a target, and a network reconceiving the divergence of a potential offender and victim in space.

Regarding the first measure of risky online lifestyle, seven survey items were operationalized to constitute risky social networking site (SNS) activities: (1) "Share most of my life events through SNS"; (2) "express my opinions and feelings through SNS"; (3) "offer a lot of personal information through SNS"; (4) "frequently write about my life on SNS"; (5) "express my opinions with honesty on SNS"; (6) "express my feelings on SNS"; and (7) "express myself on sensitive issues through SNS." The survey items chosen for this variable all pertain to what one chooses to share on social networking sites such as personal information, thoughts, and opinions. Respondents were asked to indicate their answer by selecting the box that best fit their feelings towards the given statements ranging from "strongly disagree" to "strongly agree." The measures were designed to capture the constructs prescribed by Yar's (2008) description of risky online behaviors (see studies also conducted by Ngo & Paternoster, 2011; Dredge et al., 2014; and Pereira et al., 2016 to view the use of these constructs and variables). The scale's possible aggregate range was 6–30 with greater scores reflecting higher levels of risky social networking site activity. The Cronbach's alpha was an acceptable .85, suggesting that the items are very compatible and valid. Also, the Kaiser-Meyer-Olkin (KMO) was .845. A principle component analysis was used to create a "cyber risky social networking site activities" variable labeled "CR_SNS."

The second measure of risky online lifestyles consisted of three survey items that constituted online risky leisure activities: (1) "Downloaded free games," (2) "downloaded free music," and (3) "downloaded free movies." The Cronbach's alpha score for this measure was .695, thereby falling within the acceptable range. This indicates that behaviors regarding the illegal downloading of music, movies, and games are all related topics that can be successfully merged together. Furthermore, the KMO score was .67, which was just acceptable enough to conduct the principle component analysis. This cyber risky leisure activities variable was created and subsequently labeled as "CR_L."

The third measure of risky online lifestyles consisted of four survey items to create risky vocational activities: (1) "Opened any email attachments," (2) "opened any files sent via instant messaging," (3) "clicked on any website links," and (4) "clicked on any pop ups." Respondents were asked to indicate their level of agreement by selecting the box with responses ranging from "strongly disagree" to "strongly agree". The scale's possible aggregate range was 4–20 with greater scores reflecting higher engagement in risky vocational activities. The Cronbach's alpha was .75, and the KMO was .701, which were both acceptable to conduct the principal component analysis in order to create the variable, cyber risky vocational activities labeled "CR_VC." It is worth noting that both the second and third measure of risky online lifestyle (risky leisure activities and risky vocational activities) were designed to capture the constructs prescribed by Choi's (2008) initial study (see study conducted by Choi (2008) to view the use of these constructs and variables).

Before engaging in an analysis of these measures and variables, an interesting aspect to consider is the possible relation and pairing between variables. For instance, a lack of online security management can also be considered a risky online lifestyle choice because it has the potential to increase both one's susceptibility to an invasion of privacy, as well as other types of computer crimes such as hacking and identity theft. Online security management can, therefore, be both simple and advanced depending on how consciously one's cyber security is managed. That is, it can be as simple as blocking access to a social networking site to unwanted individuals and as advanced as downloading anti-virus software and proxies. While the lack of online security may not definitively lead to online victimization, poor social network security management can elevate one's potential victimization online. The poor management of online security – such as not engaging in privacy protection on social networking sites – can thus allow anyone with access to the website the ability to view one's profile and gather information on the potential victim. This can lead to cases of cyber-sexual crimes, which can further lend itself into the physical world.

Therefore, in order to accommodate for this variable association, social networking site security was included and framed within the study, asking respondents whether or not they "set strict privacy settings on who can see my SNS contents." Like the others, this also ranged from "strongly disagree" to "strongly agree," and was reversely recorded to capture the level of inadequate online security management. However, unlike the other online risky lifestyle variables, this was categorized as an observed variable. This measure was designed to capture the constructs prescribed by Choi's (2008) initial study (see also studies conducted by Chen et al., 2017; Reyns et al., 2015; and Ngo & Paternoster, 2011 to see the applicability of these constructs and variables).

4. Analysis

For individuals who were victimized at least once, the response variables were counted based on the number of times they were victimized. The distribution of victimization showed extreme positive skewness and extreme outliers in the data due to the small victimization rate, which may indicate violations in the assumption of homogeneity of error variance (Osgood, Wilson, O'Malley, Bachman, & Johnston, 1996). For this reason, it was determined that the dependent variable responses would be treated on a dichotomous scale (no = 0, yes or more = 1). This measure was sought to be appropriate for analyzing the data and determining any such relationships.

Given the response variable's dichotomous scale, it is impossible to satisfy the required assumptions of the multiple linear regression such as normality, homoscedasticity, and linearity. This is because the sample cannot be normally distributed with a constant error variance. Thus, the sample was divided into two subgroups based on all combinations of predictors. Consider each group of a population as π_1 and $\pi_{2.}$ It defines two regions: R_1 and R_2. The density of X in π_g is f_g (x), g = 1, 2. Errors were classified following:

$$P(2|1) = P(X \in R_2|G = 1) = \int_{R_2} f_1(x)dx$$

$$P(1|2) = P(X \in R_1|G = 2) = \int_{R1} f_2(x)dx,$$

where P(1|2) is the conditional probability, the basic result is:

$$\ln[f_1(x)/f_2(x)] = (\mu_1 - \mu_2)'\sum^{-1}[x - 1/2(\mu_1 + \mu_2)]$$

Given the model with several predictors, $(z_{j1}, z_{j2,\ldots,} z_{jr})$ was viewed as the values of the r predictors for the j-th observation. As in normal linear regression, it is customary to set the first entry that is equal to 1 and $z_j = [1, z_{j1}, z_{j2,\ldots}, z_{jr}]'$. It is assumed that the observation Yj is Bernoulli with probabilities that the event occurs, p (Zj), relying on the values of the covariates. Then:

$$P(Yj = yj) = pyj(Zj)(1 - p(Zj))1 - yi, \quad \text{for } yj = 0, 1$$

$$\text{So, } E(Yj) = p(Zj) \quad \text{and} \quad Var(Yj) = p(Zj)(1 - p(Zj))$$

However, observation Yj with Bernoulli does not follow a linear regression. Thus, taking the log of the odds ratio is necessary following:

$$\begin{aligned} Ln(p(z)/1 - p(z)) &= ß_0 + ß_1 z_1(SNS) + ß_2 z_2(LS) + ß_3 z_3(SCT)\cdots \\ &\quad + ß_r z_r \\ &= ß\prime z_j, \end{aligned}$$

where $\beta = [\beta_0, \beta_1, \ldots, ß_r]'$.

In the logistic regression model, the link between several predictors was examined. It is necessary that the observations are independent and that the model is correctly specified, including all necessary predictors. Finally, a linear relationship between each predictor and the log of the ratio of the probabilities was found (Cox et al., 2005).

5. Results

The model used in this study is a first-order multivariate model that regressed both cyber-interpersonal violence victimization and offending on cyber risky social networking site activities (CR_SNS), cyber risky leisure activities (CR_L), capable guardian_ security (CG_SCT) as an online risky lifestyle, as well as sex as a control variable. All other indicators of online risky lifestyles were not displayed in the main findings in Table 3 because of the possibility of having non-significant variables alter the effects of the significant predictors. Thus, the variable of risky vocational activities was excluded in the basic model. The model fit indices for the model demonstrates an acceptable fit to the data with RMSEA = .081, CFI = .90, and TLI =.82. This is because the values of CFI, and not TLI, fell above .90 despite RMSEA being greater than .05 (see Table 4).

Within the first model of victimization, the findings provided empirical evidence supporting Choi's (2008) Cyber-Routine Activities Theory in that risky online lifestyles were positively related to the risks of cyber-interpersonal violence victimization, and poor security management also positively related to cyber-interpersonal violence victimization. One of the core measures in cyber risky leisure activities (CR_L) significantly predicted cyber-interpersonal violence victimization ($p < .001$), while risky social networking site activities (CR_SNS) was found to be non-significant. According to this result, respondents who engage in risky online leisure activities are more likely to experience interpersonal violence in cyberspace. However, individuals with risky social network activities on risky social networking sites were not significantly related to cyber-interpersonal violence victimization. Although the measures were from the theoretically driven model, the findings in the statistical model did not match the theoretical model well.

Based on the findings, online security management was also considered a risky online lifestyle. A lack of security management on SNS was significantly related to cyber-interpersonal violence victimization ($p < .01$). This means that college students with a lack of online security management (e.g., "set strict privacy settings on who can see my SNS contents") are more likely to experience cyber-interpersonal violence. Poor online security management, which allows anyone to view personal information on online platforms, can contribute to the likelihood of being victimized by cyber-interpersonal violence.

As shown in Table 3, sex was also a significant factor that contributed to explaining the risks of cyber-interpersonal violence and risky online behaviors ($p < .05$). For the types of victimization examined in this study, it could be predicted that females are more likely to experience higher levels of cyber-interpersonal violence victimization. This means that females are more likely to be targeted for cyber-interpersonal violence than males.

In the second model, cyber-interpersonal violence offending was labeled as "CIV_O". Contrary to the first model, only one variable − risky social networking site activities (SNS) − significantly predicted cyber-interpersonal violence offending ($p < .01$), with risky leisure activities (LS) being insignificant. This means that college students with risky social networking site activities (SNS) are more likely to engage in cyber-interpersonal violence. Unlike the first model, there were no significant effects of online security management and sex on offending.

When examining the overall factors contributing to victimization risk, in addition to risky online activities on social networking sites, sex was found to be a significant factor in victimization risk in model 1. Thus, the next model examined the moderating effects of sex with the three risky online activities on cyber-interpersonal violence victimization and offending. The model fit indices for the model is demonstrated with RMSEA = .058, CFI = .952, and TLI = . 914 for male college students and RMSEA = .078, CFI = .905, and

Table 3
Zero-order and first-order and multivariate effects on cyber interpersonal violence & Abuse.

Regression Weights	Model 1	Model 2
	Cyber Interpersonal Violence Victimization (CIV_V)	Cyber Interpersonal Violence Offending (CIV_O)
	Estimate (S.E.)	Estimate (S.E.)
Sex (Female)	.285* (.103)	.147 (.801)
Risky Online Lifestyle Factors		
Cyber Risky Social Networking Site Activities (CR_SNS)	.061 (.098)	1.923** (.795)
Cyber Risky Leisure Activities (CR_L)	.403*** (.124)	.136 (.800)
Capable Guardian_ Security (CG_SCT)	.126** (.06)	.538 (.423)
Model Fit		
RMSEA	.081	.076
CFI	.880	.899
TLI	.809	.818

Note: ML coefficients reported with standard errors in parentheses.
***p≤ .001; **p≤ .01.; *p≤ .05.

Table 4
First-order and multivariate effects on cyber victimization and offending for both males and females.

Regression Weights	Model 1		Model 2	
	Cyber Interpersonal Violence Victimization (CIV_V)		Cyber Interpersonal Violence Offending (CIV_O)	
	Estimate (S.E.)		Estimate (S.E.)	
Risky Online Lifestyle Factors	Males	Females	Males	Females
Cyber Risky Social Networking Site Activities (CR_SNS)	.167 (.100)	−.026 (.063)	.265 (.322)	.021 (.037)
Risky Leisure Activities (CR_L)	.220 (.102)*	.047 (.055)	−.136 (.283)	.015 (.031)
Capable Guardian_ Security(CG_SCT)	.107 (.038)*	.014 (.035)	.004 (.126)	.008 (.020)
Model Fit				
RMSEA	.058	.078	.058	.078
CFI	.952	.905	.952	.905
TLI	.914	.831	.914	.831

Note: ML coefficients reported with standard errors in parentheses.
***p≤ .001; **p≤.01.; *p≤.05

TLI = . 831 for female college students. The statistical model showed a good fit for males. This is because the values of CFI and TLI for males fell above .90 although RMSEA was around .05. For females, the model fit was at a borderline acceptable range because CFI was greater than .90, although TLI was less than .90 and RMSEA was greater than .078.

For the victimizations examined in this study, it could be predicted that females are more likely to have higher levels of cyber-interpersonal violence victimization. This can be perceived as legitimate because of the risk factors considered: Females are more likely to use social networking sites (74%) when compared to males (72%) (e.g., Brenner & Smith, 2013). This means that females have higher chances of being targeted for cyber-interpersonal violence through social networking sites because they are more readily available than males. According to this study, however, male college students who were involved in risky online leisure activities and had poor online security management were more likely to be victimized. Findings such as the one generated from this study, as well as from previous research like the one conducted by Brenner and Smith (2013), serve to demonstrate that sex can be an important factor in both offending and victimization behaviors.

In the following section, the two cyber-interpersonal violence victimizations evaluated in this study are discussed. In addition to the three models, the relationship between cyber-interpersonal violence offending and victimization are examined.

6. Discussion

The current study sought to explore how online lifestyles and cyber-security management variables affect the likelihood of both cyber-interpersonal violence victimization and offending among a sample of college students. This study hypothesized that risky online lifestyles, as well as inadequate cyber-security management, would increase the likelihood of engaging in and experiencing cyber-interpersonal violence.

According to the findings of this study, the Cyber-RAT elements that had significant effects on the likelihood of cyber-interpersonal violence victimization are somewhat consistent with the original hypothesis: Those who engage in risky online behaviors and do not adequately manage their cyber-security are more likely to experience cyber-interpersonal violence victimization. With regards to offending patterns more specifically, only one of the tested variables rendered a significant relationship – namely, risky social networking site activities. While the relationship provided to be significant and thus, serves as an indicator of cyber-interpersonal violence offending, it must be noted that the relationship is an indirect one. What this means is that there might be other factors and contributors influencing this relationship. Reviewing all the activities listed under the risky social networking site activities label, it can be argued that the items may be relevant to individuals' level of self-control – or a lack thereof. A study conducted by Donner, Marcum, Jennings, Higgins, and Banfield (2014) empirically tested Gottfredson and Hirschi's (1990) Self-Control Theory on non-digital piracy online deviance perpetration and highlighted the theoretical relevance of low self-control on cyber-offending behaviors. Therefore, while the present study did reveal a significant relationship between risky social networking site activities and the propensity to engage in cyber-interpersonal violence offending, there may be a need to further investigate this offender/offending dynamic using other theoretical principles.

Overall, the findings uncovered within this study are significant to the theory's development because it expands its capabilities to explain for not only computer-focused crimes such as hacking, but also for computer-assisted crimes such as cyber-interpersonal violence. This means that the theory is appropriate and capable of accounting for various different types of online behaviors. Furthermore, this study is important to both current and emerging literature because researchers and policy makers can use this information to better understand the online lifestyle factors that may contribute to the varying types of cyber-interpersonal violence. This suggests that education and prevention policy efforts can be designed and/or reconfigured to reduce the risk of both cyber-interpersonal violence victimization and offending patterns, while simultaneously making the Internet a safer place for individuals of all ages and sex to interact and engage with on a routine basis.

6.1. Policy implications

Considering Cyber-RAT, LRAT, and other social learning perspectives, the policy implications related to the current study are focused on education and prevention. Similar to Flick's (2009) claim, the current study proposes a policy approach towards prevention rather than prosecution. One of the most promising approaches to cyber education and prevention is the "Stop.Think.Connect" campaign presented by the Department of Homeland Security. According to the department's website, the campaign is a national public awareness initiative aimed at increasing the understanding of cyber-threats and empowering the American public to be safer and more secure online (Stop.Think.Connect, 2015). The purpose of the campaign is to equip educators and community leaders with the resources necessary for discussions on online safety. This general approach can be broken down into three steps: Stop, think, and connect.

The first step urges participants to stop others from accessing their accounts by setting secure passwords and restraining themselves from excessively sharing personal information online. This step is directly aligned with the current study's interest in online identification (concealing identity) and risky online SNS activity. The second step asks participants to "think before you click". The campaign advises people to carefully assess whether or not a given website is trustworthy – that is, "is this a trusted source?" This step directly relates to the Cyber-RAT variable for risky online vocational activity, which includes opening files, attachments, pop ups, or website links from emails or unknown webpages. Being naïve to the dangers of the Internet and freely opening unknown attachments and links may increase the likelihood of an individual continuing serious forms of online behavior. The final step urges participants to knowingly connect with others online. For example, people should be aware that not all Wi-Fi hotspots offer the same protections and that if a connection or site does not seem right, individuals should close the application or delete the file. This step is related to the measure of risky online leisure activity, which includes downloading free games, music or movies from unknown websites.

Another suggestion to improve policy is to include components of social learning theory to its foundations. For example, in order to incorporate the concept of differential association, the "Stop.-Think.Connect" campaign would benefit from including a section of its education policy on why Internet users should be cautious about who they become friends and acquaintances with online. Such educational initiatives will not only reduce potential victims from being involved in such online conflicts, but the hope is that there will be fewer opportunities for offenders to engage in online offences if more people are exposed to these types of educational programs. It is, therefore, imperative that people who use the Internet – which ranges from adolescents to college students to older adults – are educated on the potential dangers of navigating the web.

6.2. Limitations and future research

One of the major limitations of the present study is its use of only one variable to measure cyber security management – namely, whether or not an individual set strict privacy settings on who can view their SNS contents. While the study chose to only incorporate this item in its analysis, the authors are cognizant of the fact that this component is not the only one applicable to matters pertaining to online security management. In other words, while it may be the most viable and apropos to cyber security management, it is not the only indicator and/or measurement of cyber security management. In addition, the lone item used in this study is a function residing solely on Facebook. This poses a significant limitation to the entire measurement of cyber security because Facebook is not the only social networking site and/or social media platform used by individuals. While an argument can be made that Facebook is the most widely used social networking forum, the study did not adequately explore all other SNS functions equally in its assessment of cyber security management. Future studies should strive to incorporate other SNS platforms more explicitly within their examinations, as well as the security functions provided to users within their particular forums. Doing so would constitute a more complete and comprehensive understanding of online security management within frequented social networking sites.

Another notable limitation within the current study is its failure to test for other theories that may influence cyber-interpersonal violence offending. As previously mentioned in the discussions section, the present study's discovery of a significant relationship between risky social networking site activities and cyber-interpersonal violence offending can be explained using other theories and directions such as social learning principles and Gottfredson and Hirschi's (1990) Self-Control Theory (e.g., an empirical study conducted by Donner et al. (2014) highlighted the aptness of self-control in assessing online deviance perpetration among other such cyber-offending behaviors). While the current study found a significant relationship between the two variables, it must be noted that the relationship is an indirect one. This means that there may be other factors contributing to this relationship.

Social learning principles can also contribute to the cyber-offending dynamic in that cyber-aggression can be developed by one's online interactions with significant others. Given that parental monitoring is a non-factor in cyberspace, the influence of peers, acquaintances, and significant others online can be argued to be substantial in shaping one's behavioral patterns online. While this is not to devalue the findings outlined within the present study, it is a statement addressing the fact that risky SNS activities can also be linked to levels of self-control and social learning principles.

Another observable limitation of the study is the use of self-report data. Given that the study asks personal questions through a self-report survey medium – such as whether or not respondents committed cyber-interpersonal violence – the possibility of participants hiding their true behaviors due to the sensitivity of the questions must be considered. Even if the questions being asked were not sensitive in nature, since the survey was conducted through a self-reporting process, the possibility of retaining inaccurate and/or misleading data must be taken into consideration.

Therefore, while the present study did reveal a significant relationship between risky social networking site activities and the likelihood of engaging in cyber-interpersonal violence offending, future studies would greatly benefit from investigating this offender/offending dynamic using other theoretical frameworks as well.

7. Conclusion

Although the phenomenon of cyber-interpersonal violence is still relatively new to scientific research, enough information is available to make a strong case and argument that it is a serious problem and one that requires more research. It is important not only to study the risks and effects of victimization, but also to focus on offending behaviors. The current study, thus, provides an explanation for the victim-offender overlap in instances of cyber-interpersonal violence using Choi's (2008) Cyber-Routine Activities Theory. Furthermore, the present study argues that if we educate people on the potential dangers of the Internet and of cyber communications, perhaps they will engage more responsibly online and the Internet will be a safer place to carry on daily lifestyle routines and activities.

Using techniques supported by existing literature, this study applied Cyber-RAT to cyber-interpersonal violence among a sample of college students. While the study yielded significant results, it is important to keep in mind the limitations previously discussed. It is the hope of the researchers that the current study will assist in furthering the understanding of cyber-interpersonal violence victimization and offending.

References

Brenner, J., & Smith, A. (2013). *72% of online adults are social networking site users*. Washington, DC: Pew Internet & American Life Project.

Chen, X. (2009). The link between juvenile offending and victimization: The influence of risky lifestyles, social bonding, and individual characteristics. *Youth Violence and Juvenile Justice, 7*(2), 119–135.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*, 291–302.

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

Choi, K. (2015). *Cybercriminology and digital investigation*. El Paso: LFB Scholarly Publishing LLC.

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*, 90–118.

Cohen, L.,E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predator victimization: An exposition and test of a formal theory. *American Sociological Review, 46*, 505–524.

Cops, D., & Pleysier, S. (2014). Usual suspects, ideal victims and vice versa: The relationship between youth offending and victimization and the mediating influence of risky lifestyle. *European Journal of Criminology, 11*(3), 361–378.

Cox, T. F., Krzanowski, W. J., Johnson, R. A., Wichern, D. W., Haykin, S., & Bishop, C. M. (2005). *An introduction to multivariate data analysis*. London: Hodder Arnold.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior, 34*, 165–172.

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014). Cyberbullying in social networking sites: An adolescent victim's perspective. *Computers in Human Behavior, 36*, 13–20.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity theory approach. *Theory and Practice in Situational Crime Prevention, Crime Prevention Studies, 16*, 7–39.

Fenaughty, J., & Harre, N. (2013). Factors associated with distressing electronic harassment and cyberbullying. *Computers in Human Behavior, 29*(3), 803–811.

Flick, J. (2009). Prevention is better than prosecution: Deepening the defense against cybercrime. *Journal of Digital Forensics, Security and Law*, 51–71.

Gottfredson, M. R. (1984). *Victims of crime: The dimensions of risk (Home Office Research Study No. 81)*. London: Her Majesty's Stationery Office.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford: Stanford University Press.

Henson, B., Reyns, B. W., & Fisher, B. S. (2011). Security in the 21st century examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review, 36*(3), 253–268.

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 Publishing Company.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*, 189–220.

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context: Toward an integrated theory of offenders, victims, and situations*. Albany, NY: State University of New York Press.

Miller, J. (2013). Individual offending, routine activities, and activity settings: Revisiting the routine activity of general deviance. *Journal of Research in Crime and Delinquency, 50*(3), 310–416.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Nofziger, S., & Kurtz, D. (2005). Violent lives: A lifestyle model linking exposure to violence to juvenile violent offending. *Journal of Research in Crime and Delinquency, 42*(1), 3–26.

Osgood, D. W., Wilson, J. K., O'Malley, P. M., Bachman, J. G., & Johnston, L. D. (1996). Routine activity and individual deviant behavior. *American Sociological Review, 61*(4), 635–655.

Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., et al. (2014). Social media as a vector for youth violence: A review of the literature. *Computers in Human Behavior, 35*, 548–553.

Pauwels, L., & Svensson, R. (2011). Exploring the relationship between offending and victimization: What is the role of risky lifestyles and low self-control? A test in two urban samples. *European Journal on Criminal Policy and Research, 17*, 163–177.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62*, 136–146.

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.

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*, 216–238.

Reyns, B. W., Henson, B., & Fisher, B. S. (2015). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice*, 1–21.

Security DO (2015). Stop.Think.Connect. Retrieved from http://www.dhs.gov/stopthinkconnect.

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428–438.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71–92.

Svensson, R., & Pauwels, L. (2010). Is a risky lifestyle always "risky"? The interaction between individual propensity and lifestyle risk in adolescent offending: A test in two urban samples. *Crime & Delinquency*, 608–626.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. In *21st century criminology: A reference handbook*.

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.

Kyung-Shick Choi is both a Professor of Criminal Justice at Bridgewater State University as well as the Criminal Justice Cybercrime program coordinator at Boston University. His research interests are in cybercrime, cyber-criminology, and cybersecurity. [Email: kchoi@bridgew.edu/kuung@bu.edu]

Jin R. Lee is a PhD candidate at the School of Criminal Justice at Michigan State University. His research interests are in cybercrime, online interpersonal violence, cybersecurity, crime and media, and race and gender inequality within the criminal justice system. [Email: jinr.lee92@gmail.com]