The Impact of Low Self-control on Past and Future Cyber Offending

Brooke Nodeland[1]
University of North Texas, United States of America

Robert Morris[2]
RTex Research, LLC, United States of America

Abstract

The expansion of the internet and personal technology devices has been coupled with the development and increase in cyber offending behaviors. In response, a growing body of literature has sought to extend the application of traditional criminological theories to cyber offending to determine if they explain this new crime type in a similar manner. This paper utilizes an undergraduate student sample (n=428) to examine the effects of self-control on a variety of self-reported cyber offenses as well as anticipated cyber offending behaviors. Findings indicate that while self-control was not significantly predictive of past participation in cyber offending, there is a significant impact of low self-control on anticipated participation in both digital piracy as well as a general measure of cyber offending behaviors.

Keywords: Self-Control Theory, Cyber Offending, Digital Piracy.

Introduction

The internet has become a normal and extensive part of everyday life changing the way the world communicates. The breadth of information sharing now available online makes it easier to both obtain new information while simultaneously providing individuals with deviant proclivities an alternative venue to explore offending possibilities with a greater amount of anonymity than ever before. Scholars have begun paying more attention to cyber deviance in response to these developments. While there is increasing support for the application of traditional criminological theories to cyber deviance (e.g., see Al-Rafee & Cronan, 2006; Ingram & Hinduja, 2008; Morris & Higgins, 2009; Morris & Higgins, 2010; Nodeland & Morris, 2018; Reyns, 2019; Skinner & Fream, 1997), it remains

[1] Assistant Professor & Online MSCJ Program Coordinator, College of Health and Public Service, University of North Texas, Chilton Hall, 410 Avenue C, Suite 289, Denton, Texas 76201, USA. Email: Brooke.Nodeland@unt.edu
[2] Principal, RTex Research, LLC, 1308 Teasley lane, Denton, TX 76205, USA.
Email: robert@rtexresearch.com

unclear if these theories can fully explain cyber deviance in a similar manner as they have been shown to explain traditional deviance.

Self-control theory provides a logical framework for the examination of cyber offending and has received increasing attention in recent years (e.g. Evans, Cullen, Burton, Dunaway, & Benson, 1997; Foster, 2004; Gibson & Wright, 2001; Higgins, 2005, 2007; Higgins & Makin, 2004; Higgins, Wolfe & Marcum, 2007; Malin & Fowers, 2009; Marcum, Higgins, & Ricketts, 2014; Moon, McCluskey, & McCluskey, 2010; Reyns, 2019). As a general theory of crime, self-control may explain involvement in a variety of criminal acts that are naturally extended to cyber offending. Gottfredson and Hirschi's (1991) concept of self-control is described as an individual trait that produces the ability to respond to criminal opportunities either with deviance or the self-control to refrain from such behavior. With regard to cyber offending, low self-control may influence individuals to view cyber offending as a form of risk seeking behavior with instant gratification and immediate gain from commission of the act.

The current study empirically examines the relationship between self-control theory and cyber offending. Specifically, we examine the role of self-control in past and anticipated cyber offending behaviors in relation to digital piracy, hacking behaviors, and cyber harassment to explore differences in the influence of self-control on past behavior and likelihood of engaging in future cyber offenses. Using data collected from a sample of undergraduate students, the current study explores the contributions of self-control in the commission of cyber offending by examining the direct effect of self-control on different types of cyber offending.

Review of Literature: *Self-control theory and cyber offending*

Gottfredson and Hirschi's (1990) self-control theory has been used to explain involvement in a variety of traditional offenses (e.g. Arneklev, Grasmick, Tittle, & Bursik, 1993; Evans et al., 1997; Grasmick, Tittle, Bursik, & Arneklev, 1993; Keane, Maxim, & Teevan, 1993; Piquero, Gibson, & Tibbetts, 2002; Piquero, MacDonald, Dobrin, Daigle, & Cullen, 2005; Piquero & Tibbetts, 1996; Pratt & Cullen, 2000; Sellers, 1999; Unnever & Cornell, 2003), more recently, white-collar and cyber offenses (Donner, Marcum, Jennings, Higgins, & Banfield, 2014; Evans et al., 1997; Gibson & Wright 2001; Higgins & Makin 2004b; Malin & Fowers 2009; Moon et al., 2010) and even cyber victimization (Bossler & Holt, 2010; Hinduja & Patchin, 2008; Holt, Bossler, Malinski, & May, 2016; Ngo & Paternoster, 2011; Reyns, Burek, Henson, & Fisher, 2013; Reyns, Fisher, Bossler, & Holt, 2019).

A General Theory of Crime describes self-control theory and explains involvement in criminal behavior as a by-product of low self-control, or crime-propensity (Gottfredson & Hirschi, 1990). Self-control shapes an individual's response to criminal opportunities with either deviance or refrain from criminal behavior. The general theory explains both conforming and deviant behavior in that the presence of a developed sense of self-control prevents involvement in deviance in a similar manner as an underdeveloped sense of self-control, or low self-control, allows an individual to view criminal behavior as pleasurable. While two individuals may see the same opportunity for crime, the individual with low self-control who views the potential for some pleasurable gain will be the one to engage in deviance whereas the individual with established self-control would refrain from offending. The theory contends that no specific motivation for criminal behavior exists

but that given the opportunity for criminal involvement, individuals will engage in crime if they believe commission of the act will provide pleasure or reward.

The theory identifies several specific characteristics of low self-control, including: impulsivity, insensitivity, risk taking, shortsightedness, minimal tolerance for frustration, a tendency to respond to conflict through physical means, and a preference for simple tasks, however, Grasmick and colleagues (1993) operationalized these characteristics into impulsivity, simple tasks, risk seeking, physical activities, self-centered, and temper. These characteristics influence individual behavior by affecting their ability to control impulses, manage risk tasking, exact predictability on an individual's life, perform complex thought processes, and exercise control over individual emotions. The authors suggest that individuals are inherently motivated to engage in crime because they naturally view crime as pleasurable or in their own self-interest (Grasmick et al., 1993). Rather, crime satisfies individual desires for immediate or short-term gratification with the reward for criminal behavior following shortly after the commission of an act. The potential for pleasure is even more appealing in that crime is relatively easy to carry out making the quick reward an even more plausible outcome. For cyber offenders, this may occur through the quick acquisition of digital media that can be consumed for personal use or distributed for profit.

The extension of self-control theory to non-traditional crime types was discussed by Gottfredson and Hirschi (1990) early in their application of the theory to the explanation of white-collar crime:

> There is no reason to think that the offenders committing these crimes are causally distinct from other offenders. The assumption that white-collar criminals differ from other criminals is simply the assumption, in another guise, that offenders specialized in their particular crimes, an assumption for which there is no good evidence. The central elements of our theory of criminality are easily identifiable among white collar criminals (Gottfredson & Hirschi, 1990, pp. 190–191).

This discussion extends the applicability of self-control theory to explain non-traditional types of crime by arguing that individuals who engage in criminal behavior share common characteristics. For example, individuals who engage in cyber offending, including digital piracy and computer hacking, will possess characteristics of low self-control. Digital pirates, in particular, demonstrate the characteristics of low self-control in their inability to delay the gratification of waiting for the official release of digital software, music or movies or obtain digital media to distribute for monetary gain (Malin & Fowers, 2009; Moon et al., 2010). Self-control is also demonstrated in an individual's ability to suppress criminal motivations and resist temptation when an opportunity presents itself and ability to distribute media for monetary gain prior to public release may result in the impulsive response to pirate the media in individuals with low self-control. Cyber offenders in general may also have a lack of regard for the potential consequences of their actions because they do not believe they will be caught but stand to gain the immediate access to the media of interest. The act itself can produce excitement in individuals with low self-control, both at the thought of obtaining the media and by the method through which it is obtained.

The relationship between self-control and cyber offending has received increasing empirical attention in recent years (e.g. Boillot Fansher, 2017; Bossler & Holt, 2010; Higgins, 2004, 2005, 2007; Higgins, Marcum, & Wolf, 2007; Holt, Bossler, & May, 2012; Marcum et al., 2014; Malin & Fowers, 2009; Moon, McCluskey, & McCluskey,

2010; Pratt, Turanovic, Fox, & Wright, 2014; Reyns, Henson, & Fisher, 2014; Vazsonyi, Machackova, Sevcikova, Smahel, & Cerna, 2012). While a significant relationship between low self-control and digital piracy has been found consistently in the prior literature, the influence of low self-control on other forms of cyber offending remains underexplored. One prior study examined the influence of self-control on a variety of cyber offenses including posting hurtful information about someone on the internet, threatening/insulting others through email or instant messaging, excluding someone from online community, hacking into an unauthorized area of the internet, distributing malicious software, illegally downloading copyrighted files/programs, illegally uploading copyrighted files/programs, using someone else's personal information on the internet without his or her permission, using the internet to facilitate a drug transaction, and posting nude photos of someone else without his/her permission (Donner, Marcum, Jennings, Higgins, & Banfield, 2014). They utilized negative binomial regression to examine scaled measures of cyber offending among a sample of 488 undergraduate students. Their findings indicate that low self-control is a significant predictor of cyber deviance in general as well as variety of individual types of cyber offenses beyond digital piracy (Donner et al., 2014).

Self-control theory has received a considerable amount of continuous empirical attention that demonstrates its significance as a predictor of participation in deviant behavior and cyber offending, in particular digital piracy. However, less attention has been given to its application to other types of cyber offending or the differential influence of self-control of past and anticipated reports of these behaviors. This study extends the self-control literature by examining its influence on a variety of cyber offenses to determine the impact of self-control on both participation and willingness to participate in a variety of cyber offenses. Specifically, the intended outcome is to determine the role of an established individual characteristic, self-control, on deviant cyber behavior. We hypothesize that there is a direct relationship between measures of self-control on cyber offending. Rather, low self-control will have a direct relationship with involvement in computer crime, or those with low self-control will be more likely to report participation computer related deviance as well as willingness to participate in this behavior in the future.

Sampling and Methods

Data for the current study were obtained via an original data collection effort utilizing self-administered questionnaires to collect data from undergraduate students in the spring 2010 semester at a midsize southern university. It should be noted that the technological landscape at the time of this article's submission differs from that in 2010 when the data were collected. However, there is precedent for the use of previously collected cyber data (Reyns, 2019), and while it may be a limitation to the study, it should not ultimately detract from this study's findings.

Prior studies have identified college students as individuals more likely to engage in several types of cyber offending, including digital piracy and computer hacking, in comparison to individuals not in college or in the working world (Higgins & Wilson, 2006; Hollinger, 1993). We contacted instructors in a variety of majors to reach a diverse sample of students to reflect the diversity in the student population at the university. Specifically, email correspondence was sent to instructors of required high enrollment undergraduate courses a variety of majors, such as political science, computer science,

macroeconomics, as well as several criminology professors. The email asked the instructor for 10-12 minutes of their class time to administer the survey at the beginning of one of their classes. Instructors in 11 of the 17 requested undergraduate courses agreed to allow the administration of surveys to their students totaling 857 enrolled students. Students were advised that their participation was voluntary and their responses would be held confidential in an attempt to garner honest participation from as many respondents as possible. No identifying information was collected from respondents. Students were also asked to refrain from completing the survey if they had already taken it in another class to avoid duplicate responses.

Table 1. Descriptive Statistics

	Mean	SD	Minimum	Maximum
Cyber offending	1.39	0.60	1.10	5.50
Behavior in past 12 months:				
Total cyber offenses	0.75	0.43	0	1
Guessed password on social network	0.24	0.43	0	1
Retaliated against someone using a social network	0.13	0.34	0	1
Accessed someone else's files without permission	0.13	0.34	0	1
Digital piracy	0.68	0.47	0	1
Anticipated behavior in next 12 months:				
Total cyber offenses	0.62	0.49	0	1
Digital piracy	0.59	0.49	0	1
Age	21.78	4.77	17	38
White	54%			
Male	57%			
Knowledge				
Uncomfortable using computers.	2%			
Can surf the 'net, use common software, but not fix my computer problems.	21%			
Can use a variety of software and fix some of my computer problems.	44%			
Can use a variety of operating systems and fix most computer problems I have.	17%			
Comfortable manipulating or writing computer programming.	15%			

The final sample totaled 428 cases after deletion of cases with missing data. Respondents were comprised of 51.5% non-technical majors (i.e., liberal arts, social science, business, fine arts, etc.) with the remainder reporting a technical major (e.g., engineering, math, hard sciences, etc.). The sample contained 43% female and 57% male respondents. The average age of the sample was 22. The sample consisted of 54% White respondents, 5% African American respondents, 14% Hispanic respondents, 21% Asian respondents and 6% other. Finally, roughly 99% of respondents reported at least some level of comfort using a computer. (For complete descriptive overview see Table 1)

1. Measures

Anticipated cyber offending. The first outcome measure is based on the respondents anticipated involvement in cyber offending over the next 12 months. Respondents were asked to self-report the likelihood of their anticipation in malicious cyber offenses, including guessing someone else's password on a social networking site, a school website, a banking website, or an internet email account, using a social networking site (such as Myspace, Facebook, or Twitter) to retaliate against someone they felt did them some wrong, accessing computer files without authorization, adding, deleting, changing or printing another person's computer file information without them knowing it, or downloading full-version commercial software, videos, or music instead of buying them (e.g., via a torrent or file sharing network) over the next 12 months. Responses were based on a 1-5 scale where 1=not at all likely and 5= very likely. Factor analysis was conducted to create the first outcome variable measuring participation in cyber offending (α=.79).

Actual cyber offending variables. A series of dichotomous cyber offending variables were created to examine the influence of self-control on past cyber offending behavior.

Participation in cyber offending during the past 12 months. A dichotomous measure of involvement in any type of cyber offending was created by examining the responses to eight questions (e.g., password guessing on a social network, school website, banking website, internet email account; using a social network to retaliate against someone; accessing computer files without permission; altering someone else's computer information; illegally downloading commercial software, videos or music). Participation in any type of cyber offense during the past 12 months was summed and converted into a binary indicator where 0 = no participation in cyber offending over the past 12 months and 1 = participation in cyber offending during the past 12 months. The final variable consisted of 25% of respondents reporting no participation in cyber offending and 75% of respondents reporting participation in at least one form of cyber offending during the past 12 months.

Password guessing on social networks in past 12 months. A dichotomous measure of guessing someone else's password on a social networking site within the past 12 months was coded as 0 = no participation in guessing someone else's password on a social networking site over the past 12 months and 1 = participation in guessing someone else's password on a social networking site over the past 12 months. The final variable consisted of 24% of respondents reporting engaging in this behavior and 76% reporting no participation in this behavior.

Using a social network to retaliate against someone in the past 12 months. A dichotomous measure of using a social network to retaliate against someone in the past 12 months was coded as 0 = no participation in using a social network to retaliate against

someone during the past 12 months and 1 = participation in using a social network to retaliate against someone during the past 12 months. The final variable consisted of 13% of respondents reporting engaging in this behavior and 87% reporting no participation in this behavior.

Accessing computer files without authorization in past 12 months. A dichotomous measure of accessing computer files without authorization within the past 12 months was coded as 0 = no participation in accessing computer files without authorization within the past 12 months and 1 = participation in accessing computer files without authorization within the past 12 months. The final variable consisted of 14% of respondents reporting engaging in this behavior and 86% reporting no participation in this behavior.

Downloading commercial software, videos, or music within the past 12 months. A dichotomous measure of downloading commercial software, videos, or music within the past 12 months was coded as 0 = no participation in downloading commercial software, videos, or music within the past 12 months and 1 = participation in downloading commercial software, videos, or music within the past 12 months. The final variable consisted of 68% of respondents reporting engaging in this behavior and 32% reporting no participation in this behavior.

Anticipated involvement in cyber offending. A dichotomous measure encompassing anticipated involvement in any type of cyber offending was also developed. Respondents reporting at least some likelihood of involvement in the cyber offending behaviors listed above were coded as 1 = anticipated participation in cyber offending in the next 12 months and 0 = no anticipated participation in cyber offending in the next 12 months. The final variable consisted of 62% of respondents reporting anticipated participation in engaging in this behavior and 38% reporting no anticipation of engaging in this participation in this behavior.

Anticipated involvement in downloading commercial software, videos, or music without permission. A dichotomous measure encompassing anticipated involvement in downloading commercial software, videos, or music without permission was developed. Respondents reporting at least some likelihood of involvement in downloading commercial software, videos, or music without permission were coded as 1 = anticipated participation in accessing computer files without permission and 0 = no anticipated participation in downloading commercial software, videos or music without permission. The final variable consisted of 59% of respondents reporting anticipated participation in engaging in this behavior and 41% reporting no anticipation of engaging in this participation in this behavior.

Self-control. The self-control measure used in the current analysis is derived from Tangey and Baumeister's (2001) scale, is similar to that used in several previous studies of university studies and is designed to reflect the respondents established level of self-control (Higgins, Tewksbury, & Mustaine, 2007; Morris & Higgins, 2009). As such, respondents were asked a series of 13 questions measuring their established level of self-control. Specifically, the self-control scale measured higher levels of self-control and were reported on a 1-5 scale where 1=disagree strongly and 5=strongly agree: I am good at resisting temptation, I refuse things that are bad for me, people would say that I have iron self-discipline, and I am able to work effectively toward long-term goals. Additional self-control indicators were included in the scale were reported on a 1-5 scale where 1=disagree strongly and 5=strongly agree but were reverse coded prior to inclusion in the self-control for analysis: I have a hard time breaking bad habits, I am lazy, I say

inappropriate things, I do certain things that are bad for me if they are fun, I wish I had more self-discipline, pleasure and fun sometimes keep me from getting work done, I have trouble concentrating, sometimes I can't stop myself from doing something even if I know it is wrong, and I often act without thinking through all the alternatives. The result was a standardized single factor measuring the concept of self-control where higher values indicated higher levels of self-control (α=.81).

Control variables. Several control variables were selected based on their significance in previous studies of cyber offending. These included several demographic variables, including gender (Hinduja & Ingram, 2008; Hollinger, 1993; Miller & Morris, 2016; Morris & Higgins, 2009; Morris & Higgins, 2010; Skinner & Fream, 1997; Simpson, Banerjee, & Simpson, 1994; Sim, Cheng, & Teegen, 1996; Seale, Polakowski, & Schneider, 1998; Solomon & O'Brien, 1990), race (Hollinger, 1993; Husted, 2000), age (Hollinger, 1993; Seale et al., 1998; Sims et al., 1996; Solomon & O'Brien, 1990) and computer skill (Eining & Christensen, 1991; Malin & Fowers, 2009; Sims et al., 1996). Specifically, prior studies have found that males, younger individuals, and those with more computer knowledge are more likely to engage in cyber offenses compared to their counterparts.

The current analysis utilizes dichotomous measures for gender and race where 0=female, 1=male and 0=non-White, 1=White. Respondent age is a continuous variable based on the respondent's age (in years) at the time of data collection. Finally, respondent's computer skill level was by respondents' self-report of their skill level: 1 = I am uncomfortable using computers, 2 = I can "surf the 'net", use common software, but not fix my computer problems, 3 = I can use a variety of software and fix some of my computer problems, 4 = I can use a variety of operating systems and fix most computer problems I have, or 5 = I am comfortable manipulating or writing computer programming.

2. Analysis

As previously discussed, this study seeks to extend the application of self-control theory to participation in and anticipated participation in a variety of cyber offenses. Specifically, the following research question is explored: What is the direct effect of self-control on cyber offending? To answer this research question, we first establish a base model the relationship between self-control and cyber offending. The relationship will be further examined through the use of both Ordinary Least Squares (OLS) regression models as well as a series of Logistic regression models. The use of OLS or Logistic regression will depend on the outcome of interest (e.g., continuous vs. dichotomous measure of cyber offending). First, an OLS regression model will be used with the continuous measure of participation in cyber offending to assess the relationship between self-control and cyber offending. Appropriate measures of model fit and multivariate assumptions will be assessed.

Next, self-control will be incorporated into a series of logistic regression models using dichotomous cyber offending outcomes described above to determine if there are differences in theoretical predictors for a variety of cyber offending types. These additional analyses will examine the odds of engaging in cyber offending and an assessment of the overall differences between offenders and non-offenders in their odds of participation in each type of cyber offending.

Results

Table 2 establishes the baseline relationship between self-control and a composite measure of cyber offending using OLS regression. Column 1 establishes a base model for examining cyber offending while column 2 explores the relationship between self-control and cyber offending. The first column presents the results from the baseline model for the control variables. This base model indicates that, absent of any theoretical predictors, there is a positive relationship between computer knowledge and cyber offending. Additionally, there is a significant relationship between race and cyber offending; specifically, non-whites appear to be more likely to engage in cyber offending than whites. The second column displays the results of the initial model for the relationship between self-control and cyber offending. This model is similar to the base model in which higher levels of computer knowledge and race may influence involvement in cyber offending. While the coefficient for self-control was in the expected direction, with higher levels of self-control suggesting less offending (Foster, 2004; Higgins, Wolf & Marcum, 2007; Malin & Fowers, 2009; Moon et al., 2010), its effect on cyber offending was not statistically significant in this model.

Table 2. OLS base models for anticipated involvement in cyber offending

	Base model	Self-control model
	b *(se)*	*b* *(se)*
Self-control	-	-0.0081 (0.0322)
Knowledge	.1116 (.0308)★★★	.1108 (.0309)★★★
Male	0.0906 (.0627)	0.0885 (0.0633)
Age	-.0084 (.0059)	-0.0081 (.0060)
White	-.1913 (.0578)★★★	-.1907 (.0579)★★★
R^2	0.07	0.07
N	428	428

★ p<0.05, ★★ p<0.01, ★★★ p<0.001

The table 3 breaks down the relationship between individual cyber offenses and self-control to examine differences in theoretical influences on a variety of cyber offending behaviors. Specifically, table 3 displays the results from a series of logistic regression models examining the relationship between self-control and a variety of cyber offenses occurring

within the past 12 months as well as anticipated participation in any cyber offense and digital piracy. Column 1 displays the results of the logistic regression model examining the relationship between self-control and participation in any cyber offense during the past 12 months. Age was the only significant predictor in this relationship indicating that, contrary to expectations, the odds of participation in cyber offending increase with age. Columns 2-5 display the results of the logistic models examining the relationship between self-control and password guessing on a social network, retaliating against someone using a social network, accessing someone else's files without permission, and digital piracy. There were no significant predictors in any of these models. Columns 6 and 7 display the results of the relationship between self-control on anticipated participation in all cyber offending and digital piracy. Both of the overall models were significant and contained the same significant predictors for participation in cyber offending. Fit statistics indicate that 66% of cases were correctly classified for each of these models, and pseudo R^2 measures suggest reasonable fit .16 (Nagelkerke R^2) and .18 (Nagelkerke R^2) respectively. In both of these models, for individuals reporting lower levels of self-control, higher levels of computer knowledge and younger people, the odds of participating in cyber offending increased as expected, net of other effects.

Table 3. Logistic Regression Results: Self-control and Cyber Offending Types (Odds ratios, n=428)

	Behavior past 12 months					*Anticipated behavior next 12 months*	
	Any cyber offense	Guessed password on social network	Retaliated against someone using a social network	Accessed someone else's files without permission	Digital piracy	Any cyber offense	Digital piracy
Self-control	1.123 (.1310)	1.0655 (.1260)	1.2694 (.1953)	.8379 (.1211)	1.1698 (.1275)	.7426 (.0824)**	.7311 (.0807)**
Computer knowledge	1.2321 (.1525)	1.1108 (.1388)	1.2165 (.1966)	.9042 (.1362)	1.1834 (.1359)	1.4219 (.1687)**	1.4959 (.1769)**
Male	.9704 (.2427)	.7595 (.1934)	1.0653 (.3574)	1.1854 (.3683)	1.0362 (.2421)	1.2279 (.2901)	1.2417 (.2917)
Age	1.0696 (.0363)*	1.0028 (.0237)	.9652 (.0379)	.9942 (.0321)	1.0572 (.0316)	.8656 (.0269)***	.8608 (.0275)***
White	1.1761 (.2685)	1.265 (.2973)	.6131 (.1850)	.9647 (.2723)	1.0317 (.2761)	.7862 (.1702)	.8151 (.1751)
AUC	0.5939	0.5452	0.6041	0.5673	0.5860	0.7058	0.7093
Nagelkerke R^2	0.03	0.01	0.03	0.01	0.03	0.16***	0.18***

* p<0.05, ** p<0.01, *** p<0.001

Discussion and Conclusion

The goal of this study was to examine the relationship between self-control on a variety of prior as well as anticipated cyber offenses. The application of traditional criminological theories to cyber offending has received considerable attention in recent years as researchers explore whether, and to what extent, traditional criminological theories can

explain participation in cyber offending in a similar manner as for traditional crime types. Previous literature has established a link between self-control and cyber offending through an exploration of specific behaviors including digital piracy and computer hacking (e.g. Evans, Cullen, Burton, Dunaway, and Benson, 1997; Foster, 2004; Gibson & Wright, 2001; Higgins, 2005, 2007; Higgins & Makin, 2004; Higgins, Wolfe & Marcum, 2007; Holt & Bossler, 2014; Malin & Fowers, 2009; Marcum, Higgins, & Ricketts, 2014; Moon, McCluskey, & McCluskey, 2010; Reyns, 2019). While much of the previous literature has focused on the relationship between low self-control and digital piracy, there is one prior study that examined the effects of self-control on a variety of types of cyber offending (Donner et al., 2014). Specifically, their findings indicate that self-control is significantly predictive of combined measures of cybercrime using both a 5 and 7 item cybercrime scale. This paper extends the self-control cyber offending research base by specifically examining both self-reported participation in a variety of cyber offenses including password guessing, cyber retaliation, accessing someone else's files, and digital piracy as well as anticipated participation in general cyber offending and digital piracy.

Our findings indicate that the effect of self-control on a combined measure of cyber offending was non-significant in the OLS model, however, findings from the logistic regression models examining the influence of self-control on anticipated involvement in cyber offending were in line with previous research suggesting low self-control is predictive of these behaviors (Donner et al., 2014; Foster, 2004; Malin & Fowers, 2009; Moon et al., 2010). This finding indicates a willingness among respondents to participate in digital piracy and other cyber offenses. However, regression findings in all other models were contrary to expectations in that self-control did not appear to have a significant relationship with cyber offending that had already occurred. This may indicate that respondents are more willing to express likelihood in participation of cyber offending as opposed to self-report on actual behavior.

While not the focus of the study higher skill level with computers (Eining & Christensen, 1991; Hinduja, 2001; Malin & Fowers, 2009; Sims et al., 1996) and being young (Hollinger, 1993; Seale et al., 1998; Sims et al., 1996; Solomon & O'Brien, 1990) were significantly predictive of anticipated participation in cyber offending which is in line with the prior literature. This finding suggests that it may be easier for individuals with higher levels of computer skill to engage in cyber offending behavior. For example, they may see the short-term monetary gain of pirating software or other media and believe they have the technical skills to carry out the act with limited risk of getting caught.

There are several limitations and considerations for future research that warrant discussion. First, the findings may not be generalizable to a larger or more diverse population as the data were collected from a small sample of university students. While college students have been determined to be an appropriate sample for studies of cyber offending (Bossler & Burruss, 2010; Burruss et al., 2013; Foster, 2004; Higgins, 2006; Higgins, Fell, & Wilson, 2006; Higgins & Makin, 2004a, 2004b; Higgins & Wilson, 2006; Higgins et al., 2007; Hinduja & Ingram, 2008, 2009; Morris & Higgins, 2009, 2010; Skinner & Fream, 1997; Smallridge, 2012; Wolfe & Higgins, 2009), they may differ in their cyber offending participation when compared to the general public. For example, college students may differ in their computer usage and online activities from other similarly aged individuals. Different age groups, such as middle-/high-school age students or older individuals may also differ in their need and use of computers. Additionally, as use of personal computers, tablets, and mobile devices with internet capabilities has increased,

younger individuals have greater access to the internet and likely engage in different behavioral patterns online than college students (Holt, Bossler, & May, 2012; Marcum, Higgins, & Ricketts, 2014).

Changes in internet and computer use have also occurred since this data were collected. Studies utilizing more recent data and more contemporary cyber behaviors would further extend the exploration of self-control into the realm of a more complete picture of cyber offending. Computer and internet use has seen a dramatic shift to personal technology devices which could may impact behavior and anticipated behavior in different ways. Similarly, this shift may alter how current technology users respond to similar questions related to self-control and online behavior. Self-control, while stable, may present itself differently given the context of present-day computer usage.

Finally, a growing body of cyber offending research has taken a multi-theoretical approach to the examination of the relationship between self-control and cyber offending, including the influence of social learning theory (Higgins & Makin, 2004; Higgins, 2006; Higgins & Wilson, 2006; Higgins, Fell, & Wilson, 2006; Higgins, Fell, & Wilson, 2007; Hinduja & Ingram, 2008; Higgins, Scott, & Ricketts, 2009; Morris & Higgins, 2009; Nodeland & Morris, 2018; Wolfe & Higgins, 2009). The consideration of other established theoretical predictors, may provide a more detailed picture of the influence of self-control on contemporary offense types. For example, self-control may interact with the learning process, or rather, that individuals with low self-control and associate with deviant peers may be even more likely to engage in cyber offending than those with only low self-control. A multi-theoretical examination of cyber offending should be considered in the examination of a variety of cyber offenses (Higgins & Makin, 2004a; Higgins, Fell, & Wilson, 2006; Nodeland & Morris, 2018)

In conclusion, this paper sought to further distinguish the relationship between self-control and a variety of cyber offending behaviors through the examination of actual and anticipated cyber offending behaviors. Self-control was found to be a significant predictor of anticipated participation in digital piracy and general cyber offending, however, was not predictive of cyber offending behaviors that had already taken place. Taken together, these findings indicate the need for continued study to further define the relationship between self-control and cyber offending. Cyber offenses are ever changing and constantly evolving. A developed understanding of what leads to participation in these types of offenses is necessary to develop prevention and reduction strategies based on theoretical predictors.

References

Al-Rafee, S., & Cronan, T. P. (2006). Digital piracy: Factors that influence attitude toward behavior. *Journal of Business Ethics*, *63*(3), 237-259.

Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers?. In *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1499-1527). IGI Global.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*, 227-236.

Burruss, G. W., Bossler, A. M., & Holt, T. J. (2013). Assessing the Mediation of a Fuller Social Learning Model on Low Self-Control's Influence on Software Piracy. *Crime & Delinquency, 59*, 1157-1184.

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.

Eining, M. M., & Christensen, A. L. (1991). A Psycho-Social Model of Software Piracy: The Development and Test of a Model. In R. M. Dejoie, G. C. Fowler, and D. B. Paradice (Eds.), *Ethical Issues in Information Systems* (pp. 182-188). Boston, MA: Boyd and Fraser.

Evans, T. D., Cullen, F. T., Burton, Jr., V. S., Dunaway, R. G., & Benson, M. L. (1997). The Social Consequences of Self-control: Testing the General Theory of Crime. *Criminology, 35*, 475-501.

Foster, D. R. (2004). Can the general theory of crime account for computer offenders: Testing low self-control as a predictor of computer crime offending. Unpublished master thesis, University of Maryland, College Park.

Gibson, C., & Wright, J. (2001). Low Self-Control and Coworker Delinquency: A Research Note. *Journal of Criminal Justice, 29*, 483-492.

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

Grasmick, H. G., Tittle, C. R., Bursik, Jr., R. J. & Arneklev, B. J. (1993). Testing the Core Empirical Implications of Gottfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency, 30*, 5-29.

Higgins, G. E., & Makin, D. A. (2004a). Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy? *Journal of Economic Crime Management, 2*(2), 1-22.

Higgins, G. E., & Makin, D. A. (2004b). Self-control, Deviant Peers, and Software Piracy. *Psychological Reports, 95*(3), 921-931.

Higgins, G. E., Tewksbury, R., & Mustaine, E. E. (2007). Sports fan binge drinking: An examination using low self-control and peer association. *Sociological Spectrum*, *27*(4), 389-404.

Higgins, G. E., & Wilson, A. L. (2006). Low Self-Control, Moral Beliefs, and Social Learning Theory in University Students' Intentions to Pirate Software. *Security Journal, 19*(2), 75-92.

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Digital piracy: An examination of three measurements of self-control. *Deviant Behavior*, *29*(5), 440-460.

Hinduja, S. (2001). Correlates of Internet software piracy. *Journal of Contemporary Criminal Justice*, *17*(4), 369-382.

Hinduja, S., & Ingram, J. (2008). Self-Control and Ethical Beliefs on the Social Learning of Intellectual Property Theft. *Western Criminological Review, 9*(2), 52-72.

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

Hollinger, R. C. (1993). Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access. *Security Journal, 4*, 2-12.

Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice*, *32*(2), 108-128.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice, 37*, 378-395.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

Ingram, J. R. & Hinduja, S. (2008) Neutralizing music piracy: An empirical examination. *Deviant Behavior, 29*(4), 334-366.

Keane, C., Maxim, P. S., & Teevan, J. J. (1993). Drinking and driving, self-control, and gender: Testing a general theory of crime. *Journal of Research in Crime & Delinquency*, *30*, 30–46.

Malin, J., & Fowers, B. J. (2009). Adolescent self-control and music and movie piracy. *Computers in Human Behavior, 25*, 718-722.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration. *International Journal of Cyber Criminology, 8*(1), 47-56.

Miller, B., & Morris, R. G. (2016). Virtual peer effects in social learning theory. *Crime & Delinquency*, *62*(12), 1543-1569.

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, *38*(4), 767-772.

Morris, R. G., & Higgins, G. E. (2009). Neutralizing Potential and Self-Reported Digital Piracy: A Multitheoretical Exploration Among College Undergraduates. *Criminal Justice Review, 34*(2), 173-195.

Morris, R. G., & Higgins, G. E. (2010). Criminological Theory in the Digital Age: The Case of Social Learning Theory and Digital Piracy. *Journal of Criminal Justice, 38*(4), 470-480.

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

Nodeland, B., & Morris, R. (2018). A Test of Social Learning Theory and Self-Control on Cyber Offending. *Deviant Behavior*, 1-16.

Piquero, A. R., Gibson, C. L., & Tibbetts, S. G. (2002). Does Self-Control Account for the Relationship Between Binge Drinking and Alcohol-related Behaviours? *Criminal Behavior and Mental Health, 12*, 135-154.

Piquero, A. R., MacDonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime. *Journal of Quantitative Criminology, 21*(1), 55-71.

Piquero, A., & Tibbetts, S. (1996). Specifying the Direct and Indirect Effects of Low Self-Control and Situational Factors in Offenders' Decision Making: Toward a More Complete Model of Rational Offending. *Justice Quarterly, 13*, 481-510.

Piquero, N. L. (2005). Causes and Prevention of Intellectual Property Crime. *Trends in Organized Crime, 8*(6), 40-61.

Pratt, T., & Cullen, F. (2000) The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis. *Criminology, 38*(3), 931-964.

Reyns, B. W. (2019). Online pursuit in the twilight zone: cyberstalking perpetration by college students. *Victims & Offenders*, *14*(2), 183-198.

Reyns, B. W., Burek, M. W., Henson, B., & Fisher, B. S. (2013). The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice*, *36*(1), 1-17.

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization?. *American Journal of Criminal Justice*, *44*(1), 63-82.

Seale, D. A., Polakowski, M., & Schneider, S. (1998). It's Not Really Theft!: Personal and Work-place Ethics that enable Software Piracy. *Behaviour and Information Technology*, *17*, 27-40.

Sellers, C.S. (1999). Self-Control and Intimate Violence: An Examination of the Scope and Specification of the General Theory of Crime. *Criminology, 37*(2), 375-404.

Simpson, E. M., Banerjee, D., & Simpson, Jr., C. L. (1994). Softlifting: A Model of Motivating Factors, *Journal of Business Ethics*, *13*, 431-438.

Sims, R. R., Cheng, H. K., & Teegen, H. (1996). Toward a Profile of Student Software Pirates, *Journal of Business Ethics*, *15*, 839-849.

Skinner, W. F., & Fream, A. M. (1997). A Social Learning Theory Analysis of Computer Crime Among College Student. *Journal of Research in Crime and Delinquency*, *34*(4), 495-518.

Solomon, S. L., & O'Brien, J. A. (1990). The Effect of Demographic Factors on Attitudes toward Software Piracy, *Journal of Information Systems*, *30*, 40-46.

Tangney, J. P., & Baumeister, R. F. (2001). High Self-Control Predicts Good Adjustment, Less Pathology, Better Grades, and Interpersonal Success. Unpublished manuscript, Department of Psychology, George Mason University.

Thong, J. Y. L., & Yap, C. (1998). Testing an Ethical Decision-Making Theory: The Case of Softlifting. *Journal of Management Information Systems, 15*, 213-237.

Wolfe, S. E., & Higgins, G. E. (2009). Explaining deviant peer associations: An examination of low self-control, ethical predispositions, definitions, and digital piracy. *W. Criminology Rev.*, *10*, 43.