On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory

Adam M. Bossler[1]
Georgia Southern University, USA

Thomas J. Holt[2]
Michigan State University, USA

Abstract

Malicious software, such as viruses and Trojan horse programs, can automate a variety of attacks for criminals and is partially responsible for the global increase in cybercrime. Criminology, however, has been slow to explore the theoretical causes and correlates of malware victimization. This study uses a routine activities framework to explore data loss caused by malware infection in a college sample. Similar to research on traditional forms of victimization, computer deviance was related with computer victimization. Physical guardianship, however, had little effect. Policy implications to decrease malware victimization in a college sample focus on decreasing computer deviance rather than physical target hardening.

Keywords: malware; cybercrime; computer crime; routine activities

Introduction

The Internet and World Wide Web have dramatically altered the way we communicate, live, and conduct business around the world. These advancements have modified traditional activities, such as banking, dating, and shopping, into activities in which individuals interact with others but neither leave the house nor actually physically meet people (Newman & Clarke, 2003). The growth and penetration of computer technology in modern life has provided criminals with efficient tools to commit crime by providing opportunities to commit crimes that could not exist without cyberspace. Few criminologists, however, have empirically assessed the impact of computer technology on victimization. As a consequence, there is a lack of understanding in the ability of traditional theories of crime to account for the prevalence and potential reduction of cybercrime victimization. In particular, routine activities theory (Cohen & Felson, 1979)

[1] Assistant Professor, Department of Political Science, Georgia Southern University, 2216 Carroll Building, Statesboro, GA 30460, USA. E-mail: abossler@georgiasouthern.edu
[2] Assistant Professor, School of Criminal Justice, Michigan State University, 560 Baker Hall, East Lansing, MI 48824, USA. Email: holtt@msu.edu

may be successful in this endeavor as it has been traditionally used to examine how technological innovations affect crime patterns and victimization.

One of the more common and significant forms of cybercrime victimization is the destruction of data files due to malicious software, or malware (Furnell, 2002; Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006). Malware typically includes computer viruses, worms, and Trojan horse programs that alter functions within computer programs and files. Viruses can conceal their presence on computer systems and networks and spread via e-mail attachments, downloadable files, instant messaging, and other methods (Kapersky, 2003; Szor, 2005; Taylor et al., 2006). Trojan horse programs also often arrive via e-mail as a downloadable file or attachment that people would be inclined to open, such as files titled "XXX Porn" or "Receipt of Purchase." When the file is opened, it executes some form of a malicious code (Furnell, 2002; Szor, 2005; Taylor et al., 2006). In addition, some malware is activated by visiting websites, particularly pornographic websites, which exploit flaws in web browsers (Taylor et al., 2006). Though worms do not involve as much user interaction as other malware because of its ability to use system memory and to send copies of itself, humans can facilitate its spread by simply opening e-mails that have the worm code embedded in the file (Nazario, 2003).

Cybercriminals often utilize malware to compromise computer systems and automate attacks against computer networks (Furnell, 2002). These programs can disrupt e-mail and network operations, access private files, delete or corrupt files, and generally damage computer software and hardware (Taylor et al., 2006). The dissemination of viruses across computer networks can be costly for several reasons, including the loss of data and copyrighted information, identity theft, loss of revenue due to customer apprehension about website safety, time spent removing the programs, and losses in personal productivity and system functions (Symantec, 2003; Taylor et al., 2006). This is reflected in the dollar losses associated with malware infection. U.S. companies who participated in a recent Computer Security Institute reported losses of approximately $15 million because of viruses in 2006 alone (CSI, 2007). An infected system in one country can spread malicious software across the globe and cause even greater damage because of the interconnected nature of computer systems. The Melissa virus, for example, caused an estimated $80 million in damages worldwide (Taylor et al., 2006). Thus, malware infection poses a significant threat to Internet users around the globe.

A large body of information security research explores the technical aspects of malicious software. These research efforts have placed special emphasis on the creation of software applications like anti-virus programs that can identify and contain malicious software on computer systems (Kapersky, 2003; PandaLabs, 2007; Symantec, 2003). For these programs to work as effectively as possible, however, individual computer users must obtain, update, and utilize them regularly. Thus, in order to better understand the spread and prevention of malware, the exploration of a theoretical approach that focuses on human behavior, such as routine activities theory (Cohen & Felson, 1979), is necessary because of the role that human behavior and interactions play in the spread of malicious software. Routine activities theory has had significant success in accounting for traditional forms of offending and appears to apply to some on-line crimes, such as harassment or stalking (Holt & Bossler, 2009).

It is unclear as to whether routine activities theory can address forms of crime that are not based in physical time and space and that exist solely on computer systems, such as malware infection (see Choi, 2008). In order to address this gap in the literature, this

study will explore the prevalence and correlates of malware infection by examining hypotheses derived from the routine activities theory. The findings illustrate the social dimensions of this computer-focused, technological crime. We conclude with policy implications focused on the connection between participation in computer deviance and victimization rather than simple target hardening.

Routine Activities Theory and Malware Victimization

According to Cohen and Felson's (1979) routine activities theory (hereafter RAT), direct-contact predatory victimization occurs with the convergence in both space and time of three components: a motivated offender, the absence of a capable guardian, and a suitable target. Motivated offenders are individuals and groups who have both the inclination and ability to commit crime for various reasons (Cohen & Felson, 1979). Guardianship refers to the capability of persons and/or objects that prevent the motivated offender from injuring or attacking the target. Individuals are more likely to be victimized if they spend time in the presence of deviants or criminals, if they or their possessions are seen as valuable, and if no guardian is present to adequately protect the potential victims or their property. This perspective can aid in understanding the commission of crime by focusing on the way that daily routine activities affect capable guardianship and target suitability. For example, individuals typically leave their houses approximately at the same time every day to go to work or school, creating a predictable pattern that both places them in public areas closer to motivated offenders and leaving their home unguarded. Thus, routine activities are important in our understanding of crime in that they often separate individuals from the safety of their home, the people they know and trust, and the possessions they value.

RAT has had significant success in explaining a wide range of victimization types, such as burglary (Cohen & Felson, 1979; Coupe & Blake, 2006), larceny (Mustaine & Tewksbury, 1998), vandalism (Tewksbury & Mustaine, 2000), physical assault (Stewart et al., 2004), robbery (Spano & Nagy, 2005), and fraud (Holtfreter et al., 2008). Several scholars have briefly discussed how RAT can be applied to cybercrime as well (Grabosky, 2001; Grabosky & Smith, 2001; Newman & Clarke, 2003; Taylor et al., 2006; see Yar, 2005 for longer discussion). However, there are limited studies testing the empirical validity of RAT in relation to the commission of cybercrime. Specifically, Hinduja and Patchin (2008) found that computer proficiency and time spent on-line were positively related to cyber bullying victimization for adolescent Internet-users. Similarly, Holt and Bossler (2009) discovered that spending more time in on-line chat rooms and committing computer deviance increased the odds of on-line harassment.

RAT may have some applicability to person-based forms of cybercrime, though its applicability regarding property-based cybercrimes, such as malicious software infection, is unclear. Malware can be classified as a form of "cyber-theft" if a criminal uses these programs to steal data or information (Wall, 2001). Malware infection does, in fact, share characteristics with burglary, in that, malware infects and compromises computer systems in a similar fashion to how burglars enter a dwelling. Burglars surreptitiously utilize common or concealed points of entry to minimize the likelihood of detection (Wright & Decker, 1994). They may also use force to obviate locks or other security measures to gain access. Most malicious software infects computers through a weakness, or vulnerability, in the system that allows the code to covertly activate and take control of system processes (Taylor et al., 2006). Malware can also disable antivirus programs and other security

measures to ensure that its payload is delivered successfully, in much the same way that a burglar can deactivate a security system (Kapersky, 2003). Given the potential theoretical overlap between malware infection and traditional crime, specifically burglary, it would appear fruitful to consider how the three components of RAT might also apply to malware.

Proximity to Motivated Offenders

When considering the applicability of RAT to cybercrime, it is vital to consider whether daily computer activities, legal or illegal, place individuals in proximity to motivated offenders, similar to how daily activities place individuals in closer proximity to motivated offenders in physical space. A major difference between most forms of real world crime and cybercrime is the removal of physical distance between the motivated offender and a suitable target (Yar, 2005). A few motivated malware writers can have a substantial impact on a large number of victims without engaging in physical contact with the victims (Taylor et al., 2006). The critical issue therefore is not whether the potential victims are in close physical proximity to a malware writer, but are they in close virtual proximity to an offender's tool. In addition, victims do not have to have a unique temporal interaction with malware in order for their computer to become infected (Taylor et al., 2006). In most cases, malware is either present for as long a period as possible on a specific website or file, or it can activate when a certain function is performed.

Therefore, the activities of the potential victims and the websites or files they come into contact with are more important than the times of the activities. While the amount of time on-line in general might increase the odds of malware infection, RAT research has found that specific leisure activities are more strongly correlated with traditional victimization rates than simply the number of times individuals leave their homes for leisure (Mustaine and Tewksbury 1998; 2002). Thus, this indicates that it may be more likely that the number of hours one spends partaking in *specific* activities on the computer is more important in understanding malware infection. Individuals who spend more time on websites in which they download files, share personal information, or provide credit card information expose themselves to a variety of dangers that may increase their risk of malware victimization. In addition, individuals who own their own computers and utilize high speed Internet connections may increase their risk of victimization. High speed connections allow for greater and more rapid access to materials and file sharing (see Hinduja, 2001), thereby increasing contact with potentially infected files.

Considering the substantial link between offending and victimization in real world environments (e.g., Mustaine & Tewksbury, 1998; Stewart et al., 2004), it is reasonable to suspect that a similar connection exists in virtual settings as well. For example, Holt and Bossler (2009) found that computer deviance increased the odds of on-line harassment victimization. Those who engage in computer deviance may also increase their risk of exposure to infected files and motivated offenders. Pirating software and media may be important correlates of malware infection since piracy involves constant downloading and opening files of unknown origin. Visiting pornographic websites and viewing sexually explicit materials may increase exposure to malware because of viruses hidden in these files as well (Szor, 2005). Finally, participating in hacker-like behaviors has been shown to increase the risk of victimization by other hackers (Holt, 2007), which could include the use of malicious software.

Absence of Capable Guardianship

Physical guardianship is argued to be as important in preventing digital crime as it is in preventing residential burglary (Grabosky & Smith, 2001). Most studies have found that the use of physical security devices, including burglar alarms, external lights, extra locks, and other security measures, reduces the risk of burglary and larceny victimization (Coupe & Blake, 2006; Cromwell & Olson, 2004; Miethe & McDowall, 1993). Even when offenders argue that they are not concerned with these physical guardians, they still normally choose houses without them. Other scholars, however, have argued that locks are not much of a deterrent for burglars. Once the decision has been made to burglarize a house, the lock simply becomes an obstacle for the burglar to address (Wright & Decker, 1994). Though studies have produced mixed results on the impact of preventative measures (see Mustaine & Tewksbury, 1998; Tseloni et al., 2004), it appears that any target hardening that decreases opportunity and increases physical guardianship reduces the odds of victimization, especially burglary.

Grabosky and Smith (2001) argue that many forms of cybercrime victimization occur simply because of an absence of capable physical guardianship. Physical guardians are readily available on computer systems through antivirus software and similar programs (Kapersky, 2003; Mell et al., 2005; PandaLabs, 2007). These programs are expressly designed to reduce the likelihood of malware infection and data loss by either scanning and preventing infected files from being introduced to the system or identifying and removing malicious software if it already has infected the system (see Mell et al., 2005; Taylor et al., 2006). Thus, physical guardians in cyberspace work similarly to physical guardians in the real world.

Social guardianship "refers to the availability of others who may prevent personal crimes by their mere presence or by offering assistance to ward off an attack" (Spano & Nagy, 2005: 418). In fact, one of the primary characteristics of adequate guardianship according to burglars is whether a house is occupied (Coupe & Blake, 2006; Cromwell & Olson, 2004; Shover, 1996; Wright & Decker, 1994). Most burglars state that they would never intentionally burglarize a house if they knew someone was home. In addition, individuals can decrease their social guardianship by associating with delinquent friends. Associating with delinquent friends not only places an individual in closer proximity to motivated offenders, but also reduces the likelihood of their friends intervening when others are being victimized (Zhang et al., 2001).

A similar phenomenon appears to exist in cyberspace as well. Individuals who associate with friends who commit various forms of computer deviance increase their risks of being harassed on-line (Holt & Bossler, 2009). Presumably, delinquent friends are more likely to harass their friends and less likely to support and protect them in their on-line interactions. Considering how malware spreads across computer systems, the relationship between deviance and victimization exists for the spread of malicious software. Viruses and worms often identify and use e-mail address books to send copies of their program to others (Furnell, 2002; Nazario, 2003). If a close associate's computer is infected, possibly due to computer deviance, the malware may try to compromise other machines. As a result, friends who download music or view pornography on-line may increase the risk of malware distribution and infection for others.

Victims can also participate in their own guardianship by taking "evasive actions which encourage offenders to pursue targets other than their own" (Cohen & Felson, 1979: 590). Many victims of burglary are victimized because they have inadvertently provided

valuable information to others, such as when they are going to be away from home or how to deactivate a security system (Cromwell & Olson, 2004). Self-protective behaviors, however, do not appear to decrease victimization when the individual knows the perpetrator, such as in many cases of sexual assault (Mustaine & Tewksbury, 2002; Schwartz et al., 2001). In such cases, the victim does not anticipate the need for self-protective measures.

Personal guardianship plays a role in cybercrime prevention as it can be considered the primary form of defense (Grabosky, 2001). Individuals need to be aware of the possible risks and consequences that cybercrime or malware can have on their computer system and of the basic preventative measures that one can take to decrease these risks (Grabosky & Smith, 2001). Individuals need to continuously update their physical guardianship tools, including antivirus programs and critical operating system updates (Mell et al., 2005; Szor, 2005). In addition, individuals should limit interactions with strangers as it could increase the odds of different forms of on-line victimization (Ybarra et al., 2007). Opening e-mails from unknown individuals or sources also increases the risk of victimization as attachments may contain malware (Szor, 2005; Taylor et al., 2006). Gaining knowledge of computer technology may reduce the likelihood of victimization by providing the user with the ability to correctly identify any system anomalies or errors indicative of malware infection (Furnell, 2002; Taylor et al., 2006). Finally, individuals can protect themselves by using complex passwords that are changed regularly and keeping these passwords private (Furnell, 2002; Nazario, 2003; Taylor et al., 2006).

Suitable Targets

In context to RAT, suitable targets "can be any person or property that an offender would like to take or control" (Felson, 2001: 43). Research has found that offenders consider the possible rewards of offending as a more important factor in their decision-making process than potential consequences (Cromwell & Olson, 2004; Shover, 1996; Wright & Decker, 1994). Residents with a higher income who live in areas of general affluence, or visibly display signs of wealth, such as cars and electronics, are more likely to be victimized as burglars associate the wealth of the area with the value of the items within the houses (Coupe & Blake, 2006; Cromwell & Olson, 2004; Miethe & Meier, 1994; Osborn & Tseloni, 1998). Unlike burglary targets, it appears that everyone connected to the Internet, and their information, is a suitable target for most forms of malware, although malware can be used for targeted attacks as well (Newman & Clarke, 2003; Yar, 2005). Even when a specific individual or website is not directly targeted by a malware writer, it may be incidentally affected because of the connectivity of the Internet by the disruption of a specific major website. In other cases, the target is the disruption of the entire Internet itself, rather than any specific website (Newman & Clarke, 2003). As a result, there may be no gender, age, or race differences in target attractiveness relative to the risk of malware infection since computers and their contents are the primary targets, not the individuals.

The Present Study

The theoretical discussion above illustrates the linkages between on-line activities, guardianship, and malware infection using a RAT framework. In this study, we examine theoretical and literature-based risk and protective factors related to malware infection. We consider the relationship between specific measures of routine computer use,

computer deviance, physical guardianship, social guardianship, and personal guardianship with malware infection. In addition to furthering our knowledge on malware infection and the role of RAT in explaining the connection between technological developments and crime, our findings contribute to recent scholarship that examines RAT as a domain-specific theory (Holtfreter al., 2008; Lynch, 1987; Mustaine & Tewksbury, 1997, 2002; Wooldredge et al., 1992).

We utilize data from a self-report survey administered to 788 college students in 10 courses offered on a southeastern university campus between August and October 2006. Five of these 10 courses allowed students from every college to enroll, thereby increasing the representative nature of the sample by including students from all colleges within the university. The sample was 57 percent female and predominantly white (77.9%). By comparison, the sample is quite similar to the larger University population (52.5% female and 75% white). Routine computer usage comprises a major part of college students' lives. As a result of the group's knowledge of computers and other electronic devices, and their risky on-line behaviors (see Hinduja, 2001; Skinner & Fream, 1997), including deviant behaviors (Higgins, 2005), a college campus can be considered a "hot spot" of both computer crime and victimization. Therefore, a college campus is an appropriate place to understand how computer routine activities and precautions affect cybercrime.

570 cases were analyzed in full regression models. The largest proportion of missing data is because of respondents not answering questions on sex and race, totaling 126 cases. Considering the emphasis placed on anonymity and the fact that the missing data respondents' malware victimization did not statistically differ from that of the data set analyzed, the most reasonable explanation for the missing data for these two measures is because they were placed on the last page of a 9-page survey instrument used for a larger project. Furthermore, comparative analyses between the missing data respondents and the 570 cases analyzed revealed no pattern and few statistical differences.[1] Thus; we did not find any evidence that the missing data influenced our findings and our overall conclusions.

Measures

Dependent Variable

Our dependent variable assessed whether respondents had lost computerized data due to malware infection (viruses, Trojan horses, or worms) in the last 12 months. We were not interested in the mere presence of malware on a computer, but whether malware caused the loss of computerized data, which is a serious and costly type of cybercrime victimization (CSI, 2007; Taylor et al., 2006). In a single item question, respondents were asked how many times over the past 12 months had they been sent a computer virus, worm, *or* Trojan horse program that destroyed their computerized data (options being never, 1-2 times, 3-5 times, 6-9 times, and 10 or more times). Over one-third (36.1%) had lost computerized data because of malware over the last year (see Table 1). Although a large percentage of respondents had been victimized by malware at least once or twice (30%), few respondents reported multiple malware victimization. Twenty-eight respondents (4.9%) reported 3-5 victimizations, while only 5 (.9%) and 2 (.4%) respondents reported 6-9 and 10 or more victimizations respectively. Due to this severely limited variation, we dichotomized this measure (0 = no victimization; 1 = victimization) and employed logistic regression to examine what activities and precautions predict whether an individual loses computerized data because of malware.

Table 1. Pearson Correlation Matrix and Descriptive Statistics (n = 570)

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	Malware vict.	--																
2	Ownership	-0.090*	--															
3	Dial-up	-0.053	0.003	--														
4	T-1	-0.110**	0.006	-0.063	--													
5	Shopping	0.021	-0.078	-0.076	-0.011	--												
6	Video games	0.000	-0.068	-0.107*	0.009	0.225**	--											
7	E-mail	0.003	-0.045	-0.068	0.022	0.284**	0.131**	--										
8	Chatrooms	0.086*	-0.177**	-0.077	-0.002	0.130**	0.191**	0.280**	--									
9	Downloading	0.057	-0.098*	-0.055	0.075	0.240**	0.255**	0.376**	0.319**	--								
10	Programming	0.073	-0.062	0.027	0.094*	0.096*	0.174**	0.163**	0.147**	0.250**	--							
11	On-line bank	-0.004	0.079	0.148**	-0.022	-0.213**	-0.060	-0.102*	-0.039	-0.082*	0.065	--						
12	Myspace	-0.055	0.126**	0.152**	0.052	-0.080	-0.019	-0.109**	-0.330**	-0.122**	-0.027	0.041	--					
13	Dev. behavior	0.136**	-0.148**	-0.088*	0.066	0.173**	0.303**	0.001	0.110**	0.359**	0.144**	-0.084*	-0.083*	--				
14	Pirating soft.	0.048	-0.103*	-0.057	0.029	0.163**	0.250**	0.024	0.067	0.253**	0.104*	-0.099*	-0.027	0.694**	--			
15	Pirating media	0.149**	-0.165**	-0.102*	0.048	0.154**	0.180**	-0.006	0.106*	0.324**	0.111**	-0.049	-0.119**	0.767**	0.439**	--		
16	Pornography	0.057	-0.042	-0.051	0.035	0.062	0.267**	-0.035	0.034	0.180**	0.076	-0.045	-0.033	0.651**	0.305**	0.295**	--	
17	Hacking	0.084*	-0.075	-0.020	0.032	0.110**	0.214**	0.057	0.081	0.243**	0.150**	-0.029	-0.054	0.571**	0.373**	0.325**	0.251**	--
18	Unauth. wire.	0.099*	-0.090*	-0.036	0.071	0.097*	0.121**	-0.002	0.081	0.199**	0.070	-0.062	-0.024	0.627**	0.305**	0.312**	0.208**	0.292**
19	Skill level	-0.007	-0.187**	-0.082*	0.078	0.178**	0.218**	0.058	0.069	0.243**	0.227**	-0.128**	-0.063	0.312**	0.292**	0.253**	0.205**	0.138**
20	Giving passwords	0.027	-0.046	0.017	0.042	-0.071	-0.030	-0.065	-0.002	-0.051	0.060	-0.038	0.018	-0.054	-0.042	-0.005	-0.097*	-0.066
21	Physical guard.	0.026	-0.001	-0.073	0.088*	0.117**	0.147**	-0.009	-0.020	0.141**	0.137**	-0.112**	-0.003	0.125**	0.160**	0.111*	0.065	-0.011
22	Anti-virus	0.030	-0.026	-0.009	-0.014	0.078	0.015	0.043	0.020	0.071	0.010	-0.062	0.019	0.018	0.033	0.086*	-0.001	-0.113**
23	Spybot	0.026	-0.003	-0.111**	0.043	0.016	0.144**	-0.065	0.000	0.042	0.042	-0.007	0.004	0.099*	0.125**	0.066	0.056	0.028
24	Ad-aware	0.082	-0.029	-0.099*	-0.020	0.063	0.128**	0.010	0.010	0.110**	0.055	-0.129**	-0.005	0.135**	0.159**	0.084*	0.094*	0.061
25	Microsoft Upd.	0.019	-0.047	-0.070	0.053	0.092*	0.012	0.025	0.005	0.087*	0.106*	-0.102*	-0.024	0.060	0.060	0.056	0.068	-0.040
26	Security center	-0.034	0.084*	0.128**	-0.028	0.038	0.007	-0.058	0.036	0.064	0.061	0.036	-0.035	0.005	0.033	-0.008	-0.017	0.014
27	Software firewall	-0.012	0.021	-0.024	0.133**	0.025	0.064	-0.039	-0.072	0.051	0.088*	-0.057	0.019	0.025	0.051	0.060	-0.024	-0.026
28	Hardware firewall	-0.023	0.012	-0.021	0.103*	0.104*	0.122**	0.048	-0.046	0.074	0.104*	-0.049	0.009	0.078	0.084*	0.045	0.034	0.013
29	Social guard.	0.153**	-0.169**	-0.135**	0.042	0.114**	0.180**	-0.018	0.151**	0.256**	0.055	-0.086*	-0.188**	0.653**	0.438**	0.557**	0.458**	0.357**
30	Fr. pirate soft.	0.069	-0.149**	-0.090*	0.067	0.118**	0.136**	-0.030	0.113**	0.164**	0.037	-0.100*	-0.084*	0.504**	0.528**	0.369**	0.285**	0.272**
31	Fr. pirate media	0.120**	-0.178**	-0.127**	0.040	0.105*	0.085*	0.003	0.129**	0.227**	0.014	-0.088*	-0.230**	0.510**	0.278**	0.659**	0.205**	0.192**
32	Fr. pornography	0.152**	-0.102*	-0.096*	0.011	0.069	0.184**	-0.038	0.090*	0.199**	0.034	-0.062	-0.105*	0.523**	0.264**	0.310**	0.614**	0.206**
33	Fr. hacking	0.113**	-0.043	-0.080	-0.002	0.030	0.144**	0.023	0.127**	0.159**	0.116**	0.029	-0.131**	0.380**	0.242**	0.237**	0.213**	0.527**
34	Female	0.055	0.057	0.047	-0.049	0.010	-0.261**	0.161**	0.086*	-0.070	-0.005	-0.083*	-0.119**	-0.346**	-0.256**	-0.171**	-0.469**	-0.058
35	Employment	0.102*	0.035	0.014	-0.064	0.082	-0.017	-0.002	-0.112**	-0.029	-0.012	-0.133**	0.013	0.063	0.073	0.048	0.018	0.027
	Mean	0.361	0.139	0.049	0.072	1.265	0.791	2.778	1.916	2.119	0.372	0.279	0.153	0.509	0.335	1.039	0.553	0.187
	Std. Dev.	0.481	0.346	0.216	0.259	1.107	1.232	1.283	1.758	1.376	0.774	0.449	0.360	0.596	0.763	1.201	1.040	0.502

Table 1. Continued

		18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
18	Unauth. wire.	--																	
19	Skill level	0.133**	--																
20	Giving passwords	0.012	-0.037	--															
21	Physical guard.	0.062	0.218**	-0.024	--														
22	Anti-virus	-0.019	0.070	0.002	0.390**	--													
23	Spybot	0.055	0.091*	0.008	0.539**	0.078	--												
24	Ad-aware	0.057	0.168**	-0.005	0.487**	0.054	0.275**	--											
25	Microsoft Upd.	0.018	0.206**	-0.030	0.591**	0.176**	0.133**	0.130**	--										
26	Security center	0.010	0.007	-0.036	0.327**	0.027	0.078	-0.025	0.117**	--									
27	Soft. firewall	0.001	0.125**	-0.007	0.589**	0.118**	0.162**	0.136**	0.259**	0.023	--								
28	Hard. firewall	0.080	0.068	-0.020	0.557**	0.126**	0.127**	0.047	0.189**	0.156**	0.236**	--							
29	Social guard.	0.319**	0.214**	-0.059	0.059	0.011	0.041	0.126**	0.017	-0.049	0.017	0.020	--						
30	Fr. pirate soft.	0.248**	0.190**	-0.079	0.059	-0.012	0.067	0.120**	0.021	-0.015	-0.019	0.028	0.763**	--					
31	Fr. pirate media	0.229**	0.152**	-0.018	0.025	0.075	-0.007	0.074	0.005	-0.058	0.031	-0.032	0.801**	0.526**	--				
32	Fr. pornography	0.269**	0.198**	-0.028	0.051	0.011	0.042	0.092*	0.035	-0.074	-0.005	0.051	0.758**	0.367**	0.400**	--			
33	Fr. hacking	0.196**	0.067	-0.070	0.044	-0.093*	0.026	0.102*	-0.025	0.038	0.060	0.018	0.634**	0.381**	0.330**	0.432**	--		
34	Female	-0.126**	-0.249**	0.067	-0.090*	0.038	-0.153**	-0.157**	-0.010	0.040	0.009	-0.046	-0.315**	-0.253**	-0.126**	-0.410**	-0.110**	--	
35	Employment	0.048	0.068	0.005	0.066	0.032	0.058	0.047	0.004	0.047	-0.007	0.060	0.071	0.048	0.028	0.081	0.060	0.022	--
	Mean	0.430	0.670	0.907	3.183	0.870	0.295	0.351	0.614	0.132	0.518	0.404	0.907	0.756	1.447	1.056	0.370	0.575	0.821
	Std. Dev.	0.899	0.569	0.291	1.576	0.336	0.456	0.478	0.487	0.338	0.500	0.491	0.694	0.914	1.124	1.069	0.579	0.495	0.604

Notes: * $p < .05$ (Two-tailed)
** $p < .01$

Routine Activities

Following past RAT research which focused on domain-specific models, we incorporated direct and proxy measures of online routine activities to understand how the respondents utilize computer technology for work/school and personal needs. Respondents were asked who owned the computer (*ownership)* that they used most often (0 = you or your family; 1 = other, including friends, school, and employer) and to indicate the Internet connection speed of this computer. Two dummy variables (*Dial-up* and *T-1)* were included in the models with DSL/Cable modem being the comparison group. We treat connectivity as a lifestyle measure due to the demographic trends in the type of Internet connection used. Individuals living in rural rather than urban environments are more likely to use dial-up internet connections due to lack of high speed service (Pew Internet, 2009). African-Americans and those making less than $20,000 per year are also more likely to have dial-up connections, due to the higher cost of broadband connectivity (Pew Internet, 2009). Thus, individuals who desire faster connections are willing to pay for this privilege. In fact, despite the recent economic downturn, the number of broadband users has increased as individuals eliminated other services, such as cellular telephone connections, to maintain their high speed connection (Pew Internet, 2009).

We directly assessed the amount of time respondents spent on specific computer activities by asking the respondents how much time they spent on the computer each week, on an average, over the past 6 months for each of the following activities:

1) Shopping/going to auction sites *(shopping)*,
2) Playing video games (*video games)*,
3) Checking e-mail *(e-mail)*,
4) Using either chatrooms, IRC, or Instant Messaging (IM) *(chat rooms)*,
5) Downloading and uploading files *(downloading files)*, and
6) Programming *(programming)*.

The options were:

1) Never,
2) Less than 1 hour,
3) 1-2 hours,
4) 3-5 hours,
5) 6-9 hours, and
6) 10 or more hours.[2]

In addition, the use of on-line banking systems *(on-line bank)* and popular social networking websites *(Myspace)* were measured with the following questions, "I generally avoid using on-line banking systems," and, "I generally avoid using websites like Facebook, Myspace, and classmates.com" (0 = no; 1 = yes). Note that a positive response means that they do not use on-line banking or these websites.

Deviant Behavior

In order to examine the relationship between deviant computer activities and data loss due to malware infection, respondents were asked how many times (options being never, 1-2, 3-5, and 6 or more times) they used a computer in the past 12 months to:

1) Knowingly use, make, or give to another person a "pirated" copy of commercially-sold computer software;

2) Knowingly use, make, or give to another person "pirated" media (music, television show, or move);

3) Look at pornographic or obscene materials;

4) Guess another's password to get into his/her computer account or files;

5) Access another's computer account or files without his/her knowledge or permission to look at information or files;

6) Add, delete, change, or print any information in another's computer files without the owner's knowledge or permission; and

7) Use someone else's wireless Internet connection without their authorization to surf the Web or otherwise access on-line content (Rogers, 2001; Skinner & Fream, 1997).[3]

To create our *deviant behavior* measure, we first averaged items 4 – 6 to create a reliable *hacking* scale (alpha = .859) that ranged from 0 through 3. Averaging these three items allowed the other deviance measures to have the same influence in the *deviant behavior* measure, rather than having three of the seven items included in the scale be hacking related. Responses for the five items were then averaged, creating a reliable measure (alpha = .752) ranging from 0 to 3 (mean = .509; SD = .596).[4]

Guardianship

We included guardianship measures that could be categorized as: personal, physical, and social. Respondents were asked to assess their skill level with computers and technology *(skill level)* to serve as a proxy measure of their ability to protect their computers and themselves while interacting or performing various activities online. This assessment was based on a three-point ordinal scale adapted from Rogers (2001):

0) "I can surf the 'net, use common software, but not fix my own computer" (normal);

1) "I can use a variety of software and fix some computer problems I have" (intermediate); and

2) "I can use Linux, most software, and fix most computer problems I have" (advanced).

The modal category (56.8%) was intermediate with an additional 38.1 percent self-assessing their skills as normal and only 5.1 percent indicating advanced skills.[5] To further assess personal guardianship, we also asked the respondents whether or not (0 = no; 1 = yes) they protect their passwords and other sensitive information ("I avoid giving out my passwords for e-mail accounts or other sensitive information").

We assessed physical guardianship by asking respondents whether or not (0 = no; 1 = yes) the computer they use most often has updated anti-virus (*Anti-virus)*, spybot *(Spybot software)*, and ad-aware software *(Ad-aware software)*. Additionally, we asked whether they go to or use Microsoft Update (*Microsoft Update)* or AOL or ISP provided Security Centers *(Security Center)*. Finally, they were asked whether or not the computer they use most often has software *(software firewall)* and/or hardware firewalls *(hardware firewalls)*. *Physical guardianship* was measured by adding these seven items together and creating an additive scale.

Although our physical guardianship scale has low reliability (alpha=.512), we operationalize this measure as an additive scale because we hypothesize there will be a cumulative effect, meaning that the more types of physical guardianship a person obtains and updates, the less likely he/she is to have data lost due to malware (see Holtfreter et al., 2008 for similar argument regarding additive scales). We also examine the independent effects of the seven items on malware victimization as a precaution that physical guardianship cannot be operationalized as an additive scale.

It is important to note that our assessment of physical guardianship may not accurately reflect the use of these programs by the respondents. Choi (2008) notes that respondents may not understand the definition or utility of protective software programs, thus any attempt to explore their use must be carefully developed by researchers. As we did not provide definitions for each type of program in the survey, we are careful to moderate our discussion of these variables in the findings of this study.

Social guardianship was assessed by asking the respondents how many of their friends had pirated software (*fr. pirate software)* or media *(fr. pirate media)*, viewed pornographic or obscene material *(fr. pornography)*, and hacked *(fr. hacking)* during the past 12 months.

0 = none of them;
1 = very few of them;
2 = about half of them;
3 = more than half of them.[6]

Similar to the measure assessing the respondents' involvement in hacking *(hacking)*, the friends' computer hacking scale (alpha = .882) was also created by averaging the respondents' answers to how many of their friends guess passwords, access computer accounts or files without permission, and add, delete, change, or print information without permission. The *social guardianship* measure was then created by averaging the scores for the four items (pirate software, pirate media, pornography, and hacking) (alpha = .732).

Finally, we statistically control for *sex* (0 = male; 1 = female) and *employment status* (0= unemployment; 1= part-time/temp; 2= full time).[7]

Results and Discussion

The correlation matrix, presented in Table 1, illustrates that most routine activities on the computer, as well as personal and physical guardianship, are not correlated with data loss from malware victimization.[8] However, the hypothesized relationships between both deviant computer behavior (r = 0.136) and lack of social guardianship (r = 0.153) with malware victimization, are supported. Although pirating software and viewing on-line pornography are not correlated with malware victimization, pirating media (r = 0.149), hacking (r = 0.084), and unauthorized access to the Internet (r = 0.099) are also statistically correlated, albeit weakly, with malware victimization. Furthermore, *friends pirate software* is the only item from the *social guardianship* measure *not* correlated with data loss from malware victimization. Although the matrix does not indicate strong relationships between legitimate computer activities and malware victimization, these univariate analyses provide enough evidence to further explore our hypotheses via multivariate analyses.

We estimated logistic regression models with data loss caused by malware victimization as the dependent variable (see Schreck, 1999; Holtfreter et al., 2008).[9] Logistic regression is an appropriate technique for these analyses as our dependent variable

is dichotomous and skewed. For our main analyses, we ran two models (see Table 2). Model A contains the items as described in the measurement section, meaning that the components of RAT are represented as constructs. In model B, we do not use the general constructs but use the specific items that comprised the scales. Researchers have traditionally used RAT as a framework to understand how *specific* behaviors and conditions are related to victimization, rather than creating scales of the concepts themselves. This traditional approach does not directly test the theory, but has the benefit of identifying how specific behaviors are related to victimization, leading to clearer policy implications (Mustaine & Tewksbury, 1998). Thus, our two-model strategy allows us to examine the utility of using RAT as a framework to understand malware victimization (Model A) as well as understanding how specific activities and precautions affect one's likelihood of victimization (Model B).[10]

Table 2. Logistic Regression Predicting Data Loss from Malware Infection

	Full Model A			Full Model B			Male	Female
	(n = 570)			(n = 570)			(n = 242)	(n = 328)
	B	Std Error	Exp (B)	b	Std Error	Exp (B)	Exp (B)	Exp (B)
Routine Activities								
Ownership	-.480	.295	.619	-.435	.298	.647	.901	.564
Dial-up	-.622	.471	.537	-.527	.485	.590	1.381	.411
T-1	-1.221**	.446	.295	-1.161**	.453	.313	.464	.220*
Shopping	-.023	.091	.977	-.020	.093	.981	1.073	.926
Video games	-.072	.085	.930	-.059	.087	.943	.904	1.149
E-mail	-.049	.084	.952	-.049	.086	.952	.823	1.023
Chatrooms	.078	.060	1.081	.078	.061	1.081	.888	1.175*
Downloading files	.000	.082	1.000	-.019	.084	.981	1.257	.823
Programming	.212	.126	1.236	.228	.130	1.256	1.607*	1.046
On-line bank	.163	.217	1.177	.191	.222	1.211	.930	1.454
Myspace	.123	.289	1.130	.093	.298	1.097	.771	1.315
Dev. Behavior	.384	.218	1.468	--	--	--	--	--
Pirating software	--	--	--	-.079	.162	.924	.772	.893
Pirating media	--	--	--	.240*	.116	1.271	1.492*	1.238
Pornography	--	--	--	-.042	.126	.959	.977	.477*
Hacking	--	--	--	.063	.242	1.065	1.761	.621
Unauth. Wireless	--	--	--	.109	.110	1.115	1.084	1.200
Personal Guardianship								
Skill level	-.237	.185	.789	-.264	.190	.768	.610	.972
Giving passwords	.179	.322	1.196	.098	.330	1.103	.896	1.252
Physical Guardianship	.046	.061	1.047	--	--	--	--	--
Anti-virus	--	--	--	.131	.293	1.140	1.631	.792
Spybot software	--	--	--	.056	.217	1.057	.787	1.349
Ad-aware software	--	--	--	.378	.206	1.459	1.317	1.693
Microsoft Update	--	--	--	.082	.208	1.085	1.543	.946
Security Center	--	--	--	-.187	.294	.829	.821	.835
Software firewall	--	--	--	-.009	.201	.991	.718	1.201
Hardware firewall	--	--	--	-.128	.203	.880	.831	.792
Social Guardianship	.358*	.178	1.430	--	--	--	--	--
Fr. Pirate software	--	--	--	.007	.141	1.007	1.168	.924
Fr. Pirate media	--	--	--	-.061	.132	.941	.794	1.020

Fr. Pornography	--	--	--	.363★★	.133	1.438	1.548★	1.584★
Fr. Hacking	--	--	--	.004	.214	1.004	.713	1.483
Demographics								
Female	.495★	.221	1.641	.602★	.248	1.827	--	--
Employment	.359★	.157	1.431	.350★	.160	1.418	2.033★★	1.265
Constant	-1.760★★	.524	.172	-1.865★★	.568	.155	-2.029★	.280
Pseudo R^2	.111			.138			.257	.192

Note: $p \leq .05$ *, $p \leq .01$**. Full model A: Chi-square = 48.215***; -2LL = 697.597. Full model B: Chi-Square = 60.456***; -2LL = 685.357. Male model: Chi-square = 49.365; -2LL = 257.776. Female model: Chi-square = 49.954; -2LL = 386.980. Shaded cells illustrate significant difference ($z \geq 1.96$) between partitioned model

These regression models indicate that neither computer ownership nor legitimate computer-related activities, such as chat rooms and email, appear to have an influence on the risk of data loss caused by malware infection. The only routine activity measure that is statistically related to data loss from malware infection is having T-1 internet connection speed. The coefficient sign is negative, meaning that individuals who have faster and more efficient access to the Internet are less likely to get viruses, worms, and Trojans than individuals with DSL/Cable connection. While we originally conceived of connectivity as a lifestyle factor, because of the demographic correlates of connectivity and being able to access websites faster, the observed relationship between connectivity and the likelihood of malware infection may be a result of protective factors related to one's Internet connection. High speed users, particularly on T1 connections, are more likely to use the University as their Internet Service Provider (see Hinduja, 2001). Large institutions are more likely to have significant filtering and firewalls in place to protect users than those at home on dial-up or dsl modems. This insularity may play a role in reducing the risk of infection. Additionally, dial-up users are more likely to be impacted by unique forms of malicious software designed to subvert the modem that connects the computer to the Internet (Nazario, 2003). There is, however, a need for future research to explore and disentangle the operationalization of connectivity as either a guardianship or lifestyle measure.[11]

Spending time performing illegitimate computer activities was also not a strong predictor of malware infection. The only form of personal deviance that increased the risk of malware infection was pirating media. Such behavior is particularly prevalent among college students and younger people who regularly use computers (Gopal et al., 2004; Higgins, 2005; Hinduja, 2001). Those who pirate media make suitable targets for malware writers as piracy requires individuals to open files for their own benefit. Motivated offenders can easily conceal their malware to appear as a music or movie file that an individual would want to download (Szor, 2005; Taylor et al., 2006). Although hacking and unauthorized use of someone else's wireless Internet connection were correlated with malware infection (see Table 1), they were not significant in the fuller model after controlling other routine computer activities. Thus, these findings illustrate the importance of including measures covering multiple forms of computer deviance in order to avoid model misspecification.

Personal and physical guardianship played small roles in explaining whether the respondent's primary computer was infected by viruses, worms, or Trojans leading to data loss. Strong computer skills and careful password management, what we termed as personal guardianship, did not reduce the threat of malware victimization. Furthermore, malware infection was not influenced by physical guardianship. This finding is contrary to

the current understanding of malware protection, considering that anti-virus software and firewalls are made to stop computer infiltration and infection by viruses, worms, and Trojans. The cross-sectional design of our study could possibly nullify a significant negative relationship between physical guardianship measures and malware infection. If respondents purchased anti-virus programs and firewalls as a preventive measure before and after victimization, physical guardianship would have a non-significant effect in a cross-sectional design. This logic, however, assumes that the theoretical negative relationship between physical guardianship and infection is so small that the relationship could be nullified by only a few victims purchasing physical guardianship after victimization.

Our models also indicate that associating with friends who view on-line pornography increases the risk of malware infection. Peers who view pornography online may increase the risk of malware infection as these programs can spread to other computers through e-mail address books or other techniques (Szor, 2005). As a consequence, their actions place all individuals in their social network at risk of victimization. At the same time, no relationships were identified between friends who pirate software, pirate media, and commit "hacker-like" behaviors and malware victimization. This is surprising given the relationship between respondents' pirating media and victimization, as well as the connection between peers who engage in piracy and individual pirating behavior (Higgins, 2005; Skinner & Fream, 1997).

Finally, some demographic correlates of malware infection were found. Individuals who were employed were at a higher risk of malware victimization, supporting the traditional literature in which employment can be a risk factor for youth as it increases exposure to deviants (Wright & Cullen, 2004). Being female increased the odds of malware victimization by 1.827 times. 38.4 percent of the females had lost data because of malware over the last 12 months, as compared with 33.1 percent of the males. Since the literature implies that computers in general are the primary targets for malware writers and not specific groups (i.e. females), we partitioned the model by sex and ran equality of coefficient tests (see Paternoster et al., 1998) to examine whether routine activities and guardianship factors influence male and female victimization differently (see Table 2). These additional tests found no differences regarding the effects of guardianship on malware victimization. The only factor that was significant in at least one of the two models and statistically different in comparison to the other model was the number of hours the respondent spent using chat rooms, IRC, or Instant Messaging. For every one unit increase in the chat room measure, the odds of female malware victimization increased by 1.175 times. This finding supports previous research that finds females who use computer-mediated communications face a greater risk of on-line harassment and cyberstalking relative to males (Bocij, 2004; Finn, 2004; Holt & Bossler, 2009). In fact, malware has been used by harassers to install backdoor programs and do serious harm to their intended target's computer (see Bocij, 2004; Finn, 2004). Thus, malware, or at least the use of it, might not be as indiscriminate as it appears.

Conclusions and Policy Implications

In the original presentation of RAT, Cohen and Felson (1979) wrote that "it is ironic that the very factors which increase the opportunity to enjoy the benefits of life also may increase the opportunity for predatory violations" (p. 605). Over the last 20 years, the rise of the personal computer and Internet has provided enormous advantages to our society.

At the same time, it has also provided more opportunities for motivated offenders to victimize individuals in brand new ways. RAT has historically been fruitful in providing a useful framework to understand how technological shifts affect a wide variety of criminal offenses. Criminologists, however, have been slow to examine how computer routine activities and guardianship affect cybercrime. We addressed this gap by conducting an exploratory analysis of RAT to account for a computer-focused crime, malware infection.

Our findings provide partial support for the application of RAT to data loss from malicious software. Spending more time on computer activities theoretically related to malware infection, such as on-line shopping, e-mailing, and chat rooms, did not increase the odds of victimization. At the same time, individuals who engage in media piracy were at an increased risk of victimization. In addition, those whose peers viewed pornography in cyberspace were at a significant risk of malware infection. The behavior of oneself and one's peers increases the risk of victimization largely because of the ways that malware spreads across systems. These are excellent vectors for a motivated offender to distribute malicious code since media and pornographic files are attractive packages that many individuals would want to open (Furnell, 2002; Szor, 2005; Taylor et al., 2006). Thus, the findings suggest that the relationship between crime and victimization in the real world may be replicated in on-line environments.

Computer software that has been created specifically to decrease malware victimization had no significant impact for this sample. Our findings support recent studies on malicious software that highlights the difficulty of security measures to prevent malware infection (see PandaLabs, 2007). Almost 25 percent of personal computers around the world that use a variety of security solutions have malware loaded into their memory, compared with 33.28 percent of unprotected systems (PandaLabs, 2007). In addition, we did not find that different forms of personal guardianship decreased victimization. These results may, however, be a consequence of our assessment of protective software. Choi (2008) recommends careful measurement and elaboration of security software concepts to respondents in order to properly address their use. As we did not use such information in the course of this study, it is possible that the findings of this analysis are measurement-related. Thus, future researchers should explicitly define and clearly assess the influence of protective software on the risk of malware victimization (see also Choi, 2008).

These findings are quite similar to other RAT studies utilizing college samples in which guardianship measures were primarily not significant (Mustaine & Tewksbury, 1998; Schwartz et al., 2001). These studies argued that taking safety precautions was not effective when the victimization experienced was caused by friends and not strangers. Physical guardianship measures will not be as effective in decreasing malware infection since physical guardianship tools are most useful for addressing victimization caused by strangers rather than friends. Thus, these findings do not support target hardening as the strongest protection tool to decrease the probability of data loss from malware in a college sample. Instead, individuals must be aware of the possible consequences of their behavior and that of their peers and attempt to change their behavior. This is easier said than done considering that past research has illustrated the difficulty of individuals changing their behavior even when they understand the risks involved (Reisig, Pratt, & Holtfreter, 2009).

The above findings strongly support the role that criminology can play in developing a framework to understand and prevent malware infection. Malware infection will not be decreased substantially through a single approach based solely on criminology or information technology. Both physical target hardening through security solutions and

behavioral changes based on RAT will have a role in future programs and policies meant to decrease the damage caused by malware. The continued examination of the behavioral correlates of malware infection using a RAT framework is vital.

A key policy implication from this study is the need for greater awareness of the connection between computer deviance and malware victimization. The significant concentration of media piracy among young people, coupled with the increasing sophistication and efficacy of malware, suggests that this population is extremely susceptible to victimization. Most media campaigns against piracy focus on the significant financial harms caused by this crime (Higgins, 2005). These programs may, however, have little impact as piracy is largely perceived to have little effect on the artists and greater benefits for the individual (see Gopal et al., 2004; Higgins, 2005; Hinduja, 2001). Instead, anti-piracy campaigns need to focus on the risk to individuals and their peers who download media illegally. Considering the significant volume of piracy that occurs in dorms on college campuses (see Higgins, 2005; Hinduja, 2001), educating students and computer security personnel on the risks of piracy may be an important preventative tool to decrease the risk of computer crime victimization on college campuses.

A further practical implication may be to expand the regulatory power of system administrators to withhold service. Currently, system administrators can cut Internet connectivity to computer systems that are suspected of malicious activity or violations of terms of service. Those who utilize large amounts of bandwidth for piracy purposes may also be tied to the spread of malicious software across networks. Thus, regular monitoring of Internet use for potential piracy, and selective removal of those users, may help to minimize the occurrence of infection. Though such a measure may be helpful, it would require great technical resources for administrators as Internet Service Providers have very large customer populations. Improving the automated monitoring protocols that can detect and remove anomalous traffic may be a key to help combat the problem of malicious software.

Although this exploratory study increases our knowledge of cybercrime, further study is needed to elaborate and expand on the issue of malicious software infection. Specifically, we used a convenient sample of college students from a single university, populated primarily by individuals from the same state. Though college samples have been utilized extensively for criminological theory testing (see Payne & Chappell, 2008 for review of the use of college samples in criminological research), the representative nature of this study is limited. The characteristics of how malware spreads would indicate that our findings would be generalizable to other universities around the country. In addition, we assessed whether the respondents had experienced a severe form of malware victimization by asking whether they had lost computerized data. This method does not capture information on malware that caused other forms of victimization, such as identity theft, or malware that is present, but benign. Future research should utilize more direct and specific measures of malware infection to triangulate the reality of malware on a system, such as diminished functionality and identification by antivirus programming (see Choi, 2008; PandaLabs, 2007). Measures must also be employed to identify the time at which antivirus and other protective software were placed on a computer system. Finally, our study only explored the applicability of routine activities theory to malware infection and did not examine the influences of concepts from other theories, such as self-control or rational choice theories. Clearly the participation in risky computer activities is an indicator of low self-control as well as behavior that places individuals in closer proximity

to motivated offenders. Such explorations will improve our understanding of cybercrime victimization and the applicability of traditional theories of crime to account for victimization in virtual environments.

Endnotes

1. The missing data respondents were as likely to be victimized by malware over the last 12 months. Additionally, no pattern emerges that clearly separates the missing data respondents from the cases analyzed regarding their computer routines. The missing data respondents spent more time on the computer for work or school (x = 1.79) and on social networking websites (x = .22), but less time in chatrooms (x = 1.50). Additionally, they were less likely to have a hardware firewall (x = .32) and none of them were non-African-American minority students.
2. In order to examine whether spending time on the computer in general affects malware victimization, we also measured the number of hours per week spent on the computer for work or school and also outside of work or school. The options were: less than 5 hours, 5-10 hours, 11-15 hours, 16-20 hours, and 21 or more hours. These two measures tap into two distinct aspects of how computer usage is integrated into the participants' daily lives as indicated by a significant but low correlation between the two measures (Spearman = .255). These two measures were not statistically significant in any regression model.
3. The survey's options actually separate the "6 or more" category into 6-9 times and 10 or more times. The last two categories were collapsed because of limited responses in this largest category.
4. The data set does not contain a question assessing whether the respondents have knowingly created or distributed malware with the intent to cause computer damage. Although we expect that the number of respondents who engaged in this behavior within the last year is minimal or non-existent (see Rogers, 2001), we cannot directly assess the link between malware creation/distribution and malware infection with this data set. As the literature review illustrated, however, the deviant computer behaviors measured for this study can place an individual at risk for victimization as criminals may place malware within software, media, and pornographic websites. Additionally, engaging in hacking activities increases the risk of victimization from other hackers.
5. It should be noted that our *skill level* measure acts as a proxy measure for personal guardianship, but it could also be interpreted as a computer usage measure and therefore be considered a proxy for routine computer activity. We consider *skill level* to be a guardianship measure because we have controlled for various computer-related routine activities as discussed above. Any possible effect that skill level has on victimization would mostly be reduced to guardianship influences. The survey did provide a fourth option for this question: "I am afraid of computers and don't use them unless I absolutely have to." Only one student in the original data set and no student in the 570 cases analyzed indicated their skill level as remedial, indicating that this sample is computer literate.
6. The original survey question also contained the option "all of them." Only a small number of respondents reported all of their friends' pirated software or hacked computers. Thus, we combined the option "all of them" with "more than half." We also ran the models with the non-recategorized items and the models were substantively similar to the results presented in Table 2.
7. We also examined race and age as these demographics have been related to traditional victimization. For race, respondents could identify themselves as white, African-American, Hispanic, Asian or another racial/ethnic group. Hispanics, Asians, and other racial/ethnic group only comprise 2.8%, 5.3%, and 3.2% respectively of the cases analyzed. We ran full models with dummy variables for each group, but no racial group was significantly related to malware infection. *Age* was a four-point ordinal scale (0 = 19; 1 = 20-21; 2 = 22-25; 3 = 26 and up) and it was not statistically related to malware victimization in our models as well. Thus, we excluded these two demographics from our full models presented in Table 2 to simplify the models.
8. We provide a full correlation matrix, including all of our measures for models A and B, because of the exploratory nature of our study and to provide the reader and future researchers as much information as possible regarding the correlates of malware victimization.
9. The correlation matrix illustrates some moderately strong correlations between some of the independent variables [for example, *deviant behavior* and *social guardianship* (r = 0.653) and *pirating media* and *friends pirating media* (r = 0.659)]. Multicollinearity, however, was not an issue for the models. No VIF was over 10 and no tolerance level fell below .2. In Model A, *deviant behavior*

(tolerance of .478 and VIF of 2.091) and *social guardianship* (tolerance of .525 and VIF of 1.906) met acceptable standards. In Model B, *pirating media* (tolerance of .384 and VIF of 2.606) and *friends pirating media* (tolerance of .421 and VIF of 2.374) were acceptable as well. Additionally, including measures for both downloading files and media piracy did not cause problems. Models ran without the downloading files measure produced substantively similar results to the findings presented in Table 2.

10. Some readers might be concerned that our Full Model B, male model, and female model do not have enough cases for the number of measures included and that Type II error is present. In other words, would some of the non-significant results be significant if we had either more cases or fewer independent variables? There are no accepted rules for the number of cases needed per independent variable in logistic regression (i.e. 30 cases per measure). Instead, the issue is whether the results are stable depending on the number of variables included in the models. We illustrate the stability of our models two different ways. First, we provide a full correlation matrix (see Table 1) that illustrates that many of the measures were not significantly correlated with malware victimization even at the zero-order level. Thus, even when only one independent variable is being examined, most of the measures are not significantly related. Second, and most importantly, we conducted further analyses not reported in the text. Following past traditional routine activities research, we ran full and reduced models to examine the stability of the models. Similar to the work of Mustaine and Tewksbury (1998; 2002), we included all of our measures into the regression model. All measures that were not significant at $p < .205$ were excluded and the models were rerun. Specifically, we were examining whether measures that were not previously significant would be significant when fewer measures were in the models. In addition, we also ran models that only contained the measures that pertained to each construct (i.e. guardianship). The findings did not substantively differ in any of the extra models. Thus, the findings presented in Table 2, and our conclusions based off these models, are not affected by the number of measures included in our models.
11. We had argued that Internet connectivity is a lifestyle measure because individuals with faster connections can access websites more effectively and efficiently. In addition, previous research has found that Internet connectivity is related to socioeconomic factors such as race, income, and whether individuals live in rural areas (Pew Internet, 2009). Because we found that connectivity is related to malware victimization, this would suggest that connectivity could mediate the effects of socioeconomic factors on malware victimization. This does not appear to be the case, however, with our data set. Although T-1 connectivity is significantly correlated with malware victimization ($r = -.110$), race, sex, and age are not related to our connectivity or victimization measures. Employment status is correlated with victimization ($r = .102$), but is not related to connectivity. Individuals with more computers skills are less likely to have dial-up ($r = -.082$), but skill level is not related to malware victimization. In addition, when all of the measures discussed above, with the exception of the connectivity measures, are included in a logistic regression model with malware victimization as the dependent variable, only employment status is significant [Exp (B) 1.432]. When both connectivity measures are included in the model, the effects of employment status does not change substantively [Exp (B) 1.405]. Thus, these zero-order correlations and regression models do not indicate that connectivity mediates any possible effects of demographics on malware victimization. At the same time, our findings could be limited to that of a college sample. Of the 570 students, only 28 (4.9%) had dial-up and 41 (7.2%) had T-1. Thus, a more representative sample of the U.S. population could find that Internet connectivity does mediate the effects of demographics on malware victimization since there would be more variation in the connectivity measure. Clearly, this is an important issue for future research to investigate.

References

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

Choi, K. C. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308–333. Retrieved September 1, 2009 from http://cyber.kic.re.kr/data/Kyungchoiijccjan2008.pdf

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

Computer Security Institute (2007). *Computer crime and security survey*. Retrieved June 3, 2007, from http://www.cybercrime.gov/FBI2006.pdf.

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

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

Felson, M. (2001). *Crime and everyday life*, Third Edition. Thousand Oaks, CA: Sage.

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, MA: Addison-Wesley.

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

Grabosky, P. (2001).Virtual criminality: Old wine in new bottles? *Social and Legal Studies, 10*, 243-249.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.) *Crime and the internet*. London: Routledge.

Higgins, G. E. (2005) Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*, 1-24.

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

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

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.

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

Joseph, J. (2003). Cyberstalking: An international perspective. In Y. Jewkes (Ed.) *Dot.cons: Crime, deviance, and identity on the internet*. Cullompton: Willan Press.

Kapersky, E. V. (2003). *The classification of computer viruses*. Metropolitan Network BBS Inc., Bern, Switzerland. Retrieved June 4, 2005 from http://www.avp.ch/avpve/classes/classes.stm

Lynch, J. (1987). Routine activity and victimization at work. *Journal of Quantitative Criminology, 3,* 283-300.

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to malware incident prevention and handling: Recommendations of the National Institute of Standards and Technology*. Washington DC: National Institute of Standards and Technology.

Miethe, T., & McDowall, D. (1993). Contextual effects in models of criminal victimization. *Social Forces*, 71, 741-760.

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

Mustaine, E. E., & Tewksbury, R. (1997). The risk of victimization in the workplace for men and women: An analysis using routine activities/lifestyle theory. *Humanity & Society, 21*, 17-38.

_____ (1998). Predicting risk of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology, 36,* 829-857.

_____ (2002). Sexual assault of college women: A feminist interpretation of a routine activities analysis. *Criminal Justice Review, 27,* 89-123.

Nazario, J. (2003). *Defense and detection strategies against Internet worms.* Artech House.

Newman, G., & Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime.* Cullompton: Willan Press.

Osborn, D. R. & Tseloni, A. (1998). The distribution of household property crimes. *Journal of Quantitative Criminology*, 14, 307-330.

PandaLabs (2007). Malware infections in protected systems. Retrieved November 1, 2007 from http://research.pandasecurity.com/blogs/images/wp_pb_malware_infections_in_protected_systems.pdf

Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology, 36,* 859-866.

Payne, B. K., & Chappell, A. (2008). Using student samples in criminological research. *Journal of Criminal Justice Education, 19,* 175-192.

Pew Internet. (2009). Pew Internet and American Life Project. Retrieved September 1, 2009 from http://www.pewinternet.org/Reports/2009/10-Home-Broadband Adoption-2009.aspx

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

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.

Sampson, R., & Wooldredge, J. (1987). Linking the micro- and macro-dimension of lifestyle routine activity and opportunity models of predatory victimization. *Journal of Quantitative Criminology, 3,* 371-393.

Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly, 16*, 633-654.

Schwartz, M. D., DeKeseredy, W. S., Tait, D., & Alvi, S. (2001). Male peer support and a feminist routine activities theory: Understanding sexual assault on the college campus. *Justice Quarterly, 18*, 623-649.

Shover, N. (1996). *The great pretenders: Pursuits and careers of persistent thieves.* Boulder, CO: Westview Press.

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, 4*95-518.

Spano, R., & Nagy, S. (2005). Social guardianship and social isolation: An application and extension of lifestyle/routine activities theory to rural adolescents. *Rural Sociology, 70*, 414-437.

Stewart, E. A., Elifson, K. W., & Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly, 21*, 159-181.

Symantec Corporation (2003). Symantec Internet security threat report. Retrieved October 3, 2005 from http://enterprisesecurity.symantec.com/content/knowledgelibrary.cfm?EID=0

Szor, P. (2005). *The art of computer virus research and defense.* Upper Saddle River, NJ: Addison Wesley.

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). *Digital crime and digital terrorism*. Upper Saddle River, NJ: Pearson Prentice Hall.

Tewksbury, R. & Mustaine, E. (2000). Routine activities and vandalism: A theoretical and empirical study. *Journal of Crime & Justice, 23*, 81-110.

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

Wall, D. S. (2001). Cybercrimes and the Internet. In D.S. Wall (Ed.) *Crime and the Internet*. New York: Routledge.

Wright, J. P., & Cullen, F. C. (2004). Employment, peers, and life-course transitions. *Justice Quarterly*, *1,* 183–205.

Wright, R., & Decker, S. H. (1994). *Burglars on the job: Street life and residential break-ins*. Boston, MA: Northeastern University Press.

Wooldredge, J., Cullen, F., & Latessa, E. (1992). Victimization in the workplace: A test of routine activities theory. *Justice Quarterly, 9,* 325-335.

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology, 2*, 407-427.

Ybarra, M. L., Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. *Archives of Pediatrics & Adolescent Medicine, 161*, 138-145.

Zhang, L., Welte, J. W., & Wiecxorek, W. F. (2001). Deviant lifestyle and crime victimization. *Journal of Criminal Justice, 29,* 133-143.