Am J Crim Just
DOI 10.1007/s12103-011-9117-3

Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance

Thomas J. Holt · Adam M. Bossler · David C. May

Received: 29 July 2010 / Accepted: 1 December 2010

Abstract Gottfredson and Hirschi's (1990) general theory of crime and Akers' (1998) social learning theory have received strong empirical support for explaining crime in both the physical and cyberworlds. Most of the studies examining cybercrime, however, have only used college samples. In addition, the evidence on the interaction between low self-control and deviant peer associations is mixed. Therefore, this study examined whether low self-control and deviant peer associations explained various forms of cyberdeviance in a youth sample. We also tested whether associating with deviant peers mediated the effect of low self-control on cyberdeviance as well as whether it conditioned the effect. Low self-control and deviant peer associations were found to be related to cyberdeviance in general, as well as piracy, harassment, online pornography, and hacking specifically. Deviant peer associations both mediated and exacerbated the effect of low self-control on general cyberdeviance, though these interactions were not found for the five cyberdeviant types examined.

Keywords Cybercrime · Low self-control · Social learning · Peer offending · Juvenile delinquency

T. J. Holt (✉)
School of Criminal Justice, Michigan State University, 434 Baker Hall, East Lansing, MI 48824, USA
e-mail: holtt@msu.edu

A. M. Bossler
Justice Studies Program, Department of Political Science, Georgia Southern University, P.O. Box 8101, Statesboro, GA 30460, USA
e-mail: abossler@georgiasouthern.edu

D. C. May
Correctional & Juvenile Justice Services, Eastern Kentucky University, 521 Lancaster Avenue, Stratton 110, Richmond, KY 40475, USA
e-mail: David.may@eku.edu

Published online: 18 June 2011

Over the last two decades, an increasing body of research has examined the problem of cybercrime. Cybercrime refers to offenses where special knowledge of cyberspace is used to violate the law (Furnell, 2002; Wall, 2001). A wide range of behaviors can be facilitated or enhanced by electronic communications and the Internet, such as harassment (Bocij, 2004; Finn, 2004; Holt & Bossler, 2009), pornography (Buzzell, Foss, & Middleton, 2006), media piracy (e.g., Higgins, 2005), and theft (Jordan & Taylor, 1998). Criminologists have used two primary theories to examine cybercrime: Gottfredson and Hirschi's (1990) general theory of crime and Akers' (1998) social learning theory. Gottfredson and Hirschi (1990) argue that those with low self-control tend to be impulsive, insensitive, short sighted, risk takers who are unable to resist the opportunity to offend (Gottfredson & Hirschi, 1990). Akers' (1998) social learning theory, however, suggests that crime is a learned behavior stemming from peer associations that provide sources of deviant imitation, definitions and justifications, and reinforcement for offending.

These theories offer strikingly different explanations for why individuals commit crime, though both have received significant empirical support with both street crimes (e.g., Akers & Jensen, 2006; Gottfredson, 2006; Pratt & Cullen, 2000; Pratt et al., 2009; Tittle, Ward, & Grasmick, 2003) and cybercrime (e.g., Higgins, 2005, 2006; Holt, Burrus, & Bossler, 2010; Morris & Higgins, 2010; Skinner & Fream, 1997). Scholars have also examined how low self-control and deviant peer associations interact with each other to explain both traditional offenses and cybercrime (e.g., Gibson & Wright, 2001; Higgins, Fell, & Wilson, 2006). Though these studies provide significant insight into how low self-control and social learning influence the commission of cybercrime, few have considered how these relationships may operate with non-university populations, particularly juvenile populations who are thought to engage in a variety of cybercrimes (Taylor, Fritsch, Liederbach, & Holt, 2010; Yar, 2005). As young people continuously gain access to computer technology at earlier ages (Wolack, Mitchell, & Finkelhor, 2006), it is critical that researchers consider the phenomena of cybercrime offending in juvenile populations to better understand its causes and correlates.

This study addresses these issues by examining the effects of low self-control and deviant peer associations on multiple forms of cybercrime offending in a population of middle and high school students. In addition, we examine how associating with deviant peers interacts with low self-control, specifically exploring mediating and moderating effects. The findings benefit the literature on low self-control and social learning and their ability to explain novel forms of offending in juvenile populations as well as the scant literature on how low self-control and deviant peer associations interact.

Understanding Cybercrime

The problem of cybercrime is diverse, encompassing a range of behaviors with economic and emotional consequences (Taylor et al., 2010). One of the most recognized typologies of cybercrime, developed by Wall (2001), suggests that there are four forms of offending in virtual environments: deception/theft, pornography, violence, and cyber-trespass. The most common type of cyber-theft committed by

young adults and youth is digital piracy, where illegal copies of digital media are created without the explicit permission of the copyright holder (Gopal, Sanders, Bhattacharjee, Agrawal, & Wagner, 2004). Piracy is particularly challenging for law enforcement because illegally copied media can be downloaded through websites and file sharing services distributed across the Internet (Gopal et al., 2004; Hinduja, 2001). The costs of piracy are thought to be quite high, as the U. S. music industry reports losses of over $12 billion each year due to theft (Taylor et al., 2010).

The second form of cybercrime with particular significance for juvenile populations is cyber-pornography, as individuals under the age of 18 can easily view and obtain sexually explicit through the World Wide Web (DiMarco, 2003; Edleman, 2009; Lane, 2000). In fact, the adoption and popularity of various forms of media, including DVDs, webcams, digital photography, and streaming web content, are directly tied to the pornography industry (Lane, 2000). This may account for the fact that one in three children were exposed to unwanted images of nude individuals or people having sex while online in 2005 (Wolack et al., 2006).

There is a growing body of research focusing on online harassment, a form of cyber-violence, which is common among juvenile populations. This offense can lead victims to feel fear or distress in much the same manner as real-world stalking and harassment (Bocij, 2004; Finn, 2004; Wall, 2001). Harassment can take a variety of forms, including threatening or sexual messages delivered via e-mail, instant messaging services, or posts in chat rooms. In addition, the popularity of social networking sites like Myspace among youths allows them to post mean or cruel messages about other people for the public to see (Hinduja & Patchin, 2008, 2009). Although some victims may view harassing communications to be nothing more than a nuisance, some victims report physical or emotional stress (Finn, 2004).

The final type of cybercrime noted by Wall (2001) is cyber-trespass, where individuals utilize computers and technology to access computer systems they do not own or legally have permission to use (Holt, 2007; Yar, 2005). This most often involves computer hacking which is often attributed to juveniles who spend their time exploring computer networks without authorization from the system owners (Furnell, 2002; Yar, 2005). While media reports of hacking suggest these offenses are often complex and involve significant financial losses (Furnell, 2002), simple forms of hacking involve guessing passwords and accessing accounts without permission from the system owners (Bossler & Burruss, 2010; Holt, 2007).

Low Self-Control, Deviant Peers, and Cybercrime

In light of the diverse range of offending opportunities facilitated by the Internet, criminologists have begun to explore the ways in which traditional theories of crime may account for these behaviors. One of the most heavily tested theories used to examine cybercrime is Gottfredson and Hirschi's (1990) general theory of crime. They argue humans are rational beings who weigh the costs and benefits of potential behavior, including crime, and act accordingly. Individuals with low self-control, however, are impulsive, insensitive, short sighted, risk-takers who prefer simple tasks. As a result, they are likely to choose the immediate gains of crime even through the long-term consequences are greater. The general theory of crime has

been tested extensively and has received strong support as one of the most significant correlates of street crime (Gottfredson, 2006; Pratt & Cullen, 2000) and juvenile delinquency (Brownfield & Sorenson, 1993; DeLisi & Vaughn, 2008; Winfree, Taylor, He, & Esbensen, 2006

Low self-control has also been linked to various forms of cybercrime, including illegal music downloading (Higgins, Wolfe, & Marcum, 2008; Hinduja & Ingram, 2008), movie piracy (Higgins et al., 2006; Higgins, Fell, & Wilson, 2007), software piracy (Higgins, 2005, 2006; Higgins & Makin, 2004a, b; Higgins & Wilson, 2006; Moon, McCluskey, & McCluskey, 2010), and viewing sexual material online (Buzzell et al., 2006). Tests of self-control and computer hacking, however, have produced mixed effects that do not fully support the general theory of crime (Bossler & Burruss, 2010). Thus, self-control appears to have some value in explaining individual participation for a wide variety of cybercrimes.

A competing theory that has been frequently applied to offending on and off-line is Akers' (1998) social learning theory. Social learning theory argues that individuals become deviant and maintain criminal careers through a dynamic social learning process hinging on differential associations. Individuals become exposed to deviant definitions, models, and reinforcement based on their differences in association patterns. Associating with deviant peers is one of the strongest correlates of crime (Akers, 1998; Akers & Lee, 1996; Krohn, 1999; Lee, Akers, & Borg, 2004; Pratt et al., 2009; Warr, 2002), and is a stronger predictor than low self-control for most forms of crime (e.g., Pratt & Cullen, 2000; Pratt et al., 2009; Tittle et al., 2003; Warr, 2002). Deviant definitions, which consist of an individual's attitudes, perceptions, and justifications for deviance, influence a wide variety of crime and other deviant behaviors (e.g., Akers & Jensen, 2006). In addition, associating with deviant associates provides deviant models to imitate (Boeringer, Shehan, & Akers, 1991). Finally, differential reinforcement, referring to the balance between past, present, and future rewards and punishments, increases the probability of future deviant behavior (Akers & Jensen, 2006; Akers & Lee, 1996; Lee et al., 2004; Pratt et al., 2009).

Social learning theory has significant intrinsic value for understanding the commission of various forms of cybercrime since offenders must "learn not only how to operate a highly technical piece of equipment but also specific procedures, programming, and techniques for using the computer illegally" (Skinner & Fream, 1997, 498). Scholars have found consistent evidence that associating with deviant peers is one of the strongest predictors of a wide variety of cyberdeviance (Bossler & Burruss, 2010; Higgins, 2005; Higgins & Makin, 2004a, b; Higgins et al., 2006; Higgins & Wilson, 2006; Higgins et al., 2007, 2008; Hinduja & Ingram, 2008; Holt et al., 2010; Ingram & Hinduja, 2008; Morris & Higgins, 2010; Skinner & Fream, 1997). In addition, evidence also exists that the other three components of the social learning process are related to cybercrime as individuals are more likely to commit cybercrime if they have definitions favoring the violation of laws controlling the use of computers and the Internet (e.g., Higgins, 2005; Higgins et al., 2006; Hinduja & Ingram, 2008; Holt et al., 2010; Ingram & Hinduja, 2008; Morris & Higgins, 2010; Skinner & Fream, 1997), have deviant computer models to imitate (Holt et al., 2010; Ingram & Hinduja, 2008; Skinner & Fream, 1997), and experience positive reinforcement supporting the violation of computer laws (Hinduja & Ingram, 2008; Holt et al., 2010; Ingram & Hinduja, 2008; Skinner & Fream, 1997).

Since research has consistently identified that both low self-control and deviant peer associations are strong predictors of both traditional and cybercrime offending, emerging scholarship has explored the interactions between these two variables. Gottfredson and Hirschi (1987: 597) provide a theoretical basis for a mediation effect, stating that "people acquire the propensity to delinquency, find delinquent friends, and then commit delinquent acts, including serious criminal acts." Research indicates that individuals with lower levels of self-control self-select into deviant peer groups in the real world (Chapple, 2005; Evans, Cullen, Burton, Dunaway, & Benson, 1997; Longshore, Chang, Hsieh, & Messina, 2004; Mason & Windle, 2002) and online (e.g., Bossler & Holt, 2010; Higgins et al., 2006; Wolfe & Higgins, 2009). In addition, some studies have found that associating with deviant peers mediates the effect of low self-control on both traditional deviant behavior (e.g., Chapple, 2005; Longshore et al., 2004; Mason & Windle, 2002) and cybercrime (e.g., Bossler & Burruss, 2010; Bossler & Holt, 2010; Higgins et al., 2006).

An alternative explanation for this relationship is that criminal propensities interact with social settings to exacerbate the impact of individual characteristics on crime (Evans et al., 1997). It would therefore be predicted that lower levels of self-control would be a stronger predictor of deviance for those with more deviant peers than those with fewer deviant friends. The evidence for this conditioning effect, however, is inconsistent in both the traditional and cybercrime research. Gibson and Wright (2001) found that high school students with lower levels of self-control and more exposure to coworker delinquency were at the greatest risk of occupational offending. Higgins and colleagues extensive research examining the conditioning effect of deviant peer association on the relationship between low self-control and various forms of digital piracy (Higgins, 2005; Higgins et al., 2006, 2007, 2008; Higgins & Makin, 2004a, b), suggest that low self-control might be a stronger predictor of piracy for those with more deviant peer associations; however, z-tests (Paternoster, Brame, Mazerolle, & Piquero, 1998) comparing regression coefficients found no statistically significant differences Other researchers, however, have found that the impact of low self-control became less influential as peer groups became more delinquent (Hinduja & Ingram, 2008; Meldrum, Young, & Weerman, 2009). Thus, it is not clear whether associating with deviant peers strengthen or weakens the effect of low self-control on deviance.

The Present Study

There is substantial evidence that both low self-control and deviant peer associations affect crime and delinquency in the real world and virtual environments. The evidence is mixed, however, regarding the ability of deviant peer associations to mediate and condition the effect of low self-control. In addition, most studies have primarily examined the causes of computer crime and deviance within college samples, reducing our understanding of this phenomenon in juvenile populations. Thus, this study examined whether Gottfredson and Hirschi's (1990) general theory of crime and deviant peer associations explained a substantial proportion of cyberdeviance in sample of Kentucky middle and high school students. In addition,

we explored how low self-control and deviant peer associations interact to explain cybercrime.

Data

The sample for this study was developed at a middle and high school, both adjacent to a large metropolitan area in central Kentucky. These institutions consist of mostly suburban populations, selected based on existing relationships with the research team. One of the authors visited the schools in May 2008 to supervise and explain the data collection process. An online survey instrument was used where students used their school log-in accounts to access the questionnaire that was hosted on the district server. All eighth graders were given the opportunity to participate in the survey. In the high school, only the freshmen class, technology classes, and business classes were provided the opportunity to participate since each of these groups had at least one period in which they had access to computers during the school day.

Due to missing cases and listwise regression, a total of 435 cases were analyzed from the total sample of 518 respondents. Further analyses indicated that the missing cases did not differ significantly on key measures from the cases analyzed. Thus, missing data did not substantively alter the findings and conclusions. The sample represents approximately 25% of the high school population and 35% of the middle school. The sample was 50% female and 79% White, consistent with the school's demographics.

Measures

Dependent Variable

Cyberdeviance On a nine-point ordinal scale (0 = never; 1 = once or twice a year; 2 = once every two to 3 months; 3 = once a month; 4 = once every two to 3 weeks; 5 = once a week; 6 = two to three times a week; 7 = once a day; 8 = two to three times per day), students were asked how many times they committed the following acts within the previous 12 months: 1) knowingly use, make, or give to another person "pirated" media (music, television show, or movie) (mean = 1.29; std.dev. = 2.05); 2) knowingly use, make, or give to another person a "pirated" copy of commercially-sold computer software (mean = .51; std.dev. = 1.39); 3) go to websites to view sexual materials on purpose (mean = .99; std. dev. = 2.08); 4) post mean or threatening messages about another person for others to see (mean = .40; std. dev. = .1.09); and 5) access another's computer account or files without his/her knowledge or permission to look at information or files (mean = .50; std. dev. = 1.30) (Rogers, 2001; Skinner & Fream, 1997; Wolack et al., 2006). Principle components analysis with a varimax rotation indicated a one-factor solution based on the eigenvalues and a scree discontinuity test. The responses to these five items were standardized and averaged (alpha = .713). In order to decrease skewness and kurtosis, the outlier with the highest score was changed to the second highest. In addition, we took the square root of the scores plus one. The final measure ranged from .75 to 2.00 (mean = .96; std. dev. = .28) (see Table 1).

Table 1 Zero-order correlations (n=435)

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	Cyber deviance	–																		
2	Media piracy	.63**	–																	
3	Soft. Piracy	.61**	.46**	–																
4	Pornography	.57**	.23**	.28**	–															
5	Harassment	.55**	.27**	.19**	.17**	–														
6	Hacking	.54**	.19**	.29**	.25**	.41**	–													
7	Self-control	.34**	.17**	.17**	.24**	.27**	.29**	–												
8	Peer deviance	.74**	.49**	.51**	.44**	.44**	.42**	.24**	–											
9	Pr. med. Piracy	.53**	.58**	.44**	.23**	.27**	.22**	.08	.74**	–										
10	Pr. soft. Piracy	.53**	.37**	.55**	.27**	.25**	.21**	.12**	.76**	.59**	–									
11	Pr. porn	.57**	.28**	.29**	.63**	.27**	.31**	.21**	.70**	.38**	.40**	–								
12	Pr. harassment	.48**	.23**	.22**	.15**	.46**	.34**	.22**	.69**	.33**	.34**	.31**	–							
13	Pr. hack	.56**	.28**	.35**	.28**	.38**	.48**	.26**	.75**	.35**	.39**	.43**	.60**	–						
14	Non-school hrs.	.23**	.15**	.14**	.14**	.15**	.18**	.09	.21**	.10*	.11*	.15**	.20**	.22**	–					
15	Computer skill	.28**	.20**	.28**	.17**	.11*	.16**	−.01	.30**	.23**	.24**	.26**	.10*	.24**	.21**	–				
16	Computer loc.	.18**	.10*	.10*	.04	.08	.14**	.03	.13**	.03	.04	.10*	.14	.18	.24**	.12	–			
17	Female	−.27**	−.16**	−.24**	−.46**	.08	−.08	−.15**	−.16**	−.10*	−.14**	−.38**	.12	−.03	−.04	−.22**	−.03	–		
18	Age	.11*	.14**	.14**	.05	−.04	−.07	−.00	.06	.15**	.14**	.01	−.04	−.08	−.14**	.06	.11*	−.14**	–	
19	Report card	−.24**	−.12*	−.06	−.18**	−.20**	−.06	−.30**	−.18**	−.06	−.18**	−.21**	−.08	−.12	−.04	−.02	−.09	.15**	−.15**	–
	Mean	.96	.27	.19	.26	.20	.22	59.37	.00	.95	.49	.96	.00	.00	2.87	1.69	.27	.50	14.99	3.06
	Std. Dev.	.28	.45	.39	.44	.40	.42	12.11	.69	1.12	.87	1.20	.90	.87	1.48	.68	.44	.50	1.38	.92
	Min.	.75	0	0	0	0	0	30	−.69	0	0	0	−.55	−.68	1	0	0	0	13	0
	Max.	2.00	1	1	1	1	1	96	3.50	4	4	4	5.08	4.48	5	3	1	1	19	4

* p<.05; ** p<.01. Media piracy, software piracy, pornography, harassment, and hacking are the dichotomous measures used for the logistic regression models, not the ordinal measures used to create the cyberdeviance measure

Independent Variables

Low Self-Control Low self-control was measured with the 24-item scale (coded 1 = strongly disagree to 4 = strongly agree) created by Grasmick, Tittle, Bursik, and Arneklev (1993) in order to better compare the results with prior studies on crime in general and cybercrime specifically. The scores for the 24 items were summed, creating a measure ranging from 30 to 96 (mean = 59.37; std. dev. = 12.11). Higher scores on the scale indicate less self-control; a positive correlation was thus expected between this measure and the dependent variables. Cronbach's alpha for the index was .87, indicating good reliability. Similar to previous research, principle components analysis indicated six factors with eigenvalues over one. The scree discontinuity test, however, revealed a one-factor solution with the largest drop between the first and second factors.

A small number of scholars have found that there are biased items in the Grasmick et al. scale using Rasch rating scale model analysis (Gibson, Ward, Wright, Beaver, & Delisi, 2010; Higgins, 2007; Piquero, MacIntosh, & Hickman, 2000). Although Gibson, Ward, Wright, Beaver, and Delisi (2010) found that their reduced scale had similar effects on criminal behavior as the full Grasmick et al. scale, we reran all analyses (Tables 1, 2, 3 and 4) with low self-control scales created from the Higgins (2007) (min. 21; max. 64; mean = 40.75; std. dev. = 7.96) and Gibson et al. (2010) (min. 19; max. 64; mean = 41.29; std. dev. = 8.38) models to test the robustness of our findings.[1] In order to compare this study with previous research, we present the traditional Grasmick et al. scale findings in the tables and note the few significant differences (i.e., z-tests between regression coefficients) in the text and footnotes.

Deviant Peer Association On a five-point scale (0 = none; 1 = very few; 2 = about half; 3 = more than half; 4 = all of them), respondents were asked to assess how many of their friends engaged in the following acts of cyberdeviance in the past 12 months: 1) pirating media; 2) pirating computer software; 3) viewing sexual offensive materials online; 4) harassing other online; and 5) engaging in computer hacking (Rogers, 2001; Skinner & Fream, 1997).[2] *Peer deviance* was then computed

[1] We focused on the work of Higgins (2007) and Gibson et al. (2010) because they examined the construct validity of the original Grasmick et al. scale with four options ranging from strongly agree to strong disagree. Piquero, MacIntosh, and Hickman (2000) tested a revised version of the Grasmick et al. scale that had five options measuring how frequent someone acted in that fashion.

[2] Pirating media, pirating software, and viewing offensive sexual materials online were measured with the following three items respectively: 1) knowingly used, made, or gave to another person "pirated" media (music, television show, or movie); 2) knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software; 3) looked at pornographic, obscene, or offensive materials online. Peer harassment was computed by taking the average of the standardized scores for the following four measures (alpha = .919): 1) posted or sent a message about someone for other people to see that made that person feel bad; 2) posted or sent a message about someone for other people to see that made that person feel threatened or worried; 3) sent a message to someone via e-mail or instant message that made that person feel threatened or worried; and 4) sent a message to someone via e-mail or instant message that made that person feel bad. Peer computer hacking was created by averaging the standardized scores for the following three items (alpha = .832): 1) tried to guess another's password to get into his/her computer account or files; 2) accessed another's computer account or files without his/her knowledge or permission just to look at the information or files; and 3) added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission.

Table 2 Linear regression models for total cyberdeviance measure (n=435)

	Model 1			Model 2			Model 3						
							Low association			High association			
	B	SE	Beta	B	SE	Beta	B	SE	Beta	B	SE	Beta	z
LSC	.003**	.001	.148	.006**	.001	.273	.003**	.001	.257	.008**	.002	.290	−2.24
Peer deviance	.253**	.013	.637	–	–	–	–	–	–	–	–	–	
Non-school hrs	.010	.006	.056	.026**	.008	.138	.003	.006	.031	.026*	.013	.127	−1.61
Computer skill	.018	.014	.044	.083**	.018	.203	.021	.012	.111	.058	.030	.122	−1.15
Computer loc.	.041*	.020	.065	.061*	.027	.098	−.013	.019	−.045	.098*	.042	.145	−2.41
Female	−.065**	.018	−.119	−.083**	.024	−.151	−.020	.016	−.081	−.126**	.039	−.205	2.51
Age	.010	.006	.048	.014	.009	.070	.003	.006	.029	.023	.014	.108	−.13
Report grade	−.013	.010	−.043	−.031*	.013	−.103	−.022*	.010	−.155	−.023	.021	−.072	.04
Constant	.617**	.124		.290	.166		.674**	.109		.179	.293		
R2	.595			.259			.121			.260			

*p<.05; **p<.01

Table 3 Logistic regression models for separate cyberdeviance types (n=435)

	Media piracy		Software piracy		Pornography		Harassment		Hacking	
	1	2	1	2	1	2	1	2	1	2
LSC	.033** (.013)	.028** (.010)	.044** (.015)	.038** (.012)	.040** (.014)	.044** (.012)	.043** (.013)	.056** (.012)	.053** (.013)	.067** (.012)
Peer deviance	1.300** (.142)	–	1.568** (.208)	–	1.271** (.158)	–	1.102** (.177)	–	1.124** (.171)	–
Non-school hrs	.159 (.097)	.193* (.081)	.140 (.113)	.167 (.095)	.223 (.116)	.242** (.093)	.101 (.102)	.179 (.092)	.100 (.097)	.169 (.088)
Computer skill	.172 (.217)	.495** (.175)	.698** (.252)	.919** (.212)	−.213 (.239)	.263 (.196)	.388 (.218)	.495* (.199)	.280 (.217)	.520** (.191)
Computer loc.	.391 (.313)	.135 (.259)	.523 (.348)	.185 (.300)	−.398 (.376)	−.109 (.302)	.006 (.332)	.207 (.299)	.335 (.316)	.610* (.280)
Female	−.508 (.290)	−.432 (.239)	−1.038** (.341)	−1.001** (.294)	−2.154** (.381)	−2.557** (.335)	.694* (.312)	.912** (.283)	−.221 (.285)	−.135 (.260)
Age	.109 (.101)	.219** (.084)	.190 (.112)	.226 (.096)*	.095 (.113)	−.016 (.092)	−.074 (.113)	−.072 (.104)	−.087 (.107)	−.153 (.098)
Report card	−.084 (.161)	−.090 (.128)	.463* (.198)	.135 (.154)	−.021 (.182)	−.217 (.142)	−.494* (.162)	−.436** (.149)	.253 (.170)	.130 (.148)
Constant	−6.57** (2.097)	−7.01** (1.689)	−10.97** (2.470)	−9.46** (2.016)	−5.92* (2.319)	−3.16 (1.814)	−3.08 (2.188)	−4.50* (1.991)	−4.98* (2.110)	−5.04** (1.895)
Model χ^2	172.275	48.087	157.052	70.945	227.681	130.549	113.693	63.256	116.260	63.666
R^2	.473	.152	.487	.242	.599	.381	.366	.216	.359	.208

Unstandardized coefficients are presented (standard errors in parentheses); *p<.05; **p<.01. All χ^2 were significant. Pseudo R^2 are Nagelkerke R^2. Software piracy, pornography, harassment, and hacking are all coded as 0 (never) and 1 (options 1–8). Media piracy is coded as 0 (never and option 1) and 1 (options 2–8). Peer deviance is not the overall peer deviance measure used in the linear regression model. It is the peer deviance measure that matches the cyberdeviance type being examined. For example, in the media piracy model, the peer deviance measure is the item assessing how many of the respondents' peers pirate media

Table 4 Logistic regression models for separate cyberdeviance types partitioned by deviant peer association (n=435)

	Media piracy		Software piracy		Pornography		Harassment		Hacking	
	Low (n=198)	High (n=237)	Low (n=293)	High (n=142)	Low (n=211)	High (n=224)	Low (n=233)	High (n=202)	Low (n=170)	High (n=265)
LSC	.048 (.029)	.026* (.013)	.023 (.022)	.067** (.022)	.088* (.037)	.038* (.015)	.056* (.025)	.057** (.016)	.059 (.031)	.071** (.015)
Non-school hrs	.478 (.286)	.153 (.096)	−.025 (.196)	.169 (.136)	.779* (.332)	.128 (.111)	.144 (.248)	.100 (.117)	−.033 (.245)	.147 (.101)
Computer skill	.643 (.524)	.246 (.213)	.863 (.443)	.691* (.313)	−.141 (.560)	.102 (.254)	−.239 (.519)	.588* (.251)	.835 (.449)	.262 (.235)
Computer loc.	.357 (.776)	.218 (.315)	.000 (.662)	.329 (.430)	–[a]	–[a]	−1.214 (1.128)	.124 (.366)	1.153 (.767)	.412 (.319)
Female	−.423 (.758)	−.406 (.290)	−1.362* (.672)	−.975* (.406)	−3.069** (1.164)	−2.232** (.377)	1.361* (.686)	.349 (.362)	.367 (.714)	−.298 (.300)
Age	.150 (.244)	.214* (.103)	.266 (.184)	.259 (.146)	.067 (.285)	.029 (.116)	.120 (.244)	−.041 (.132)	−.215 (.276)	−.039 (.115)
Report card	−.876* (.372)	.018 (.162)	.057 (.300)	.499* (.233)	−.205 (.451)	−.176 (.172)	−.253 (.386)	−.449* (.186)	−.354 (.346)	.211 (.174)
Constant	−8.56 (4.420)	−5.81** (2.213)	−9.47* (3.786)	−11.16** (3.350)	−10.536 (6.032)	−2.312 (2.343)	−8.08 (4.590)	−3.76 (2.667)	−3.99 (4.545)	−6.12** (2.333)
Model χ^2	21.428	20.431	14.579	33.879	24.709	62.809	12.790	36.984	11.299	41.219
R^2	.311	.110	.146	.283	.401	.327	.169	.229	.178	.201

Unstandardized coefficients are presented (standard errors in parentheses); *p<.05; **p<.01; All χ^2 were significant except for the low association models for harassment and hacking. Pseudo R^2 are Nagelkerke R^2. [a] Computer location has a large coefficient (−17.945) and standard error (4887) when included in the low association model. This is because 0 of the 51 individuals with low association who also had a computer in a private setting viewed pornography. Only 8 of the 160 individuals with low association and who had a computer in a public setting viewed pornography. Thus, the viewing of pornography is strongly related to higher levels of deviant associations. We therefore ran the models without the computer location measure and included those results in the table. There were no substantively different results for the other measures

by averaging the standardized scores for these five items, giving each of the five items equal weight in the measure (a=.776).

Control Variables

Non-school hours was assessed by asking the respondents how many hours per week they spent on computers for non-school related reasons over the last 6 months (1 = less than 5 h; 2 = five to 10 h; 3 = 11 to 15 h; 4 = 16 to 20 h; 5 = 21 or more hours). Spending more time in online environments for personal use unrelated to school or work may provide greater opportunities to offend, such as sending threatening or emotionally hurtful messages (Hinduja & Patchin, 2009; Holt & Bossler, 2009).

Computer skill was a four-point ordinal measure based on general categories of computer proficiency: (0) I am afraid of computers and don't use them unless I absolutely have to (afraid); (1) I can surf the 'net, use common software, but cannot fix my own computer (beginner); (2) I can use a variety of software and fix some computer problems I have (intermediate); and (3) I can use Linux, most software, and fix most computer problems I have (advanced) (Rogers, 2001). This measure was included to understand the influence that computer skill may have on an individual's capacity to offend, since those with greater knowledge of technology may be better able to engage in more complex offenses (Higgins, 2005; Hinduja, 2001; Holt, 2007).

Computer location was a dichotomous measure (0 = public setting; 1 = bedroom or laptop). Parents can more easily detect computer deviance when the computer is in a public area such as a family room or kitchen (Bocij, 2004; Wolack et al., 2006). Thus, requiring computer use in heavily trafficked areas can reduce opportunities for juveniles to engage in cybercrime.

Demographics Sex (0 = male; 1 = female) was a dichotomous measure. *Age* was a continuous measure ranging from 13 to 19 (mean = 14.99; std. dev. = 1.38). *Grades on report cards* was a self-reported ordinal measure consisting of: (0) mostly Fs; (1) mostly Ds; (2) mostly Cs; (3) mostly Bs; and (4) mostly As.

Results

The correlation matrix, presented in Table 1, indicated that the hypothesized relationships were supported. Low self-control (r=.34) was positively correlated with the commission of cyberdeviance. Associating with deviant peers had a strong correlation with respondent cyberdeviance (r=.74). Low self-control and deviant peer associations were correlated with each other (r=.24). In addition, the three opportunity variables were correlated with cyberdeviance. Spending more time online for non-school related reasons (r=.23), possessing greater computer skill (r=.28), and having a computer in a personal setting (r=.18) were all positively related with the commission of cyberdeviance. Age (r=.11) was positively correlated with cyberdeviance while being female (r=−.27) and having higher grades (r=−.24) were negatively correlated (Hinduja, 2001; Jordan & Taylor, 1998). Thus, these bivariate analyses provided strong support to further explore the hypotheses via multivariate analyses.

We estimated a linear regression model with cyberdeviance as the dependent variable (see Table 2, Model 1). Multicollinearity did not appear to bias the parameter estimates as the independent variables were not strongly correlated with each other (see Table 1) and the highest VIF and lowest tolerance were 1.223 and .817 respectively (results not shown). The linear regression model indicated that individuals with lower levels of self-control were more likely to commit cyberdeviance in general. Associating with peers who commit computer deviance, however, remained significant and was the strongest predictor of cyberdeviance overall (Bossler & Burruss, 2010; Higgins et al., 2006). Keeping a computer in a personal setting increased participation in cyberdeviance by decreasing parental monitoring. Females were also less likely to commit online deviance in keeping with larger research on cybercrime (Hinduja, 2001; Jordan & Taylor, 1998; Skinner & Fream, 1997). Most of the other measures were not significant in the full model, although they had significant zero-order correlations.

An additional model was run without the peer cyberdeviance measure in order to examine whether associating with deviant peers mediated the effect of low self-control (see Table 2, Model 2). Model 2 explained 25.9% of the variation, while Model 1 explained 59.5%, illustrating the importance of peer deviance in predicting cyberdeviance (Bossler & Burruss, 2010; Higgins et al., 2006). Model 2 also indicated that the effect of low self-control on cyberdeviance significantly increased when peer deviance was not included in the model (z score = −2.12).[3] In addition, the number of hours spent online for non-school related reasons, computer skill, and grades were significant when peer deviance was not included in the model. Thus, peer deviance appears to mediate the relationship between self-control, opportunity, and cyberdeviance. Additionally, low self-control appears to have both a direct and indirect effect via peer offending on youth cyberdeviance.[4]

In order to examine whether different levels of deviant peer associations conditioned the effect of low self-control on cyberdeviance, the sample was partitioned by the median of peer deviance (−.181) and models were run separately for those with low and high deviant peer associations (Higgins et al., 2007; Higgins & Makin, 2004a). Model 3 indicated that low self-control was significant for both groups, but that low self-control had a significantly larger effect for those with more deviant peer associations, thus strengthening its effect (z=−2.24). This indicated that associating with deviant peers exacerbated the effect of low self-control, supporting the finding of Gibson and Wright (2001) and the suggestive evidence of Higgins and colleagues work on digital piracy (e.g., Higgins et al., 2006, 2007; Higgins & Makin, 2004a, b).[5]

[3] There are two statistically significant differences (Paternoster et al., 1998) between the three self-control measures in Model 2. First, the Gibson measure had a statistically significant stronger effect on cyberdeviance (b = .009; std. error = .001). Second, a statistically significant mediation effect is found in Model 2 when using the traditional Grasmick et al. scale and the Gibson scale, but not the Higgins scale. The standard error for low self-control using the Higgins scale is .002 rather than .001 as is found for the other two measurements.

[4] In order to further verify this conclusion, a linear regression was conducted with peer deviance as the dependent variable (results not shown). This model indicated that low self-control, spending more time online for non-school related reasons, computer skill, and lower report card grades all increased the association with delinquent others.

[5] Although there were no statistically significant differences between the three different measures of low self-control within the two subgroups, the Gibson et al. measure indicated a conditioning effect (z=−3.13), congruent with that of the unstandardized scale. The Higgins measure had no such effect (z=−1.58), though this was because of the larger standard errors.

The above analyses were also run for each of the five components of the cyberdeviance measure to examine whether the findings were consistent for all cybercrime types. The correlation matrix (see Table 1) indicated that low self-control and deviant peer associations were significantly correlated with each form. We ran a logistic regression model for each of the dichotomized components (see Table 3, Model 1 s).[6] These models indicated that the effects of both low self-control and deviant peer associations were robust. Lower levels of self-control and higher levels of deviant peer associations increased the odds of each of the five forms of cyberdeviance, representing the entire range of Wall's (2001) typology. In fact, z-tests (results not shown) indicated that low self-control had consistent effects for all five cyberdeviance types, meaning that low self-control did not predict one type of cyberdeviance better than another. Thus, low self-control was able to predict simple forms of cyberdeviance, like viewing online sexual material and harassing others online, as well as cybercrimes that require some knowledge of computer technology, including piracy (see Higgins, 2005; Higgins et al., 2006) and hacking (Bossler & Burruss, 2010).[7] Z-tests (results not shown) found this to be true for peer deviance as well, meaning that associating with deviant peers did not increase the odds of committing one form of cyberdeviance more than another.

Although the logistic regression models indicated that low self-control and peer deviance predicted each form of cyberdeviance (see Table 3), not all of the other factors predicted the cyberdeviance types equally. For example, students with higher levels of computer skill and higher grades were more likely to pirate software (Hinduja, 2001). Computer skills did not, however, predict other forms of offending when controlling for peer deviance. Gender was not related to either media piracy or hacking, incongruent with previous research (Higgins et al., 2006; Holt, 2007; Jordan & Taylor, 1998). Males were more likely to pirate software (Higgins, 2005, 2006; Hinduja, 2001) and view sexual materials online. Females, however, were more likely than their male counterparts to harass others online (Hinduja & Patchin, 2009).

We also examined whether the mediating and conditioning effects found in the above analyses for cyberdeviance in general (see Table 2) would hold for each of the five cyberdeviance types. The model 2s in Table 3 exclude their respective peer deviance measure to examine for mediating effects. Z-tests (results not shown) indicated that the low self-control coefficients were not significantly different between the model 1s and model 2s. Table 4 contains the models for each type partitioned by its respective peer deviance measure to test for conditioning effects.[8] Z-tests (results not shown) did not

[6] We dichotomized the components because of heavy skew and little variation. Most students did not commit these offenses or performed them at lower levels (see descriptives Table 1). Therefore, we dichotomized software piracy, pornography, harassment, and computer hacking (0 = no; 1 = yes) in order to examine whether self-control predicted the probability of committing these acts. Media piracy (mean = 1.29; std. dev. = 2.05) was a partial exception to the trend, as 55.9% of the sample did not engage in this offense within the last year. Another 16.8% stated that they had pirated media once or twice in the last year. This total (72.7%) is similar to the percentages of students who had not committed any of the other offenses; thus we dichotomized media piracy based on students who engaged in piracy less than twice in the last 12 months (0) and those who committed it more often (1).

[7] Z-tests indicate that there were no significant differences in the abilities of the Grasmick et al., Higgins, and Gibson scales in predicting the five types of cyberdeviance.

[8] Since the individual peer deviance measures were five-point ordinal measures, we could not partition the models by medians. Instead, we partitioned on whether or not the person had deviant peer associations for that specific item (i.e. low = 0; high = all other options).

find any significant differences between the low self-control regression coefficients between the subgroups. Thus, no significant evidence was found that deviant peer associations mediated or conditioned the effect of low self-control on any of the five cyberdeviance types. Deviant peer associations, however, mediated and conditioned the effect of low self-control on cyberdeviance in general (see Table 2).

Discussion and Conclusions

Gottfredson and Hirschi's (1990) general theory of crime and Akers' (1998) social learning theory are two of the most widely supported theories in criminology (Akers & Jensen, 2006; Gottfredson, 2006; Pratt & Cullen, 2000; Pratt et al., 2009). Both low self-control and deviant peer associations have been linked to numerous forms of real world crime and cybercrime. Most of our knowledge on the link between low self-control, peer associations, and cyberdeviance, however, is primarily based on college samples (e.g., Higgins, 2005, Higgins & Makin 2004a, b; Holt et al., 2010). Few studies have considered the applicability of low self-control and social learning theory to juvenile participation in cybercrime. This study utilized a sample of middle and high school students and found that low self-control predicted the commission of cyberdeviance in general and various forms of cyberdeviance specifically (e.g., Higgins, 2005, 2006; Higgins & Makin, 2004a, b; Higgins et al., 2006, 2007). In addition, self-control did not significantly predict any form of cyberdeviance with more emphasis than another.

This study also found that peer offending had a stronger effect on offending than low self-control (Pratt & Cullen, 2000; Tittle et al., 2003) and consistently predicted each type of cyberdeviance. In fact, it appears that peer offending partially mediated and conditioned the relationship between low self-control and cybercrime offending in general. As a consequence, peers with low self-control appear to coalesce in virtual environments in much the same way as in the real world (Higgins et al., 2006; Wolfe & Higgins, 2009). In addition, associating with deviant peers exacerbated the effect of low self-control on cyberdeviance in general (e.g., Gibson & Wright, 2001). However, these interactions were not found when examining the five components of the cyberdeviance measure. Thus, further research is needed to disentangle the influence and interaction of peers and low self-control in on and off-line contexts.

Additionally, the findings from this research raise questions about the relationship between juvenile participation in cybercrime and juvenile delinquency off-line. There is a clear relationship between low self-control, deviant peers, and cybercrime, though it is less clear if there is an association between real world offending and participation in cybercrime. The anonymity afforded by the Internet and computer technology, coupled with the relative ease and innocuous appearance of most online activities in public settings, may make cyberdeviance more attractive to some youths than real world offenses. Limited research suggests individuals who engage in bullying in online environments also bully others in the real world (Hinduja & Patchin, 2009). Thus, future research is needed to explore the relationship between low self-control, deviant peers, and participation in real world crime and cybercrime.

The limitations of this study, however, necessitate further research on the problem of cybercrime. Specifically, a cross-sectional study was conducted at one middle

school and one high school in Kentucky. The findings appear to be generalizable to other groups, though sampling in other parts of the country would determine whether a regional effect exists. In addition, the cross-sectional nature of the study does not allow for a causal examination of deviant peer association and delinquency. Longitudinal data would better allow the disentanglement of these effects. Additionally, while basic demographic correlates were examined, there were no measures for parental income or other factors that may affect access to technology and the Internet on a regular basis. Future research is needed to consider the ways in which ecological conditions may affect cybercrime offending at an early age.

References

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press.

Akers, R. L., & Jensen, G. F. (2006). The empirical status of social learning theory of crime and deviance: The past, present, and future. In F. T. Cullen, J. P. Wright, & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 37–76). New Brunswick: Transaction Publishers.

Akers, R. L., & Lee, G. (1996). A longitudinal test of social learning theory: Adolescent smoking. *Journal of Drug Issues, 26*, 317–343.

Bocij, P. (2004). *Cyberstalking: Harassment in the internet age and how to protect your family*. Westport: Praeger.

Boeringer, S., Shehan, C. L., & Akers, R. L. (1991). Social contexts and sexual learning in sexual coercion and aggression: Assessing the contribution of fraternity membership. *Family Relations, 40*, 558–564.

Bossler, A. M., & Burruss, G. W. (2010). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 57–81). Hershey: 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.

Brownfield, D., & Sorenson, A. (1993). Self-control and juvenile delinquency: Theoretical issues and an empirical assessment of selected elements of a general theory of crime. *Deviant Behavior, 14*, 243–264.

Buzzell, B., Foss, D., & Middleton, Z. (2006). Explaining use of online pornography: A test of self-control theory and opportunities for deviance. *Journal of Criminal Justice and Popular Culture, 13*, 96–116.

Chapple, C. L. (2005). Self-control, peer relations, and delinquency. *Justice Quarterly, 22*, 89–106.

DeLisi, M., & Vaughn, M. (2008). The Gottfredson-Hirschi critiques revisited: Reconciling self-control theory, criminal careers, and career criminals. *International Journal of Offender Therapy and Comparative Criminology, 52*, 520–537.

DiMarco, H. (2003). The electronic cloak: Secret sexual deviance in cybersociety. In Y. Jewkes (Ed.), *Dot. cons: Crime, deviance, and identity on the internet* (pp. 53–67). Portland: Willan Publishing.

Edleman, B. (2009). Red light states: Who buys online adult entertainment? *Journal of Economic Perspectives, 23*, 209–220.

Evans, T. D., Cullen, F. T., Burton, V. S., Jr., Dunaway, R. G., & Benson, M. L. (1997). The social consequences of self-control: Testing the general theory of crime. *Criminology, 35*, 475–501.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*, 468–483.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Boston: Addison Wesley.

Gibson, C. L., Ward, J. T., Wright, J. P., Beaver, K. M., & Delisi, M. (2010). Where does gender fit in the measurement of self-control? *Criminal Justice and Behavior, 37*, 883–903.

Gibson, C., & Wright, J. (2001). Low self-control and coworker delinquency: A research note. *Journal of Criminal Justice, 29*, 483–492.

Gopal, R., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. (2004). A behavioral model of digital music piracy. *Journal of Organizational Computing and Electronic Commerce, 14*, 89–105.

Gottfredson, M. R. (2006). The empirical status of control theory in criminology. In F. Cullen, J. P. Wright, & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 77–100). New Brunswick: Transaction Publishers.

Gottfredson, M. R., & Hirschi, T. (1987). The methodological adequacy of longitudinal research on crime. *Criminology, 25*, 581–614.

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

Grasmick, H. G., Tittle, C. R., Bursik, R. J., Jr., & 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. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*, 1–24.

Higgins, G. E. (2006). Gender differences in software piracy: The mediating roles of self-control theory and social learning theory. *Journal of Economic Crime Management, 4*, 1–30.

Higgins, G. E. (2007). Examining the original Grasmick scale: A Rasch model approach. *Criminal Justice and Behavior, 34*, 157–178.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies, 19*, 3–22.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2007). Low self-control and social learning in understanding students' intentions to pirate movies in the United States. *Social Science Computer Review, 25*, 339–357.

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*, 1–21.

Higgins, G. E., & Makin, D. A. (2004b). Self-control, deviant peers, and software piracy. *Psychological Reports, 95*, 921–931.

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*, 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*, 440–460.

Hinduja, S. (2001). Correlates of internet software piracy. *Journal of Contemporary Criminal Justice, 17*, 369–382.

Hinduja, S., & Ingram, J. R. (2008). Self-control and ethical beliefs on the social learning of intellectual property theft. *Western Criminology Review, 9*, 52–72.

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

Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks: Sage Publications.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*, 171–198.

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

Holt, T. J., Burruss, G. W., Bossler, A. M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice 33,* page numbers not assigned yet

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

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*, 757–780.

Krohn, M. D. (1999). Social learning theory: The continuing development of a perspective. *Theoretical Criminology, 3*, 462–475.

Lane, F. S. (2000). *Obscene profits: The entrepreneurs of pornography in the cyber age*. New York: Routledge.

Lee, G., Akers, R. L., & Borg, M. J. (2004). Social learning and structural factors in adolescent substance use. *Western Criminology Review, 5*, 17–34.

Longshore, D., Chang, E., Hsieh, S., & Messina, N. (2004). Self-control and social bonds: A combined control perspective on deviance. *Crime & Delinquency, 50*, 542–564.

Mason, W. A., & Windle, M. (2002). Gender, self-control, and informal control in adolescence: A test of three models of the continuity of delinquent behavior. *Youth and Society, 33*, 479–514.

Meldrum, R. C., Young, J. T. N., & Weerman, F. M. (2009). Reconsidering the effect of self-control and delinquent peers: Implications of measurement for theoretical significance. *Journal of Research in Crime and Delinquency, 46*, 353–376.

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*, 767–772.

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*, 470–480.
Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology, 36*, 859–866.
Piquero, A. R., MacIntosh, R., & Hickman, M. (2000). Does self-control affect survey response? Applying exploratory, confirmatory, and item response theory analysis to Grasmick et al.'s self-control scale. *Criminology, 38*, 897–929.
Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology, 38*, 931–964.
Pratt, T. C., Cullen, F. T., Sellers, C. S., Winfree, L. T., Madensen, T., Daigle, L. E., et al. (2009). The empirical status of social learning theory: A meta-analysis. *Justice Quarterly, 27*, 765–802.
Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study.* Unpublished doctoral dissertation. Manitoba University, Canada
Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*, 495–518.
Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2010). *Digital crime and digital terrorism* (2nd ed.). Upper Saddle River: Pearson Prentice Hall.
Tittle, C. R., Ward, D. A., & Grasmick, H. G. (2003). Gender, age, and crime/deviance: A challenge to self-control theory. *Journal of Research in Crime and Delinquency, 40*, 426–453.
Wall, D. S. (2001). Cybercrimes and the internet. In D. S. Wall (Ed.), *Crime and the internet* (pp. 1–17). New York: Routledge.
Warr, M. (2002). *Companions in crime: The social aspects of criminal conduct*. Cambridge: Cambridge University Press.
Winfree, L. T., Taylor, T. J., He, N., & Esbensen, F. (2006). Self-control and variability over time: Multivariate results using a 5-year, multisite panel of youths. *Crime and Delinquency, 52*, 253–286.
Wolack, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimization of youth: 5 years later*. Washington: National Center for Missing & Exploited Children.
Wolfe, S. E., & Higgins, G. E. (2009). Explaining deviant peer associations: An examination of low self-control, ethical predispositions, definitions, and digital piracy. *Western Criminology Review, 10*, 43–55.
Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal, 44*, 387–399.

Thomas J. Holt is an Assistant Professor in the School of Criminal Justice at Michigan State University. He received his Ph.D. in criminology and criminal justice from the University of Missouri—Saint Louis. His research focuses on cybercrime and the ways that technology and the Internet facilitate deviance.

Adam M. Bossler is an Assistant Professor of Justice Studies at Georgia Southern University. He has a doctorate in criminology and criminal justice from the University of Missouri—St. Louis. His current research focuses on the application of traditional criminological theories to cybercrime offending and victimization.

David C. May is a Professor and Kentucky Center for School Safety Research Fellow in the Department of Criminal Justice at Eastern Kentucky University. He has published numerous articles in the areas of responses to school violence, perceptions of the severity of correctional punishments, fear of crime, and weapon possession, two books examining the antecedents of gun ownership and possession among male delinquents, and a book on perceptions of the punitiveness of prison.