Computer Crime Victimization and Integrated Theory: An Empirical Assessment

Kyung-shick Choi[1]
Bridgewater State College, USA

Abstract

This study empirically assessed a computer-crime victimization model by applying Routine Activities Theory. Routine Activities Theory is arguably, as presented in detail in the main body of this study, merely an expansion of Hindelang, Gottfredson, and Garofalo's lifestyle-exposure theory. A self-report survey, which contained multiple measures of computer security, online lifestyles, and computer-crime victimization, was administered to 204 college students to gather data to test the model. Utilizing structural equation modeling facilitated the assessment of the new theoretical model by conveying an overall picture of the relationship among the causal factors in the proposed model. The findings from this study provided empirical supports for the components of Routine Activities Theory by delineating patterns of computer-crime victimization.

Keywords: Routine Activities Theory; Lifestyle exposure theory; Computer crime victimization;

Introduction

Cyber crime has the potential to affect everyone's daily activities. Society depends heavily on computer technology for almost everything in life. Computer technology use ranges from individual consumer sales to processing billions of dollars in the banking and financial industries. The rapid development of technology is also increasing dependency on computer systems. Today, computer criminals are using this increased dependency as a significant opportunity to engage in illicit or delinquent behaviors.

It is almost impossible to have precise statistics on the number of computer crime and the monetary loss to victims because computer crimes are rarely detected by victims or reported to authorities (Standler 2002). In addition, policing in cyberspace is very scarce (Britz 2004). Moreover, the sophistication of computer criminal acts, by the criminals utilizing anonymous re-mailers, encryption devices, and accessing third-party systems to commit an offense for the original target, makes it difficult for law enforcement agencies to apprehend and prosecute the offenders (Furnell 2002; Grabosky & Smith 2001; Yar 2005). This could, arguably, become a real threat to our lives. However, the general population has not yet fully recognized the overall impact of computer crime.

The purpose of this study is to estimate patterns of computer-crime victimization by applying *routine activities theory*. This shall be done by presenting the argument that Cohen and Felson's (1979) routine activities theory is actually an expansion of Hindelang, Gottfredson, and Garofalo's (1978) *life-exposure theory*. One of the main concepts from life-

[1] Assistant Professor, Department of Criminal Justice, Bridgewater State College, 24 Meadow LN Apt. #8, Bridgewater, MA 02324. Email: kchoi@bridgew.edu

exposure theory, lifestyle variables, is arguably what Cohen and Felson (1979) refer to in routine activities theory as their target suitability component. It is these lifestyle variables that contribute to potential computer-crime victimization. The concept of interest is individuals' daily patterns of routine activities, including vocational activities and leisure activities, in cyberspace that increase the potential for computer-crime victimization. Also of importance is one of the three major tenets from routine activities theory, "capable guardianship." The tenet of interest is how computer security, as an important capable guardian in cyberspace, plays a major role against computer-crime victimization.

Most people are confused about the difference between cyber-crime and computer crime. In fact, some cyber crime authors do not appropriately separate the use of the terms. Therefore, before looking into the details on computer-crime victimization, it is necessary to define the difference between cyber crime and computer crime.

Casey (2001) defines cyber crime as "any crime that involves computers and networks, including crimes that do not rely heavily on computers" (p. 8). Thomas and Loader (2000) also note that cyber crime is "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3). Basically, cyber crimes cover wide categories of crime in cyberspace or on the World Wide Web including, "computer-assisted crimes" and "computer-focused crimes" (Furnell 2002, p. 22).

In general, special computer operating skills are not required to commit cyber crime. For example, a suspect and a victim may communicate via Web based chat-rooms, Microsoft Network messenger (MSN), or e-mail. Once the criminal gains the potential victim's trust, the criminal is in the position to commit a crime against the victim. In this case, even though the Internet probably assisted the suspect in communicating with the victim, it does not mean that the technology or the Internet caused the crime (Casey 2000). Indeed, in computer-assisted crimes, a computer does not have to play a major role in the crime. It can merely be the tool that is used by the suspect that assists in facilitating the eventual offense such as in the case of fraud or in a confidence scam.

The computer crimes usually require more than a basic level of computer-operating skill for offenders to commit these crimes successfully against the victims. In fact, offenders who commit a cyber crime or a computer crime are both contacting this new place, cyber-space, which is a realm different from the physical world, and which has different jurisdictions and different laws that we can apply (Carter & Katz 1997).

In this study, the individuals committing illegal or unwanted invasions of someone else's computer, including the implantation of viruses, are referred to as "computer criminals," because the project focuses solely on computer-crime victimizations. The focus of the proposed research is on individual victimization through computer crimes, particularly computer hacking, which can include the implantation of computer viruses. The term "hacking" originally referred to access by computer experts, who love to explore systems, programs, or networks in order to identify computer systems' vulnerabilities and develop ways to correct the problems (National White-Collar Crime Center 2003). However, the term "hacking" currently, and more correctly refers to unauthorized access with "intent – to cause damage, steal property (data or services), or simply leave behind some evidence of a successful break-in" (National White-Collar Crime Center 2003, p. 1).

The number of individuals victimized by computer crimes has increased annually (Gordon et al 2004). Flanagan and McMenamin (1992) state that, computer crimes

committed by the new generation of hackers, might cost cyber crime victims, as a collective, anywhere from $500 million to $5 billion an year (19). The Computer Emergency Response Team Coordination Center (CERT/CC) reports that "the number of reported incidences of security breaches in the first three quarters of 2000 has risen by 54 percent over the total number of reported incidences in 1999" (McConnell International LLC, 2000, p.1). This suggests that the hacker world is rapidly changing for the worse. Kabay's (2001) summary of studies and surveys of computer crime estimated that losses to victims of virus infections reached approximately $7.6 billion in the first half of 1999. Moreover, according to the 2005 CSI/FBI Computer Crime and Security Survey, virus attacks continue to effectuate the most substantial financial losses and, compared to the Year 2004, monetary losses have significantly escalated due to "unauthorized access to information" and the "theft of proprietary information" (Gordon et al., p. 15).

Unfortunately, the general population has still not recognized the overall seriousness of computer crime. This may explain, in part, an individual's online lifestyle patterns and the lack of computer security that can both significantly increase criminal opportunities for computer criminals in cyberspace.

As previously stated, the purpose of this study is to explain the causes of computer-crime victimization via specific components from traditional victimization theories (lifestyle-exposure theory and routine activities theory) at a micro level. This will be accomplished by examining the individual's online lifestyle, and measuring the presence of the actual installed computer security in their computer system.

The sections that follow will present an overview of lifestyle-exposure theory and routine activities theory, how routine activities theory is merely an expansion of lifestyle-exposure theory, and an overview of computer crime and victimization. A review of the relevant literature is presented followed by a discussion of the research methods, and a presentation of the data analysis. Finally, this study concludes with a discussion of the findings, limitations, and implications of this study.

Theoretical Perspectives

Both Hindelang et al. (1978) lifestyle and Cohen and Felson's (1979) routine activities theories were espoused during the same period of time that the criminal justice system began to place value on studying victimization issues (Williams & McShane 1999, pp. 233-234). Criminologists in the early 1970s began to realize the importance of victimization studies because they previously placed their focus on the criminal offender and ignored the crime victim (Karmen 2006). Creation of "the self-report survey" and the emergence of national victimization studies in 1972 facilitated the development of victimization theories in this era (Karmen 2006, p. 51). Lifestyle-exposure theory and routine activities theory were introduced based on the evidence of "the new victimization statistics" as a part of a rational theoretical perspective embedded in sociological orientation (Williams & McShane 1999, p. 235). The two theories appear to be ideally suited for understanding why individuals are predisposed to crime and how an individual's activities, interactions, and social structure provide opportunities for offenders.

Hindelang et al. (1978) suggest that an individual's daily patterned activities, such as vocational and leisure activities, contribute to victimization. They posit that an individual's expected social roles and social position influence their personal lifestyle

patterns, and contribute to the individual's decision to engage in certain activities. More importantly, engaging in risky activities can be made through individual rational choice.

Cohen and Felson (1979) assume that there are three main components to predict a likelihood of an occurring victimization event. First, a motivated offender must exist for the victimization to occur. Second, the presence of a suitable target is necessary for the occurrence of the victimization. Third, the absence of a capable guardian makes easy access for offenders to victimize the target. There must be a confluence or convergence of all three components for the victimization to occur. Thus, absence of one of the three components is likely to decrease or eliminate the victimization occurrence.

Both routine activities theory and lifestyle-exposure theory are widely applied to explain various criminal victimizations. In general, most studies found fairly strong support for both victimization theories with predatory and property crimes (Cohen & Felson 1979; Felson 1986, 1988; Kennedy & Forde 1990; Massey Krohn & Bonati 1989; Miethe Stafford & Long 1987; Roneck & Maier 1991; Sherman Gartin & Buerger 1989). Even though the two theories are empirically supported in the criminological research, the major critique resides in the failure of these theories to specify testable propositions regarding certain offenders' and victims' conditions, as such specification would allow for more accurate predictions of crime (Meier & Miethe 1993). In addition, little research has been empirically tested on individual computer-crime victimization (Kowalski 2002; Moitra 2005).

Moreover, it is proffered here that routine activities theory is simply an expansion of the lifestyle-exposure theory espoused by Hindelang et al. in 1978. In other words, routine activities theory is really a theoretical expansion of lifestyle-exposure theory, as it adopts the main tenet in lifestyle-exposure theory, the individual's vocational and leisure activities. It appears that Cohen and Felson (1979) absorbed this tenet into what they call their suitable target tenet, and then add a motivated offender and a lack of capable guardianship. It is posited here that an individual's vocational and leisure activities are what makes him or her suitable target. Even Cohen and Felson (1979) acknowledged this point. Cohen and Felson (1979) asserted that the individuals' lifestyles reflect the individuals' routine activities such as social interaction, social activities, "the timing of work, schooling, and leisure" (p. 591). These activities, in turn, create the level of target suitability that a motivated offender assigns to that particular target.

Thus, routine activities theory shares more than an important common theme with the lifestyle variable from lifestyle-exposure theory; it has actually incorporated this tenet and added the additional tenets of capable guardianship and motivated offender. Hence, it is proffered here that these two theories, routine activities theory and lifestyle-exposure theory, are not two separate theories, but that routine activities theory is simply an expansion of lifestyle-exposure theory. Therefore, this study will apply routine activities theory while acknowledging that lifestyle-exposure theory provides a more complete explanation of the "suitable target" tenet found in routine activities theory.

From the routine activities theoretical perspective, one of three tenets, capable guardian, contributes to the new computer-crime victimization model in this project. This project assumes that motivated offenders and suitable targets are given situational factors. In cyberspace, pools of motivated computer criminals can find suitable targets in the form of online users who connect to the Internet without precaution or without equipping adequate computer security (Yar 2005). In routine activities theory, Felson (1998) stated that target suitability is likely to reflect four main criteria: the value of crime target, the

inertia of crime target, the physical visibility of crime target, and the accessibility of crime target (VIVA). The application of VIVA to cyberspace indicates that target suitability in cyberspace is a fully given situation (Yar 2005). When an online user accesses the Internet, personal information in his or her computer naturally carries valuable information into cyberspace that attracts computer criminals. In addition, if computer criminals have sufficiently capable computer systems, the inertia of the crime target becomes almost weightless in cyberspace (Yar 2005). The nature of visibility and accessibility within the cyber-environment also allows the motivated cyber-offenders to detect crime targets and commit offenses from anywhere in the world (Yar 2005). Therefore, the current project speculates that within the three Routine Activities theoretical components, the most viable tenet that can control the level of computer-crime victimization is the level of capable guardianship.

The routine activities approach would lead to the practical application of situational computer-crime prevention measures by changing the conditions and circumstances. This project finds that the most feasible method of preventing computer-crime victimization that can be adapted from routine activities theory is a target-hardening strategy. This is accomplished in the form of up-to-date, adequate computer-security equipment. A target-hardening approach via computer security will make it more difficult for computer criminals to commit computer crimes in cyberspace. Since the operation of formal social control agents in cyberspace is very limited, establishing a viable target-hardening strategy can be made via equipping adequate computer security in the computer system (Tieran 2000; Yar 2005). It is also of note that the individual can also increase the target-hardening strategy by updating and maintaining this computer security. However, updating and maintaining this computer security equates to the lifestyle choices made by the individual. Regardless of whether the person properly updates and maintains the computer security, the fact remains that equipping the computer with computer security is a crucial component in reducing computer criminal opportunities in the new theoretical model (Piazza 2006).

General research on the lifestyle-exposure theory is limited in explaining computer-crime victimization, but supportive of the new theoretical computer-crime victimization model. Although studies associated with lifestyle exposure theory have not focused on computer-crime victimization, a victimology perspective based on a personal lifestyle measure under lifestyle-exposure theory is appropriate and useful for understanding computer-crime victimization. This is because the gist of the lifestyle-exposure theory is that different lifestyles expose individuals to different levels of risk of victimization. Thus, one of the research interests is to estimate the level of target suitability by measuring risk-taking factors that potentially contribute to computer-crime victimization. The project assumes that online users, who are willing to visit unknown Web sites or download Web sites in order to gain free MP 3 files or free software programs, or who click on icons without precaution, are likely to be victimized by computer criminals. In other words, the levels of online vocational and leisure activities produce greater or lesser opportunities for computer-crime victimization. Numerous findings support that lifestyle factors play significant roles in individual crime victimization in the physical world. This project hypothesizes that the level of online lifestyle activities would contribute to the potential for computer-crime victimization.

Hindelang et al. (1978) suggest that "vocational activities and leisure activities" are the most crucial components in a lifestyle which have a direct impact on exposure to the

level of victimization risk. Here, the specific tenets from lifestyle-exposure theory, as expanded upon by routine activities theory, addressed herein as the online lifestyle activities measure, will be presented as an important theoretical component. This statement is also a crucial point, which is compatible with the main lifestyle exposure theoretical perspective that explains why online users become suitable targets by computer criminals. It is the vocational and leisure activities that translate into the level of target suitability ascribed to Felson's (1998) VIVA assessment.

Mustain and Tewksbury (1998) argued that people who engage in delinquent lifestyle activities are likely to become suitable targets "because of their anticipated lack of willingness to mobilize the legal system" (p. 836). More importantly, the victims tend to neglect their risk of victimization by failing to inspect themselves regarding "*where* you are, *what* your behaviors are, and what you are doing to protect yourself" (Mustain & Tewksbury, p. 852). This study is designed to follow Mustain and Tewksbury's statement above.

This study seeks to analyze the behaviors of college students, specifically by looking at where they are on the Internet, what their behaviors are on the Internet, and what they are doing to protect themselves while they are on the Internet. The statistical method that is applied to achieve this analysis will be the application of SEM. This study hopes to make a contribution to the literature of criminology by delineating the potential correlation between the elements of an online lifestyle and the level of computer-security protection, with the resultant levels of computer-crime victimization that are experienced by the students. This shall be done by analyzing self-reports from college students with SEM. This study uses a format similar to the one that Gibbs, Giever, and Higgins (2003) employed to divide a self-report measure of deviance into multiple measures to satisfy the minimum requirements for SEM.

Methodology and Analysis

This section presents the research methods and analysis that are used to assess empirically the new computer-crime victimization model. The section consists of four phases. Phase 1 presents sampling techniques and procedure of the sample. Phase 2 of the analysis examines psychometric properties of scales on two main factors, digital guardian and individuals' online lifestyle, and computer-crime victimization. Descriptive statistics and factor analysis were mainly used to estimate the quality of measurement. In the final phase of the analysis, the measurement and structural models derived from the combination of two victimization theories were tested. Using structural equation modeling, the causal relationships among digital guardian, online lifestyle, and computer-crime victimization indexes are assessed. This assessment mainly focuses on whether digital-capable guardianship and online lifestyle directly influence computer-crime victimization.

Phase 1: Sample and Procedure

In the spring 2007 semester, a self-report survey that contained items intended to measure the major constructs of routine activities theory was administered to university

students in nine liberal studies classes at a university in the Pennsylvania State System of Higher Education (PaSSHE).

The study used a stratified-cluster, random-sample design. The sampling strategy consists of three steps. First, the full lists of liberal studies requirement classes that were available during spring 2007 were entered into a computer program known as the Statistical Package for the Social Sciences (SPSS). Second, the lists of liberal studies requirements was stratified by class level (e.g., freshman—100 level classes, sophomore—200 level classes, and upperclassmen—300 level classes and 400 level classes). Third, a proportionate sub sample of classes was randomly selected by using SPSS. In essence, a list of the university's entire liberal studies requirement classes, the classes required for all students regardless of major, was entered into SPSS. The SPSS random number generator then randomly chose 9 of these general studies classes, based on class level, for inclusion in the sample.

Entering 10 predictors (two observed variables from the digital-capable guardianship latent variable, three observed variables from online lifestyle latent variable, and three observed variables from online victimization latent variable, and two demographic variables) with a power of .95, and a medium effect size of $f = .15$, into the G*Power program computed the total sample ($N = 172$) at the .05 alpha level. Thus, threats to statistical conclusion validity were not an issue in this research. Surveying a minimum of 172 students allowed the researcher to have a large enough sample from which to assure that the sample size accurately represented the student population at IUP.

For the class selection, among 579 classes (freshmen level: 364 classes, sophomore level: 149 classes, upperclassmen level: 66 classes), 9 classes based on class level were randomly selected, using SPSS 14 (SPSS, 2006). A total of 345 respondents took part in the study, and 204 respondents fully completed the survey. Hence, a useable sample of 204 surveys was analyzed for this project.

Any student, who was enrolled in the general studies course and utilized his or her own personal computer, or laptop, was qualified to participate in the proposed survey. This qualification was necessary because it would be extremely difficult to identify individual computer-crime victimization if the students only used public computers for their online activities. In addition, most students utilizing the public computers might be unaware of the security measures installed on those computers, thus affecting the accuracy of the measurements necessary for purposes of this study.

The survey instrument was used to delineate the big picture of computer-crime victimization patterns among the university student population. There were a couple of advantages in utilizing university students as the target sample for the proposed study. First, university students are expected to be literate and experienced in completing self-administered, self-report instruments. Second, this researcher believes that, because of the reduction of costs of computers over the years and the fact that most students are required to submit typed work for their classes; the students are constantly using a computer for their work and entertainment. In addition, the younger generations are believed to be more likely to view a computer as a necessity of life than older generations are (Internet Fraud Complaint Center 2003).

Phase 2: Properties of Measures

Digital Guardian

In terms of the digital-capable guardianship, this project identified the three most common digital-capable guardians available to online users: antivirus programs, antispyware programs, and firewall programs. Each of digital guardians has its own distinctive function to protect computer system from computer criminals. First digital guardian, an antivirus program, mainly monitors whether computer viruses have gained an access through digital files, software, or hardware, and if the antivirus computer software finds a virus, the software attempts to delete or isolate it to prevent a threat to the computer system (Moore, 2005). The second digital guardian is a firewall program that is mainly designed to prevent computer criminals from accessing the computer system over the online network; however, unlike the antivirus software, firewalls do not detect or eliminate viruses (Casey, 2000). The last digital guardian, antispyware program, is mainly designed to prevent spyware from being installed in the computer system (Casey 2000). Once spyware is being installed, it intercepts users' valuable digital information such as passwords or credit card numbers as a user enters them into a Web form or other applications (Ramsastry 2004).

Prior to administering the survey, potential respondents were supplied with a pre-survey guideline. The pre-survey guideline provided respondents with definitions of the three digital guardian measures and asked the potential respondents to examine their personal or laptop computer so that they could determine, prior to participation in the actual survey, whether they had any of the digital guardian measures already installed on their computers. The purpose of the pre-survey guideline was to ensure content validity in the portion of the actual survey focusing on digital guardian measure.

The researcher posits that the level of capable digital guardianship, in the form of installed computer-security systems, will differentiate the level of computer-crime victimization. Thus, the number of installed security programs on a computer and the duration of equipping the installed security programs was measured in order to estimate the level of digital-capable guardianship.

The first observed variable consisted of three items that asked the respondents to state what types of computer security they had in their own computer prior to participation in the survey. The three items were based on dichotomous structure, which was identified 0 as *absence of security* and 1 as *presence of security*. The possible range for the number of installed computer-security programs was between 0 to 3. The value 0 refers to absence of computer security and 3 means that computer users installed antivirus, anti-spyware, and firewall software in their own computer. The mean of the number of computer-security score for this sample was 2.6, with a standard deviation of .73, a skewness of -1.96, and a kurtosis of 3.37.

The internal consistency coefficient of .62 indicates an undesirable range of Cronbach's alpha based on DeVellis's (2003) reliability standards. However, the item-total correlations (Item 1 = .40, Item 2 = .43, and Item 3 = .44) were respectable, with all three items above the acceptable levels of item total correlations of .30.

The second observed variable also consisted of three items with a series of three visual analogues by asking the participants to indicate on a 10-centimeter line their responses regarding each of the three main computer-security measures. Their level of agreement with each statement was identified by asking whether they had the specific

computer-security program on their personal or lap top computers during the 10-month period. Each line had a range of 0 to 10, with the total possible range for this capable guardian scale between 0 and 30. The mean of the duration of having computer-security score for this sample was 22.3, with a standard deviation of 7.65, a skewness of -.99, and a kurtosis of .25.

The data indicate that this digital guardian scale had an adequate alpha coefficient of .70, which was sufficient for research purposes. All three scale items (Item 1 = .50, Item 2 = .52, and Item 3 = .55) performed well and sufficiently met the acceptable levels of item-total correlation, and the unidimensionality of the scales was confirmed by Cattell's *Scree test*[2] with principal components factor analysis using a varimax rotation.

Online Lifestyle

Britz (2004) asserted that even tight computer-security systems do not fully protect against all the new virus attacks because computer criminals generate various malevolent viruses on a daily basis. The research found that different online vocational and leisure activities on the Internet offer different levels of risk of victimization. The researcher posited that users' online lifestyle is also a substantial factor in minimizing computer-crime victimization. Individual online lifestyle is measured by three distinct observed variables: (a) vocational and leisure activities on the Internet, (b) online risky leisure activities (c) online risky vocational activities.

For the first measure of online lifestyle, eight survey items that made up the vocational and leisure activities scale, along with their item-total correlations. As with the vocational and leisure activities scale, respondents were asked to indicate on a 10-centimeter response line their level of agreement or disagreement with each statement. The items were anchored by *strongly agree* at the lower limit and *strongly disagree* at the upper limit. The scale's possible aggregate range is 0 to 80 with higher scores reflecting higher online vocational and leisure activities. The mean vocational and leisure activities score for this sample is 53.62, with a standard deviation of 11.22. The scale based on eight items had satisfactory skewness and kurtosis levels, and the assessment of principal factor analysis and a *Scree test* validated the scale items as a unitary construct.

For the measures of two categories of online risky lifestyle, each of four survey items was designed to rate the respondents' online leisure and vocational activities that are risky. Like other online lifestyle scale, respondents were asked to indicate on a 10-centimeter response line their level of agreement or disagreement with each statement. The terms *strongly agree* and *strongly disagree* anchor the response line.

In the category of online risky activities ("Risky Leisure Activities"), the scale's possible aggregate range is from 0 to 40. The mean of the first risky activities score for this sample is 16.02, with standard deviation of 8.93. The second category of online risky

[2] The scree test was developed by Cattell. "Scree" is a term from geology. The scree is the rubble at the bottom of a clif. If you take a correlation matrix, you can decompose it into independent weighted combinations of the original variables (these combinations correspond to factors). Each set will have some variance associated with it. The idea in the scree test is that if a factor is important, it will have a large variance. What you do is order the factors by variance, and plot the variance against the factor number. Then you keep the number of factors above the "elbow" in the plot. These are the important factors which account for the bulk of the correlations in the matrix. It's called a scree test because the graph looks a bit like where a cliff meets the plain. In looking at a cliff, you might want to decide where the cliff stops and the plain begins. With the scree test you see where the important factors stop and the unimportant ones start. What we can do is to create a plot of the eigenvalues (variances) against their serial order.

activities ("Risky Vocational Activities") consisted of four items, so the scale's possible aggregate range is also from 0 to 40. Both categories have met the appropriate levels of skewness and kurtosis for SEM analysis, and the results based on principal components factor analysis and a *Scree test* suggested that each of scale items consists of unitary construct.

Computer-Crime Victimization

Three computer-crime victimization items have been developed for this study. Major computer crime reports tend to focus on victimization based on the private sector, and these reports clearly delineate the number of victimization occurrence, time loss, and monetary loss as major findings. Thus, the current project has adapted the construct of corporate computer-crime victimization to delineate individual-crime victimization.

Computer-crime victimization scale consists of three distinct observed variables: (a) total frequency of victimization, (b) total number of hour loss, and (c) total monetary loss. In terms of data quality, the descriptive statistics imply conditions of severe non-normality of data that are one of violations in SEM assumptions. Three computer-crime victimization scales contained extreme values of skewness and kurtosis, and the reliability coefficient indicated poor variability and low item scale correlations due to strong outliers. In order to adjust a highly skewed distribution to better approximate a normal distribution, the original items were transformed, ratio level, to a Likert-like scale format based on 4 possible responses (0 to 3), which was applied through a recoding process by minimizing the magnitude of outliers.

The research has adapted the existing scales from the 2004 Australian Computer Crime and Security Survey. Even though the survey primarily focused on private organization sectors, the adaptation of their scales should be adequate to delineate individual computer-crime victimization. In the first item, "During the last 10 months, how many times did you have computer virus infection incidents?," the original responses were coded to 0 to 3 scales (0 = *0 time*, 1 = *1 – 5 times*, 2 = *6 – 10 times*, 3 = *over 10*) that are equivalent to the scales from 2004 Australian Computer Crime and Security Survey. In the second item, "During the last 10 months, approximately how much money did you spend fixing your computer due to computer virus infections?" the original responses were labeled to a scale from 0 to 3 (0 = *$0*, 1 = *$1-$50*, 2 = *$51-$100*, 3 = *over $100*). In fact, there were no specific guidelines of monetary loss in the survey, so this category of the scales was developed based on the distribution of responses from participants and the adaptation of the survey structure. In the third item, "During the last 10 months, approximately how many hours were spent fixing your computer due to the virus infections?," the original values were transformed to a scale from 0 to 3 (0 = *0 hour*, 1 = *1 -12 hours*, 2 = *13 – 84 hours*, 3 = *over 84 hours*). In the 2004 Australian Computer Crime and Security Survey (2005), the time it took to recover from the most serious incident based on day, week, and month period was estimated. The research adapted this time period by calculating 12 hours per one day for fixing computer, so scale 1, 2, and 3 respectively represent an hourly basis for days, weeks, and months.

After the application of the transformation to Likert-like format, the values of skewness and kurtosis have significantly decreased. In addition, both Cronbach's alpha and item total correlation values have significantly improved. Even though the transformation to Likert-like format could not achieve appropriate normal distribution, it offered the minimal acceptance of skewness and kurtosis levels for SEM analysis.

The computer-crime victimization scales also met the basic measurement criteria for SEM after the application of transformation to Likert-like scale. The scales have acceptable reliability (Cronbach's Alpha = .66), acceptable item-total correlations, acceptable skewness and kurtosis levels, and the observed variables are unidimensional.

Phase 3-1: Measurement Model

Nine fit indices were examined in order to determine the model fitness of the measurement model (See Table 1). Table 2 from Gibbs et al. (2003) indicated the fit indices, their justifications, and standards. Five indexes of absolute fit including chi-square, adjusted chi-square, root mean square residual (RMR), root mean square error of approximation (RMSEA), and global fit index (GFI) are reported. In addition, the Tucker-Lewis Index (TLI), the comparative fit index (CFI), the parsimonious goodness of fit (PGFI), and the expected cross-validation (ECVI) are presented in order to measure relative fitness by comparing the specified model with the measurement model.

Three out of five measures of absolute fit (adjusted chi-square, RMSEA, and GFI) sufficiently met their standards. Since the probability value of the chi-square test was smaller than the .05 level, the test result indicates the rejection of the null hypothesis that the model fits the data. However, such a rejection based on the chi-square test result was relatively less substantial compared to other descriptive fit statistics because the chi-square test is very sensitive to sample size and nonnormal distribution of the input variables (Hu & Bentler 1999; Kline 1998; Kaplan 2000). Thus, examining other descriptive fit statistics would be of substantive interest in this project.

Even though there was no absolute RMR standard, the obtained RMR value of 1.70 appeared to be high because an RMR of 0 indicates a perfect fit. The CFI and TLI, which compare the absolute fit of the specified model to the absolute fit of the measurement model, also sufficiently met the standard for appropriate model fit. Although the PGFI and ECVI do not have precise standards, the guideline of Gibbs et al. (2003) suggest that these obtained values are very close to good model fit. Despite of fact that it is very difficult to construct a model that fits well at first, the measurement model has acquired the overall good model fit. Therefore, the measurement model fits well, based on the suggested descriptive measures of fit.

Figure 1 indicates that the digital guardian latent variable has statistically significant unstandardized regression coefficients. The negative statistical relationship between the digital guardian and crime victimization is illustrated by the statistically significant unstandardized regression coefficient of -.75. The standardized coefficient of -.74 also reveals the digital guardian is the most substantial factor on computer-crime victimization. Among digital guardian observed variables, standardized coefficients indicate that both equipping number of computer-security software and the duration of the presence of computer-security software provide almost an evenly substantial impact on minimizing computer-crime victimization. These findings sufficiently support the routine activities theoretical component, capable guardianship, by emphasizing the importance of computer security that contributes to reduce computer-crime victimization.

The research findings indicated that the relationship between the online lifestyle factor and computer-crime victimization is strong as well. The unstandarized path coefficient of .04 revealed that a substantial, statistically significant relationship exists between the online lifestyle factor and computer crime victimization. The unstandarized coefficients of online lifestyle confirmed that the online users, who spend significant time

and engaged in risky online behaviors in cyberspace, are likely to be victimized. In addition, the standardized coefficient of .67 indicates that risky online leisure activities (visiting unknown Web sites, downloading games, music, and movies) provide the most substantial contribution to computer-crime victimization among online lifestyle categories. It is a very important finding because previous research has failed to identify certain types of online risky behaviors that are more susceptible to other online behaviors.

The researcher also hypothesized that there will be an interaction effect among two factors, digital-capable guardianship and online lifestyle, and this effect will directly contribute to the level of computer-crime victimization. Surprisingly, the results indicated that there was little correlation among two latent variables. Although the covariance between digital guardian and online lifestyle indicator suggested positive covariance, the result was insignificant (p = .056). In other words, the research uncovered that there was no interaction effect between personal online lifestyle and equipping computer-security features on personal desktop or laptop computers.

Table 1: *Selected Fit Indexes for the Measurement Model*

	Model fitness	Index	Value	Standard point
1.	Absolute fit	Chi-square (χ^2)	34.47 (df = 18) P. = .011	p. > .05
2.	Absolute fit	Normal Chi-square (χ^2 / df)	1.915	< 3
3.	Absolute fit	Root mean square residual (RMR)	1.73	Close to 0
4.	Absolute fit	Root mean square error of approximation (RMSEA)	.07	< .10
5.	Absolute fit	Goodness of fit index (GFI)	.96	.90
6.	Incremental fit	Tucker-Lewis Index (TLI)	.95	Close to 1
7.	Incremental fit	Comparative fit index	.97	Close to 1

		(CFI)		
8.	Parsimony	Parsimony goodness of fit index (PGFI)	.48	Larger value = Better fit
9.	Comparative fit	Expected cross-validation index (ECVI)	.35	Smaller value = Better fit

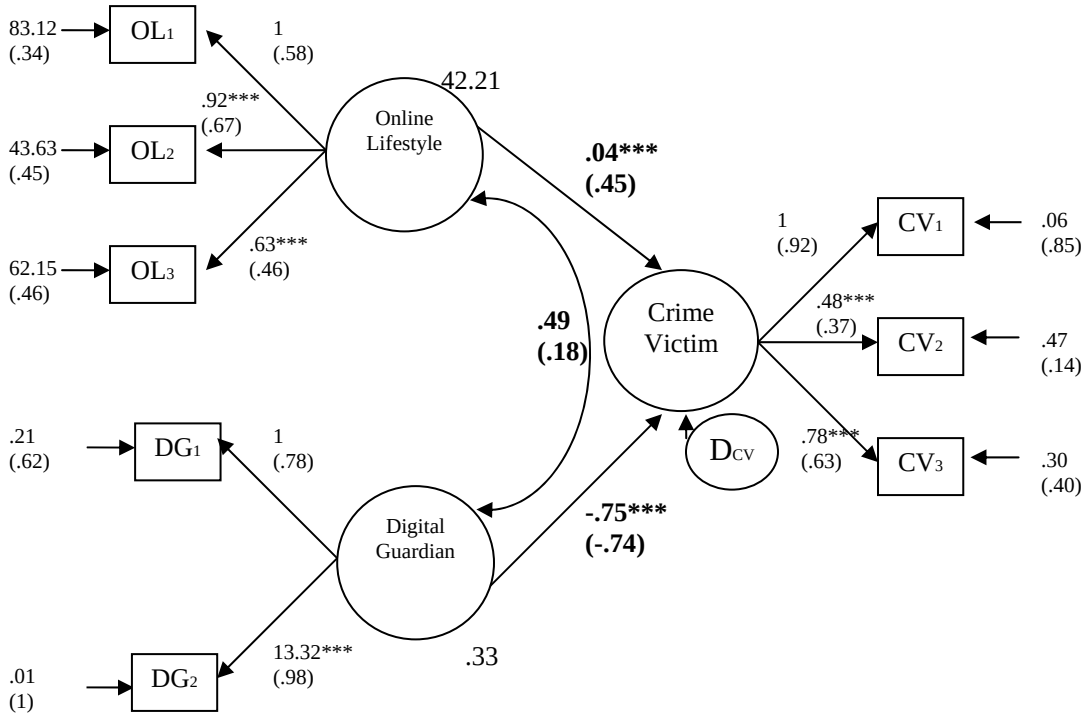

Figure 1. Measurement model.

Phase 3-2: Structural Model

Similar to the measurement model, the probability value of the chi-square test (p. = .005) was less than the .05 level. As stated in the measurement model, such a rejection based on the chi-square test result appeared to be due to sample size. Three measures of absolute fit (adjusted chi-square, RMSEA, and GFI) met or exceeded their standards. The obtained RMR value of 3.03 was higher than measurement model that indicated the structural model did not offer a perfect fit. The CFI, TLI, PGFI, and ECVI values were similar to the measurement model, which sufficiently met the standard for appropriate model. Although the structural model was unable to convey an adequate fit for model

compared to the measurement model, the model had acquired the overall good model fit for the purposes of the research (See Table 2).

Like the measurement model, the structural model also provides empirical support on the components of routine activities theory (See Figure 2). More precisely, computer-crime victims are more susceptible to personal computer victimization compared to other online users who have fully installed computer-security programs, or who use the Internet less and who avoid risky online behaviors.

Table 2: Selected Fit Indexes for the Measurement Model

	Model fitness	Index	Value	Standard point
1.	Absolute fit	Chi-square (χ^2)	38.392 (df = 19) P. = .005	p. > .05
2.	Absolute fit	Normal Chi-square (χ^2 / df)	2.02	< 3
3.	Absolute fit	Root mean square residual (RMR)	3.03	Close to 0
4.	Absolute fit	Root mean square error of approximation (RMSEA)	.07	< .10
5.	Absolute fit	Goodness of fit index (GFI)	.96	.90
6.	Incremental fit	Tucker-Lewis Index (TLI)	.94	Close to 1
7.	Incremental fit	Comparative fit index	.96	Close to 1

		(CFI)		
8.	Parsimony	Parsimony goodness of fit index (PGFI)	.50	Larger value = Better fit
9.	Comparative fit	Expected cross-validation index (ECVI)	.36	Smaller value = Better fit

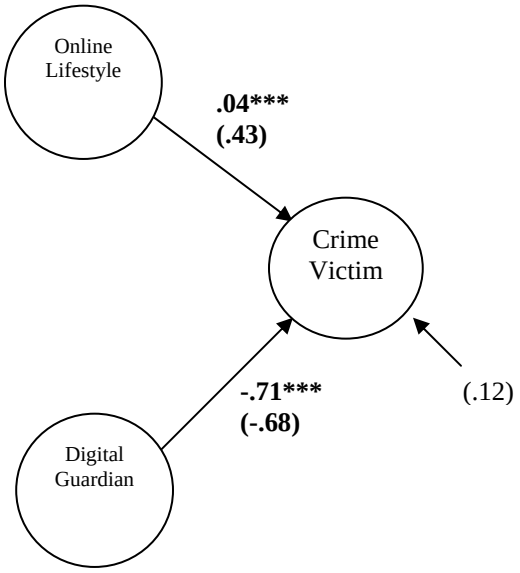

Figure 2. Structural model.

Findings and Discussion

This study assessed a new theoretical model that is theoretically derived from Hindelang et al. (1978) lifestyle-exposure theory and Cohen and Felson's (1979) routine activities theory. The central conceptual model is that digital-capable guardianship and online lifestyle directly influence computer-crime victimization. Comparisons of structural coefficients and measures of fit indicated that the central measurement model of this study is superior over the structural model.

Computer crimes constantly pose a significant threat to online users, the victimization ranges from significant monetary loss and low productivity due to work hours lost to clean up and to the loss of personal identification obtained by computer criminals (Grabosky & Smith, 2001). The findings from this project have valuable policy

relevance. The findings from this empirical study suggest that college students who overlook their computer-oriented lifestyle in cyberspace or who neglect the presence of computer-security software in their computer are likely to be victimized. The results revealed differential lifestyle patterns directly link with the occurrence of criminal victimization in cyberspace. In addition, this research supports the conclusion that the presence of computer security is the most crucial component to protect the computer systems from computer criminals. MaQuade (2006) stated that "routine activities theory has important implications for understanding crimes committed with or prevented with computers, other IT devices, or information systems" (p. 147).

The findings suggest that establishing pro-social views of promoting adequate online lifestyle and utilizing efficient computer security will contribute to the reduction in computer-crime victimization. Even though self-directed decisions by computer users for acquiring adequate online lifestyle and installed computer security on their computers have become increasingly important, contemporary criminal justice crime prevention programs tend to neglect the importance of these issues. In addition, while the number of computer users is increasing everyday, structured computer-crime prevention programs are not fully available to online users (Moitra 2005). Computer-crime prevention programs, however, can be logically categorized as school-based crime prevention programs. In fact, some colleges and universities currently offer introductory and specialized courses in computer-crime and information security issues (McQuade 2006).

McQuade (2006) asserts that a major opportunity to minimize computer crime through enhanced information security is via "public awareness, formal education, and professional training" (p. 487). The program should not only address specific methods such as general knowledge on information security and valuable tips to avoid crime victimization to help prevent computer crime, but also it should emphasize law and regulations relating to cyber crime to facilitate the acquisition of solid ethical standards for students.

In addition, the program must employ adequate online lifestyles by alerting the individual to online risk-taking behaviors that allow students to transform the constructed general online practices into their personal lifestyles. Furthermore, the program should emphasize law and regulations on computer crime with the goal of reinforcing ethical norms and expectations for computer users' behaviors (Moitra 2005).

This study has a number of limitations that should be considered for future research. Even though the results from this study may represent the university's student population, such results should not be extended as representative for the entire Pennsylvania state university population, or the university population in the United States. In addition, the potential universities for future research should be selected by taking into consideration the level of computer technical support and the size of the student populations. Therefore, future research needs to include diverse sites that are carefully examined to ensure that the geographic locations and characteristics of the student population represent the entire university population in the United States.

An additional limitation in this study is that it is impossible to have a completely precise measure of computer security. It is also important to acknowledge that there might be some error associated with the measurement of digital guardianship. This is due to the fact that most participants might not remember how long such computer-security products had been loaded on their computers. In future studies, the researcher must be aware of this issue, and prior to the general survey administration, identifying specific dates

of individual computer-security installations from participants' computer systems would be crucial in order to enhance the quality of computer-security measurement.

The research also concerned content validity regarding computer security. It is possible that the participants in the study might not fully understand each of the computer-security definitions or precise functions of the computer-security software. This lack of understanding could lead to underreporting or over-reporting. Thus, this lack of understanding would affect the content validity of the study. However, steps have been taken here to increase the precision of measurement regarding these components by providing the participants with the pre-survey guideline, but even that precaution is not infallible.

In criminology literature, it is commonly acknowledged that demographic factors are associated with general crime victimization in the physical world. However, the relationship between social context variables and factors associated with individual computer crime victimization has not been precisely revealed. In fact, the sample used in this study did not focus on the relationship between demographic factors and cyber crime factors. The assessment of causal relationships between demographic variables (age, race, and gender) and cyber crime factors needs to be discussed in future research. Future assessment should focus on how demographic variables are statistically associated with many causal variables such as fear of cyber-crime, digital capable guardianship, online lifestyle activities, and computer crime victimization.

It is also important to note that criminology literature has attempted to elucidate various risk-taking behaviors via the application of other theoretical insights. At an early stage, many researchers believed that risk-taking behaviors were "predisposed by personality" and they posited that individuals with two modal personality characteristics have determined to their susceptibility of engagement in risk-taking behaviors. Lyng (1990) identified five terms for the two modal types (risk seeker vs. risk averter) from the early literature: (a) the "narcissistic" vs. the "anaclitic" (Freud 1925), (b) the "extrovert" vs. the "introvert" (Jung 1924), (c) the "Schizoid" vs. the "Cycloid" (Kretchmer 1936), (d) the "counterphobic" vs. "phobic" (Fenichel 1939), and (e) the "philobatic" vs. the "ocnophilic" (Balint 1959). In addition, other terms such as "stress-seekers" (Klausner, 1968), "sensation-seekers" (Zucherman et al 1968), "eudaemonists" (Bernard 1968) were used to identify individuals who seek high-risk experiences (Lyng 1990, p. 853). Unfortunately, these studies were unable to convey adequate empirical validity due to the failure of explaining causal factors in risk-taking behaviors (Lyng 1990).

On the contrary, other studies unveiled a causal factor of high-risk-taking behavior using the term as the "intrinsic motivation approach" by blending a broad range of "physiological, psychological, and neurological" perspectives that explain individuals' risk-taking behaviors. Klausner (1968) asserted that stress seeking can be used as a method to suffice "a need for arousal" and facilitates personal abilities to competently control over environmental barriers. Delk (1980) also identified risk-seeking behaviors as a method to reduce tension associated with the increase of intoxicating stress hormones. However, micro-macro connections among the variables within the concepts of intrinsic motivation approach were major concerns, and these studies were unable to operationalize the concept of "intrinsic motives." Lyng (1990) also introduced a concept of edgework that explains voluntary risk-taking behaviors by accounting social psychological perspective derived from the amalgamation of the Marxian and Meadian frameworks into consideration.

In the future, it is crucial for researchers to consider various theoretical perspectives in order to uncover individual victimization in online environments by exploring why individuals continue to use risky online behaviors.

Thus, researchers in future studies need to develop more precise scales to measure computer security and online users' behaviors and explore other theoretical perspectives for delineating a true crime victimization model. Future research must also remain cognizant of this fact and apply the same, if not more, protection to ensure this aspect of content validity.

Conclusions

This project is an initial step toward constructing a solid computer-crime victimization model based on routine activities theory. In this study, routine activities theory is presented in detail in the main body of this study, via the combination of Hindelang et al.'s (1978) lifestyle-exposure theory and Cohen and Felson's (1979) routine activities theory.

In fact, many criticisms on computer crime related quantitative and qualitative research are driven from lack of "generalizable data" based on computer-crime incidents against private victims in quantitative research, and small sample sizes in qualitative research that may draw biased outcomes (Moitra 2005). The research has accomplished most of its main objectives. The main contribution of this research is that it constitutes an inventive attempt to uncover computer crime victimization by integrating two criminological victimization theories with the empirical assessment of SEM. From lifestyle-exposure theory, the research transformed from its crucial theoretical component, individual's daily living patterns, to individual's computer-oriented lifestyle in cyberspace as one of main tenet in the model. From the perspective of routine activities theory, the crucial key element of a capable guardian was logically reconstructed with digital capable guardian, which represents computer security in this research.

The logical underpinning of the research has conveyed adequate empirical validity. The results of the empirical assessment demonstrate that online lifestyle and digital guardianship are all important aspects of a model delineating patterns of computer crime victimization.

References

2002 Internet fraud report. (2003). Retrieved June 1, 2007, from http://www.ic3.gov/media/annualreports.aspx

2004 Australian computer crime and security survey. (2005). Retrieved June 1, 2007, from http://www.auscert.org.au/render.html?it=2001

2004 IC3 Internet crime report. (2005). Retrieved June 1, 2007, from http://www.ic3.gov/media/annualreports.aspx

2005 FBI computer crime survey. (2006). Retrieved November 6, 2006, from http://www.fbi.gov/publications/ccs2005.pdf

Britz, M. T. (2004). *Computer forensics and cyber crime*. New Jersey: Pearson Prentice Hall.

Carter, L. D., & Katz, J. A. (1997). *Computer crime: An emerging challenge for law enforcement*. Retrieved November 20, 2004, from http://www.sgrm.com/ art11.htm

Casey, E. (2000). *Digital evidence and computer crime*. London: Academic Press.

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

Delk, L. (1980). *The many faces of suicide*. New York: McGraw-Hill.

DeVellis, R. (2004). *Scale development*. London: Sage.

Erdfelder, E., Faul, F., & Buchner, A. (1996). GPOWER: A general power analysis program. *Behavior Research Methods, Instruments, & Computers, 28*(1), 1-11.

Etter, B. (2001). *The forensic challenges of e-crime, current commentary No.3*. Adelaide, Australia: Australasian centre for Policing Research.

Flanagan, W., & McMenamin, B. (1992). The playground bullies are learning to type, *Forbes, 150,* 184-189. Retrieved February 6, 2007. from http://www.mindvox .com/cgi-bin/WebObjects/MindVoxUI.woa/wa/staticpage%

Felson, M. (1986). Routine activities, social controls, rational decisions and criminal outcomes. In D. Cornish and R. Clarke (Eds), *The reasoning criminal* (pp. 302-327). New York: Springer Verlag.

Felson, M. (1998). *Crime and everyday life: Insights and implications for society*, (2nd ed.). Thousand Oaks, CA: Pine Forge Press.

Furnell, S. (2002). *Cyber crime: Vandalizing the information society*. London: Addison Wesley.

Gibbs, J. J., Giever, D. (1995). Self-control and its manifestations among university students: an empirical test of Gottfredson and Hirshi's general theory. *Justice Quarterly, 12*, 231-235.

Gibbs, J. J., Giever, D., & Higgins, G. E. (2003). A test of the Gottfredson and Hirschi general theory of crime using structural equation modeling. *Criminal Justice and Behavior, 30*, 441-458.

Gordon, M. P., Loef, M. P., Lucyshyn, W., & Richardson, R. (2004). *CSI/FBI computer crime and security survey*. Los Angeles: Computer Security Institute.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.) *Crime and the Internet* (pp. 23-45). London: Routledge.

Hidelang, M. J., Gottfredson, M. R., & Gaffalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

Hu, L., & Bentler, P. M. (1995). Evaluating model fit. In R. H. Hoyle (Ed.), *Structural equation modeling: Concepts, issues, and applications* (pp. 76-99). Thousand Oaks, CA: Sage.

Internet Fraud Complaint Center. (2003). *IFCC 2002 Internet fraud report*. Washington, DC: U.S. Government Printing Office.

Kaplan, D. (2000). *Structural equation modeling: Foundations and extensions*. Thousand Oaks, CA: Sage.

Karmen, A. (2006). *Crime victims*. Thousand Oaks, CA: Thomson Higher Education

Kabay, M. E. (2001). *Studies and surveys of computer crime*. Norwich, CT: Department of Computer Information Systems.

Kennedy, L. W., & Forde, D. R. (1990). Routine activities and crime: An analysis of victimization in Canada. *Criminology* 28, 137-151.

Klausner, Z. (1968). *Why men take chances*. New York: Anchor.

Kline, R. B. (1998). *Principles and practices of structural equation modeling*. New York: Guildford Press.

Kowalski, M. (2002). *Cyber-crime: Issues, data sources, and feasibility of collecting police-reported statistics*. Ottawa: Statistics Canada.

Lyng, Stephen (1990). Edgework: A social psychological analysis of voluntary risk taking. *The American Journal of Sociology 95*, 851-886.

McConnell International LLC. (2000). *Cyber crime… and punishment? Archaic laws threaten global Information*. Washington, DC: McConnell International.

McQuade, S. C. (2006). *Understanding and managing cyber crime*. Boston:Pearson/Allyn and Bacon.

Massey, J., Krohn, M., & Bonati, L. (1989). Property crime and the routine activities of individuals. *Journal of Research in Crime and Delinquency 26*, 378-400.

Meier R., & Miethe, T. (1993). Understanding theories of criminal victimization. *Crime and Justice 17*, 459-499.

Miethe, T., Stafford, M., & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/ lifestyle theories. *American Sociological Review 52*(2), 184-194.

Moitra, S. D. (2005) Developing policies for cyber crime. *European Journal of Crime, Criminal Law and Criminal Justice*, *13*(3), 435-464

Moore, R. (2005). *Cyber crime: Investigating high-technology computer crime*. Philadelphia: LexisNexis Group.

Mustaine, E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology 36*, 829-857.

Piazza, P. (2006, November). Technofile:Antisocial networking sites. *Security Management*, 1-5.

Ramasastry, A. (2004). *Cable News Network (CNN).com. Can Utah's new antispyware law work?* Retrieved January 16, 2007, from http://www.cnn.com/2004/ LAW/06/03/ramasastry.spyware/index.html

Roncek, D. W., & Maier, P. A. (1991) Bars, blocks, and crimes revisited: Linking the theory of routine activities to the empiricism of hot spots. *Criminology, 29*, 725-753.

Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). Hot spots of predatory crime: routine activities and the criminology of place. *Criminology, 27*(2), 27-55.

Standler, B. R. (2002, September 4). *Computer crime*. Retrieved February 6, 2005, from http://www.rbs2.com/ccrime.htm

Thomas, D., & Loader, B. (2000). Introduction–Cyber crime: Law enforcement, security and surveillance in the information age. In D. Thomas & B. Loader (Eds.), *Cyber crime: Law enforcement, security and surveillance in the information age*. London: Routledge.

Williams, F. P., & McShane, M. D. (1999). *Criminological theory*. Upper Saddle River, NJ: Prentice Hall.

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

APPENDIX A: DIGITAL GUARDIAN ITEMS & QUALITY OF MEASURES

Item-Total Correlations for Digital Guardian (Number of Security): Three Items

Item		Item total correlation	Cronbach's alpha if item deleted
1.	Did you have antivirus software on your computer during the last 10 months?	.40	.55
2.	Did you have antispyware software on your computer during the last 10 months?	.43	.42
3.	Did you have firewall software on your computer during the last 10 months?	.44	.41

Cronbach's Alpha = .62

Item-Total Correlations for Digital Guardian (Duration of Having Security): Three Items

Item		Item total correlation	Cronbach's alpha if item deleted
1.	I always had antivirus software on my computer during the last 10 months.	.50	.64
2.	I always had antispyware software on my computer during the last 10 months.	.52	.60
3.	I always had firewall software on my computer during the last 10 months.	.55	.56

Cronbach's Alpha = .70

Principal Components Analysis (Varimax Rotation) of Digital Guardian: Number of Security

Factor	Eigenvalue
1	1.69
2	.68
3	.63

Principal Components Analysis (Varimax Rotation) of Digital Guardian: Duration of Having Installed Security

Factor	Eigenvalue
1	1.88
2	.59
3	.52

APPENDIX B: ONLINE LIFESTYLE ITEMS & QUALITY OF MEASURES

Item-Total Correlations for Vocational and Leisure Activities: Eight Items

Item		Item total correlation	Cronbach's alpha if item deleted
1.	I frequently checked my e-mail during the last 10 months.	.33	.64
2.	I frequently used an instant messenger (e.g., MSN, AOL, etc.) to communicate with people during the last 10 months.	.37	.62
3.	I frequently spent time downloading materials from the Internet during the last 10 months.	.34	.63
4.	I frequently spent time shopping on the Internet during the last 10 months.	.21	.66
5.	I frequently spent time on the Internet to entertain myself during the last 10 months.	.55	.57
6.	I frequently viewed or watched news on the Internet during the last 10 months.	.30	.64
7.	I frequently sent e-mails to people during the last 10 months	.26	.64
8.	I frequently spent time on the Internet when I was bored during the last 10 months.	.54	.58

Cronbach's Alpha = .66

Principal Components Analysis (Varimax Rotation) of Vocational and Leisure Activities

Factor	Eigenvalue
1	2.58
2	1.32
3	1.16
4	.92
5	.65
6	.57
7	.50
8	.31

Item-Total Correlations for Risky Leisure Activities: Four Items

Item		Item total correlation
1: B10	I frequently visited Web sites that were new to me during the last 10 months.	.31

2: B12	I frequently downloaded free games from any Web site during the last 10 months.	.69
3: B13	I frequently downloaded free music that interested me from any Web site during the last 10 months.	.66
4: B14	I frequently downloaded free movies that interested me from any Web site during the last 10 months.	.67

Cronbach's Alpha = .73

Item-Total Correlations for Risky Vocational Activities: Four Items

Item		Item total correlation
1: B15	I frequently opened any attachment in the e-mails that I received during the last 10 months.	.72
2: B16	I frequently clicked on any Web-links in the e-mails that I received during the last 10 months.	.77
3: B17	I frequently opened any file or attachment I received through my instant messenger during the last 10 months.	.63
4: B18	I frequently clicked on a pop-up message that interested me during the last 10 months.	.41

Cronbach's Alpha = .80

Principal Components Analysis (Varimax Rotation) of Risky Leisure Activities

Factor	Eigenvalue
1	1.96
2	.91
3	.61
4	.52

Principal Components Analysis (Varimax Rotation) of Risky Vocational Activities

Factor	Eigenvalue
1	2.32
2	.84
3	.55
4	.30

APPENDIX C: COMPUTER CRIME VICTIMIZATION ITEMS & QUALITY OF MEASURES

Descriptive Qualities of Computer-Crime Victimization Measures

Name of Scale	*N*	*M*	*SD*	Skewness	Kurtosis
Frequency of virus infection	204	3.85	21.45	9.54	97.88
Monetary loss	204	$ 17.85	75.95	6.50	49.39
Hour loss	204	6.23 Hrs	13.69	3.89	18.33

Descriptive Qualities of Computer-Crime Victimization Measures: Likert-like Format

Name of scale	*N*	*M*	*SD*	Skewness	Kurtosis
Frequency of virus infection	204	.65	.63	.92	1.98
Monetary loss	204	.25	.74	3	7.76
Hour loss	204	.58	.80	1.14	.27

Item-Total Correlations for Computer-Crime Victimization

Item		Item total correlation
1.	During the last 10 months, how many times did you have computer virus infection incidents?	.28
2.	During the last 10 months, approximately how much money did you spend fixing your computer due to computer virus infections?	.24
3.	During the last 10 months, approximately how many hours were spent fixing your computer due to the virus infections?	.29

Cronbach's Alpha = .26

Item-Total Correlations for Computer-Crime Victimization: (Likert-like Format)

Item		Item total correlation
1.	During the last 10 months, how many times did you have computer virus infection incidents?	.55
2.	During the last 10 months, approximately how much money did you spend fixing your computer due to computer virus infections?	.35

3.	During the last 10 months, approximately how many hours were spent fixing your computer due to the virus infections?	.53

Cronbach's Alpha = .66

Principal Components Analysis (Varimax Rotation) of Computer-Crime Victimization: (Likert-like Format)

Factor	Eigenvalue
1	1.81
2	.76
3	.43

APPENDIX D: CORRELATIONS AND COVARIANCES BETWEEN OBSERVED VARIABLES

	DG1	DG2	OL1	OL2	OL3	CV1	CV2	CV3
DG1	1 .536							
DG2	.785 (**) 4.395	1 58.538						
OL1	.178 (**) 1.466	.181* 15.576	1 125.939					
OL2	.146 (*) .955	.112 7.667	.412 (**) 41.232	1 79.731				
OL3	.006 .038	-.019 -1.318	.268 (**) 26.751	.272 (**) 21.633	1 79.064			
CV1	-.423 (**) -.195	-.615(**) -2.965	.064 .454	.187 (*) 1.050	.266 (*) 1.488	1 .397		
CV2	-.183 (**) -.099	-.317 (**) -1.801	-.042 -.352	.094 .623	.143 (*) .944	.312 (**) .146	1 .550	
CV3	-.147 (*) -.076	-.334 (**) -1.822	.106 .845	.227 (**) 1.440	.176 (*) 1.111	.590 (**) .265	.296 (**) .157	1 .507

The top value in each cell is the correlation coefficient. The value below it is the variances or covariances
** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).