A SOCIAL LEARNING THEORY AND MORAL DISENGAGEMENT ANALYSIS OF CRIMINAL COMPUTER BEHAVIOR: AN EXPLORATORY STUDY

BY

Marcus K. Rogers

A Thesis
Submitted to the Faculty of Graduate Studies
in Partial Fulfillment of the Requirements
for the Degree Of

DOCTOR OF PHILOSOPHY

Department of Psychology
University of Manitoba
Winnipeg, Manitoba

Abstract

This study was exploratory and examined the characteristics of individuals engaged in computer criminal activity. It was predicted that individuals who had engaged in illicit computer activity would have higher rates of differential association, differential reinforcement, and moral disengagement than non-criminals. It was also hypothesized that the combination of differential association, differential reinforcement, and moral disengagement better predict criminal computer behavior than either variable alone. In Phase 1 of the study, a comparative analysis was conducted on demographic data from 132 computer and general criminals. In phases 2 and 3, 112 Internet participants, and 36 general criminals participants completed the Computer Crime Index & Social Learning Questionnaire and the Paulhus Deception Scale (Paulhus, 1998). The hypotheses regarding differential association, differential reinforcement, and moral disengagement were supported. However, contrary to the predictions, the reduced model consisting of moral disengagement and differential association better predict criminal computer behavior. Additional exploratory analyses and the implications for future research are also discussed.

Table of Contents

Abstract i
List of Figures vi
List of Tables vii
Introduction 1
    Legislation 5
    Evolution of the Term Hacker 9
    Social Learning Theory 12
        Differential association 19
        Differential reinforcement 21
        Definitions 22
        Imitation 25
        Supporting research and criticisms 26
    Moral Disengagement 36
        Supporting research and criticisms 41
    Hacker Research 47
    Psychological Profiles 56
Present Study 60
    Phase One 61
    Phase Two 62
    Phase Three 63
Summary of Hypotheses 63
    Hypothesis One 63

Hypothesis Two 64
Hypothesis Three 64
METHOD 64
Participants 64
Phase One 64
Phases Two & Three 66
General criminals 68
Internet participants 68
Instruments 69
Computer crime and social learning questionnaire (CCISLQ) 69
Paulhus deception scale (PDS) 77
Procedure 79
Phase One 79
Phases Two & Three 79
General criminals 79
Internet 81
RESULTS 84
Data Exploration 84
Phase One 84
Descriptive statistics 84
Computer criminal and general criminal comparison 88
Phases Two and Three 92

Missing data 92
Descriptive statistics 94
Demographics: sample vs. population 96
Demographics: criminal computer activity and no criminal activity 96
Frequency and prevalence of computer crime 101
Formal Hypotheses Testing 104
Hypothesis One: Differential Association and Differential Reinforcement 104
Hypothesis Two: Moral Disengagement 111
Hypothesis Three: Predictive Model 114
Additional Data Analyses 117
Multiple Regression Correlation Analysis of Crime Index and Social Learning Measures 117
MANCOVA Criminal Categories by Social Learning Measures 119
DISCUSSION 127
Social-demographics 130
Computer Crime Activities 132
Differential Association and Differential Reinforcement 135
Moral Disengagement 137
Predictive Model 139
Exploration 141

Definitions and differential association 142
All categories by social learning measures 143
Limitations of the Study 145
Summary 148
REFERENCES 152
Appendix A: Research Agreement-Province of British Columbia 163
Appendix B: Research Agreement-Province of Alberta 164
Appendix C: Research Agreement-Province of Manitoba 165
Appendix D: Computer Crime Index and Social Learning Questionnaire-Handout Version 166
Appendix E: Computer Crime Index and Social Learning Questionnaire-Web Based Version 179
Appendix F: E-mail Correspondence 218
Appendix G: Questionnaire Instructions-Jail 219
Appendix H: Consent Form 220
Appendix I: Participant Debriefing Report 221
Appendix J: Questionnaire Instructions-Probation 222
Appendix K: Web Consent 223
Appendix L: Web Participant Debriefing 224

List of Figures

Mechanisms of Moral Disengagement.....38

List of Tables

Table 1: Social-demographic Characteristics of Computer Criminals and General Criminals 86

Table 2: Descriptive Statistics: Age by Criminal Category 87

Table 3: Likelihood Ratio Chi-square Tests: Social-demographics by Criminal Category 89

Table 4: Cross Tabulation: Race by Criminal Category 91

Table 5: Non-parametric Test: Age and Sentence by Criminal Category 93

Table 6: Demographics: Internet and General Criminals 95

Table 7: Sample vs. Population Demographics 97

Table 8: Demographics: Computer Criminal Activity and No Criminal Activity 98

Table 9: Additional Demographics: Criminal Computer Activity and No Criminal Activity 100

Table 10: Frequecny and Indices of Criminal Computer Activity in The Past Three Years 102

Table 11: Prevalence of Criminal Computer Activities 103

Table 12: Criminal Activity by Age 105

Table 13: Pearson Correlation: PDS by Category by Social Learning Measures 106

Table 14: Descriptive: Social Learning Measures by Criminal Category 107

Table 15: Multivariate Tests: Criminal Category by Social Learning Measures 109
Table 16: Comparison of Social Learning Measure by Criminal Category 110
Table 17: Descriptive: Moral Disengagements by Criminal Category 112
Table 18: Analysis of Covariance Sel-deceptive Enhancing by Moral Disengagement by Criminal Category Between Subjects Effects 113
Table 19: Backward Stepwise (Wald) Omnibus Tests of Model Coefficients and Model Summary 115
Table 20: Variables in Equation Backward Stepwise Wald Procedure 116
Table 21: Classification Table 118
Table 22: Descriptive: Crime Index and CCISLQ Measures .. 120
Table 23: Stepwise Multiple Regression Analysis for Variables Predicting Crime Index Scores 121
Table 24: Descriptive: Social Learning Measures by All Criminal Categories 123
Table 25: Multivariate Tests: All Criminal Categories by Social Learning Measures 124
Table 26: Univariate Tests: All Criminal Categories by Social Learning Measures 126

A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study

The second half of the twentieth century has become known as the “Information Revolution” (United Nations, 1999). Information technology now touches almost every aspect of life and has become the backbone for telecommunications businesses, finance, governments, health care, and education (Garfinkel & Spafford, 1996; Gattiker & Kelly, 1997; Goodell, 1992; Littman, 1996; Rapalus, 1997; United Nations, 1999). Entire infrastructures have been built to support information technology (i.e., high-speed network backbones, fiber optics, etc.). Advances in information technology, such as the Internet, have effectively erased economic borders and further strengthened the concept of the “Global Community” (Flohr, 1995; United Nations, 1999).

The Information Revolution also has brought with it some unique social, moral, and legal problems. As with other advances, the staggering growth of information technology has outpaced society’s ability to govern, and possibly understand its implications (Denning, 1998; Mizrach, 1997; Parker, 1998; Power, 1998; United Nations, 1999). The growth rate of the Internet alone is staggering. In 1996, it was estimated that there were 13 million host

computers attached to the Internet. It has been predicted that by the year 2003 there will be over 500 million host computers attached to the Internet (United Nations, 1999). It also has been estimated that by the year 2003 the revenue generated by e-business in North America will be in the trillions of dollars (United Nations, 1999).

The world of information technology is unique in that it is without borders and, to date, there is no clear delineation of jurisdiction (Davis & Hutchison, 1999; United Nations, 1999). Information technology has opened the doors for the dissemination of information and the sharing of ideas (Denning, 1998; Michalowski & Pfuhl, 1991; Rogers, 1999). However, a certain negative element has arisen, characterized by the use of information technology for fraudulent activity, espionage, terrorism, revenge, perversion, and other criminal activities (Denning, 1998; Kanrow, Landels, & Landels, 1994; Mizrach, 1997; Rapalus, 1997; Schwartau, 1994). With society’s increasing dependence on computer systems, the consequences of computer crimes can be extremely grave. To date, there have been documented attacks against emergency 911 systems, air traffic control systems, stock exchanges, railways, banks, the military, and private businesses (Denning, 1998; Parker, 1998; United Nations, 1999). The most recent

figures from the United States indicate that in 1998-99, computer crimes cost US businesses a minimum of US $216 million (Power, 2000).

Due to the potential for harm, computer crimes and computer criminals are attracting the attention of governments, law enforcement, and many international bodies such as the United Nations (United Nations, 1999). These organizations are struggling with the nuances of dealing with both the individuals involved and the political fallout from their activities (i.e., extradition treaties, international definitions of crime).

In today's society, the media has referred to computer criminals as "hackers." The term hacker was not originally saddled with a negative connotation (Levy, 1985). The term at one time referred to an innovative programmer at the Massachusetts Institute of Technology (MIT) or Stanford University, who could figure out novel methods to overcome obstacles (Chandler, 1996; Gattiker & Kelley, 1997; Sterling, 1992). Today, however, the term hacker is synonymous with criminal computer-related activities or as Hafner and Markoff (1995) suggested, "cyberpunks."

The media devotes considerable attention to the phenomenon of hackers and the sensationalism of the acts they commit (Chantler, 1996; Rogers, 1999a; Skinner &

Fream, 1997; Wynn, 1996). Yet, despite the media attention, there have been few empirical studies of these individuals (Chantler, 1996; Denning, 1998; Parker, 1998; Post et al., 1998). We actually know very little about who these people are (Parker, 1998; Rogers, 1999b).

Computer crime is gaining the attention of law enforcement agencies and legislators (Denning, 1998; Parker, 1998; United Nations, 1999). Several governments have developed special task forces to protect their critical infrastructures from attackers (Denning, 1998; Rapalus, 1997; United Nations, 1999). Legislation has been passed in Canada, adding several computer specific offences to the Criminal Code (e.g., trafficking in passwords) (Davis & Hutchison, 1999). However, due to a lack of research on those individuals engaged in computer crimes, most of the bodies developing legislation rely on the computer security field for education and direction (Michalowski & Pfuhl, 1991).

Unfortunately, there has been a lack of formal research in information security, and the majority of computer security techniques and policies have evolved mainly from unsubstantiated anecdotes about the methods, trends, and motivations of computer criminals (Howard, 1997; Michalowski & Pfuhl, 1991; Parker, 1998). Drafting

effective legislation based purely on anecdotal information is unrealistic. Legislators clearly need more formal research to assist them in drafting both meaningful and effective legislation (Davis & Hutchison, 1999; Parker, 1998; Rasch, 1996).

Legislation

Criminal law has struggled to keep up with the expanding technologies of cyberspace (Davis & Hutchison, 1999; Michalowski & Pfuhl, 1991; Rasch, 1996; Rubinstein, 1997; Sterling, 1992). Ambiguous definitions of criminal activities in relation to computers and the Internet have caused problems in Canada and throughout the world (Davis & Hutchison, 1999). Sterling (1992) chronicled U.S. law enforcement's attempts to come to grips with hackers and their perceived threat to society. Sterling's book, The Hacker Crackdown, which chronicled Operation Sun-Devil in the U.S., concluded that inadequate and antiquated laws severely hampered law enforcement activities and ultimately embarrassed the U.S. Government (Sterling, 1992). Several of the arrested hackers in Operation Sun-Devil received little if any punishment from the courts, and some of the information allegedly stolen by the hackers was actually non-confidential public material (Sterling, 1992).

For the law to keep pace with technology, it must be able to define what constitutes a criminal act (Davis & Hutchison, 1999; Michalowski & Pfuhl, 1991; Rasch, 1996; Rubinstein, 1997; Sterling, 1992). The adversarial legal system in North America places the burden on the Crown for proving beyond a reasonable doubt each of the required elements of the offence: jurisdiction, competence and intent, along with the actions of the accused which make up the criminal offence (Rasch, 1996). Defining computer-specific criminal acts has been difficult since most legislators do not understand the technology or the ramifications of security breaches (i.e., loss of confidentiality, integrity of data, or availability of data and systems)(Davis & Hutchison, 1999).

Canadian legislators historically have reacted conservatively to any perceived need for changes to the Criminal Code.[1] This conservatism has been particularly evident with the needed changes directed at the unique characteristics of computers and the Internet (Davis & Hutchison, 1999). Instead, the courts have turned to common law concepts of crime in an attempt to define new

---

[1] The Criminal Code is the official act passed by Parliament that defines criminal offences in Canada.

restricted computer activities (Rasch, 1996). Legislators have attempted to fit Internet and computer related criminal activities into existing offences and processes (Davis & Hutchison, 1999; Rasch, 1996).

The courts and legislators have relied on metaphors to represent computer and Internet events. Some legislators, unable to grasp technological concepts, compare computer break-ins to a burglar breaking into a house or e-mail monitoring as wire tapping (Davis & Hutchison, 1999). As Davis & Hutchison (1998) stated:

> So long as the law fails to address computer specific situations with computer specific rules, we are obliged to carry our old world laws into cyberspace and try to make them work there by using such metaphors (p. 10).

Using metaphors to deal with criminal activities where the computer is merely a tool may be sufficient. A fraud is still fraud in cyberspace. The audience that can be reached by using the computer and the Internet is very large, so the scope of the offence and the jurisdiction could be multiple, but the fundamentals of some of the offences have not changed (Michalowski & Pfuhl, 1991). However, offences

that rely on an understanding of computers, network technologies, and vulnerabilities (e.g., denial of service, buffer over-runs, network sniffing) are unique. Extending the metaphor concept here can be problematic and in some cases impossible (Rasch, 1996).

An individual sitting at a terminal, who remotely accesses a network system in another country without authorization, may be guilty of an offence. The individual has broken into the system in the electronic sense, but do current break and enter laws sufficiently cover the activity? No physical entry has occurred, nor have any doors or windows been pried open in the physical sense. If the individual makes copies of some data on the network, has an offence occurred? The metaphorical approach might claim that the person committed theft and stole the information. Yet, the owner of the data has not been deprived of the data, the original data remains in its original place.

It is clear that specific laws and definitions are required when computer criminal activity falls into the category of requiring specific knowledge of a computer, system, network, or application vulnerability (Davis & Hutchison, 1999; Hollinger, 1988; Rasch, 1996). In order for legislation to be effective, an understanding of both

the technology and the individuals engaged in using it is essential (Chantler, 1996; Davis & Hutchison, 1999; Denning, 1998). In the past, the courts have been reluctant to treat computer attacks as crimes, due largely to the fact that the object of the attack has been something intangible, namely data (Davis & Hutchison, 1999). Until just a few years ago, data was not defined in the Criminal Code and, as such, it could not be criminally attacked (Davis & Hutchison, 1999). Today, data has been defined as a document and is offered protection by the Criminal Code (Davis & Hutchison, 1999).

Evolution of the Term Hacker

Many of the individuals who are using computer technology for criminal purposes have been termed hackers. There has been some controversy and confusion over the use of terms like hackers, crackers, and phreakers (Goodell, 1996; Littman, 1995; Parker, 1998). The term phreaker commonly refers to a person who is adept at manipulating and attacking telephone systems (Goodell, 1996). Hackers, on the other hand, are thought to be solely interested in networks and computers. Crackers attempt to break into systems or “crack” into them (Parker, 1998). The distinction between terms is unnecessary, as telephone systems are controlled by computer systems and have been

for over 10 years, and the term hacker is sufficiently generic to cover cracker activities (Goodell, 1996; Littman, 1995; Rogers, 1999b).

Today's use of the term hacker is vastly different from what hacking originally meant. Many of today's hackers do not appear to be interested in purely academic endeavors despite their claims in the media (Denning, 1998; Parker, 1998). For the most part, the new generation claiming to be hackers does not have computer science or programming backgrounds (Chandler, 1996; Duff & Gardiner, 1996; Levy, 1985; Sterling, 1992). Many hackers appear to be novices running pre-compiled applications, or petty criminals operating behind the guise of technology. These individuals like to refer to themselves in terms that conjure up notions of importance rather than those of contempt, such as cyber-criminals, thieves, punks, etc. (Chandler, 1996; Chantler, 1996; Duff & Gardiner, 1996). Parker (1998) stated that, while the complexity of attacks is increasing (i.e., attacking networking protocols), the skill level of the hackers is decreasing. This is due to the introduction of automated and precompiled attack software or scripts, which allow the unskilled to launch attacks on systems and networks. Fortunately, there appears to be only a few

skilled hackers creating this type of software (Denning, 1998).

The term hacker has evolved over four generations (Chandler, 1996; Levy, 1985). The first generation of hackers consisted of the talented students, programmers, and computer scientists from the Massachusetts Institute of Technology (MIT) and, later, the Stanford Artificial Intelligence Center (SAIC), during the 1950s and 1960s (Levy, 1985). They were academics or professionals interested in the lines of code or sets of instructions being processed. They were often pioneers in their field (Chandler, 1996; Levy, 1985; Sterling, 1992). To them, the motivation for their type of hacking was the intellectual challenge (Levy, 1985).

The second generation of hackers evolved from the technical elite in the 1970s. These individuals tended to be technological radicals who were forward-thinking and recognized the potential of a second computer niche from mainframe to personal systems (Chandler, 1996; Levy, 1985). Due to the often radical beliefs of these individuals (e.g., disregard for the concept of private or commercial code), minor criminal activity was not uncommon (Levy, 1985). These individuals appeared to be motivated by the

intellectual challenge and the need to think outside of traditional boundaries (Levy, 1985).

The third generation included young people who embraced the personal computer (PC) during the 1980s. They recognized the potential entertainment value of the PC and began developing games (Chandler, 1996; Levy, 1985). Many of the games were protected by code from being copied illegally, which encouraged these individuals to find novel ways of breaking the copyright codes (Levy, 1985). Here again, the criminal activity was minor in nature (Chandler, 1996; Duff & Gardiner, 1996).

The fourth, and current, generation of hackers that emerged in the late 1990s and early 2000, have embraced criminal activity as if it is some sort of game or sport (Chandler, 1996; Chantler, 1996; Denning, 1998; Duff & Gardiner, 1996; Schwartau, 1994). The motivation is neither curiosity, nor a hunger for knowledge, although these are often presented as rationales by arrested hackers. The actual motivation seems to be greed, power, revenge, or some other malicious intent (Anonymous, 1997; Goodell, 1996; Parker, 1998; Power, 1998).

Social Learning Theory

The shift toward increased criminal behavior within the hacker community is problematic and needs to be better

understood (Chantler, 1996; Denning, 1998; Rogers, 1999a). Within the fields of psychology and criminology, there have been several theories offered to try to explain why individuals engage in criminal behavior (Akers, 1977; Akers, Krohn, Lanza-Kaduce, & Radosevich, 1979; Blackburn, 1993; Burgess & Akers, 1966; Hirschi, 1969; Parker, 1998; Skinner & Fream, 1997). One such theory is social learning theory, which has evolved as an important tool for understanding traditional criminal behavior (Akers, 1977; Akers et al., 1979; Blackburn, 1993; Skinner & Fream, 1997; Wynn, 1996). Both of the disciplines of psychology and criminology have played a role in the development of social learning theory (Akers, 1977).

Social learning theory in psychology is generally associated with the work of Albert Bandura and his research on modeling and imitation (Feldman, 1993; West, 1988; Ewen, 1980). Bandura postulated that behavior could be learned at the cognitive level through observing other people’s actions (Blackburn, 1993; Feldman, 1993; Hollin, 1989). Bandura believed that people were capable of imagining themselves in similar situations, and of incurring similar outcomes (Ewen, 1980). Once the behavior is learned it may be reinforced or punished by the consequences it generates.

Bandura focused on several key concepts of the operant conditioning theory: reinforcement, punishment, and motivation (Feldman, 1993). According to Bandura there are three aspects to motivation: external reinforcement, vicarious reinforcement, and self-reinforcement (Ewen, 1980; Feldman, 1993; Hollin, 1989). External reinforcement is similar to B.F. Skinner's concept of reinforcement, and refers to stimuli in the environment that influence the likelihood of a response occurring (Ewen, 1980). Vicarious reinforcement is derived from observing other people's behavior being either reinforced or punished (Ewen, 1980). Self-reinforcement refers to one's sense of pride, or to the meeting of standards in one's own behavior (Ewen, 1980).

Although Bandura's contributions to the development of social learning theory are of major importance, Bandura tended to focus on general criminal behavior and deviance (Ewen, 1980; Feldman, 1993; Hollin, 1989). Other researchers have focused on how to apply the theory to specific criminal behavior such as computer crime. To date these researchers primarily have been from the field of criminology.

Social learning theory in criminology is associated with the work of Akers and Burgess (Ewen, 1980; Feldman,

1993; Skinner & Fream, 1997; West, 1988). In criminology the theory has been strongly influenced by the work of Sutherland (1947) and his theory of differential association. Differential association theory as described by Sutherland posited that criminal behavior was learned through a process of interactions with others. The interactions usually occurred in primary groups, where the person is presented with both criminal and anti-criminal patterns of behavior, techniques, motivations and definitions favorable or unfavorable toward crime (Burgess & Akers, 1966; Sutherland, 1947). The theory further emphasized the importance of definitions and stated that an imbalance between favorable and unfavorable definitions toward crime, with more weight on the favorable, would result in criminal behavior being exhibited (Burgess & Akers, 1966; Sutherland, 1947). Several factors, such as frequency, duration, and intensity of the definitions, affected the balance.

Burgess and Akers (1966) revised differential association theory and developed a theory they termed “differential association-reinforcement.” The primary difference between differential association-reinforcement theory and Sutherland’s (1947) differential association theory was the conceptualization of the learning process

(Burgess & Akers, 1966). Although Sutherland (1947) indicated that a learning process was part of the development of criminal behavior, the exact process was never really expanded upon. While it was assumed that the process was based on Skinner's operant conditioning principles, this was never really articulated in the original theory (Akers, 1998; Burgess & Akers, 1966).

Differential association-reinforcement explicitly conceptualized the learning process as having its basis in operant conditioning (Burgess & Akers, 1966). The individual's interactions with the environment played a large role. The theory stated that an individual's behavior was shaped and that reinforcement (negative and positive) and punishment determined the likelihood that the behavior, once exhibited, would continue (Burgess & Akers, 1966). Negative reinforcement could entail such negative events as being ostracized by one's friends or the group. An example of a positive reinforcement would be acceptance by the group or elevation in status. Punishment could include being caught by authorities and incarcerated or fined.

Akers (1977) modified the differential association-reinforcement theory and called the new theory "social learning," emphasizing the synergy between sociology and psychology. The key concepts of the new theory were

differential association and definitions (from Sutherland's 1947 theory), and differential reinforcement and imitation (from behavioral science's learning theory) (Akers, 1977; Akers, 1998).

Akers, Krohn, Lanza-Kaduce, & Radosevich (1979) indicate that social learning theory is a general theory of deviance and focuses not only on the learning of criminal techniques, but also the role of drives, motives, and rationalizations (Akers, 1977; Skinner & Fream, 1997). The central constructs of the theory can be operationalized, allowing for measurement, and can be tested empirically (Akers et al., 1979). Social learning theory also can be applied toward understanding other types of non-traditional crimes such as computer crime (Akers et al., 1979).

Social learning theory's basic assumption is that the same learning process produces both deviant and conforming behavior (Akers, 1998). The learning process operates in a context of social structure, interactions, and situations (Akers, 1998). The probability of criminal (deviant) or conforming behavior occurring is a function of the variables operating at the underlying social learning process (e.g., reinforcement)(Akers, 1977; Akers, 1998). Akers (1998) presented the theory in terms of four testable hypotheses:

> The individual is more likely to commit violations when:
>
> 1) He or she differentially associates with others who commit, model, and support violations of social and legal norms.
>
> 2) The violative behavior is differentially reinforced over behavior in conformity to the norm.
>
> 3) He or she is more exposed to and observes more deviant than conforming models.
>
> 4) His or her own learned definitions are favorable toward committing deviant acts (p. 51).

The primary learning mechanisms in the theory are differential reinforcement and imitation. The learning mechanisms are believed to operate in a process of differential association and are influenced by definitions (Akers, 1998). Differential association occurs first and provides the social environment in which the exposure to definitions and imitation of models occur (Akers, 1977; Akers et al., 1979). The definitions are learned through imitation and through observational learning (Akers, 1977; Akers et al., 1979; Ewen, 1980; Feldman, 1993; Hollin, 1989). Differential reinforcement comes from both internal

and external sources. The reinforcement can be in the form of tangible rewards of the activity itself (i.e., money) or from social rewards (i.e., increase in peer status) (Akers, 1977; Akers et al., 1979; Blackburn, 1993; Hollin, 1989). Over time, the imitation becomes less important, and reinforcement or consequences of the actions determine the probability that the activity will continue (Akers, 1977; Akers et al., 1979).

Differential Association.

Differential association in social learning theory is derived almost directly from Sutherland's (1947) conceptualization. Sutherland emphasized the importance that intimate personal groups, especially groups such as family and friends, have on individuals (Akers, 1998). He maintained that for a young child, the family plays the principle role in determining or shaping conformity or deviant behavior. In adolescence, the significance of the family is reduced and school, leisure, and recreational peer groups become more important (Akers, 1998). As the individual matures, the propensity to conform or commit criminal acts is influenced by neighbors, churches, authority figures, and the mass media (Akers, 1998).

Sutherland (1947) identified four dimensions or “modalities” along which association could vary: frequency, duration, priority, and intensity. Frequency referred to how often an individual interacts with the group or person. Duration referred to both the length of time of the relationship and the amount of time spent in the differential association. Priority here referred to “prior” in time, not a relative ranking of importance (i.e. formed early in life). Intensity referred to the significance, saliency, or importance of the association (Sutherland, 1947).

Social learning theory maintains that the “modalities” of association are important to the extent that they affect the different dimensions of reinforcement (Burgess & Akers, 1966). The modalities of association affect reinforcement due to the fact that the rewarding or negative outcomes of a behavior depend on the extent to which they are socially defined as good, desirable, important, or approved by the individual’s peers or associates (Akers, 1998).

Akers (1998) is careful to point out that differential association with peers is not synonymous with peer pressure. Peer pressure is commonly invoked as an explanation of adolescent deviant and criminal behavior. Peer pressure denotes overt expressions of influence in an

attempt to make someone commit some act (e.g., ostracizing) (Akers, 1998). Differential association with peers is subtler and often is not perceived by the adolescents themselves, but is nonetheless very influential (Akers, 1998).

According to social learning theory, the groups and persons with whom the individual is in differential association provide the social contexts in which all the mechanisms of social learning operate (Akers, 1998).

Differential Reinforcement.

The concept of differential reinforcement stems from Sutherland's (1947) idea that learning is a component of criminal behavior, and from B. F. Skinner's theory of operant conditioning (Akers, 1977; Akers et al., 1979; Blackburn, 1993; Hollin, 1989). Criminal behavior continues or is directly maintained by the consequences of the act, as in operant conditioning (Blackburn, 1993).

Akers (1977) stated that there will be a high probability of a criminal act occurring in an environment where the individual in the past has been reinforced for behaving in such a manner, and the negative consequences of the behavior have been minor (Akers et al., 1979; Hollin, 1989). Due to the fact that criminal behavior can result in

differing schedules of reinforcement and punishment (e.g. being caught), the behavior is subject to a complex learning history and is hard to extinguish (Akers et al., 1979; Feldman, 1993).

Definitions.

Social learning theory maintains Sutherland's (1947) original assertions that the learning of criminal behavior involves the learning of techniques to commit the crimes, the learning of motives, drives and rationalizations, and attitudes (Akers, 1998; Sutherland, 1947). The concept of definitions is derived from Sutherland's notion of orienting attitudes toward different behavior (i.e., rationalizations and attitudes)(Akers, 1998). Social learning theory considers exposures to other individuals shared definitions as an essential component of the process by which a person acquires his or her own definitions (Akers, 1998). According to Akers (1998) definitions can be thought of as:

> orientations, rationalizations, definitions of the situation, and other attitudes that label the commission of an act as right or wrong, good or bad, desirable or undesirable, justified or unjustified (p.78).

Social learning theory further states that definitions can be either general or specific (Akers, 1998). General definitions are usually favorable to conforming behavior, and unfavorable to aberrant or criminal behavior (Akers, 1998). General definitions are based on general beliefs, which include religious, moral and other conventional values (Akers, 1979; Akers, 1998). Specific definitions are thought to orient an individual to particular acts or series of acts (Akers, 1998). This can allow an individual who generally adheres to the norms or laws to rationalize specific aberrant or criminal acts (e.g., drinking and driving) (Akers, 1998).

Social learning theory states that the likelihood of engaging in specific acts is a function of the attitudes that the individual holds about the act (Akers, 1998). The more the individual holds a negative attitude or disapproves of the act, the less likely they are to engage in the act (Akers, 1998). Since the conventional or general beliefs of a society are negative toward criminal behavior, it is theorized that specific definitions have a more significant effect on the commission of specific criminal acts (Akers, 1998).

Definitions that favor criminal or aberrant behavior can be classified as positive or neutralizing (Akers, 1998). Positive definitions are assumed to occur less frequently than neutralizing definitions (Akers, 1998). Positive definitions are based on beliefs or attitudes that make the behavior in question desirable or “wholly permissible.” These definitions are learned primarily through positive reinforcement, often in subcultures. Examples of positive definitions toward criminal behavior or deviance can be found in the rhetoric of political dissidents, etc. (e.g., disobeying laws brings about anarchy and will lead to the demise of the current government) (Akers, 1998).

Neutralizing definitions, on the other hand, do not make the acts out to be desirable (Akers, 1998). The neutralizing definitions excuse or attempt to justify the behavior (e.g., thou shalt not kill unless in the line of duty). Neutralizing definitions view the acts as an undesirable but see the unfortunate side effects as justified given the situation (Akers, 1998). The learning of these neutralizing definitions can be accomplished in mainstream society outside of any subcultures (e.g., the media) (Akers, 1998). Neutralizing definitions incorporate notions of verbalizations or disclaimers and

rationalization (e.g., everyone else lies on their tax return.) Neutralizing definitions attempt to reduce the amount of guilt or self-censure an individual experiences after engaging in some aberrant or criminal behavior (Akers, 1998). The concept of neutralizing definitions is similar to Bandura's (1996) concept of moral disengagement (Akers, 1998).

Imitation.

Social learning theory defines imitation as committing behavior modeled on, and following the observation of, similar behavior in others (Akers, 1998). The actual imitation of the modeled behavior is affected by vicarious reinforcement (i.e., the observed consequences of the behavior) (Akers, 1998; Akers et al., 1979). The theory states that modeling is important in the initial phases of acquiring a behavior, but less so in the maintenance or cessation of behavioral patterns once they have been established (Akers, 1998).

Social learning theory holds that the media plays a role in the imitation process (Akers, 1998). The main effects of media are modeling, vicarious reinforcement, and desensitization toward violence (Akers, 1998). The media is thought to provide additional reference groups and sources

of exposure to criminal and non-criminal patterns of behavior. However, the effects of the media are believed to be weaker than face-to-face or primary group interactions (Akers, 1998).

Supporting Research and Criticisms.

Social learning theory, although popular, has been criticized for its lack of empirical testing in applied, natural settings (Akers et al., 1979). Akers et al. (1979) indicated that, although there has been a sizeable amount of research that, post hoc, appears to be supportive of social learning theory, there has been a lack of research specifically designed to test its propositions.

To address the criticisms, Akers et al. (1979) conducted a study on social learning and adolescent drinking and drug behavior. Data for the study were collected by administering a self-report questionnaire to 3065 students attending grades 7 through 12 in three midwestern states in the U.S. The questionnaire measured imitation, differential association, definitions, and differential reinforcement.

Imitation and modeling were measured by a series of items asking both users and non-users of alcohol, marijuana, stimulants, depressants and stronger drugs, if

they had seen anyone they admire use the substances (Akers, 1998). An Imitation Index was developed for each substance by summing the number of categories checked by each respondent for that substance (Akers, 1998).

Differential association was measured by asking respondents to report the normal qualities (i.e., the degree of attitudinal approval or disapproval) that they perceived were held by their important reference groups towards alcohol, marijuana, stimulants, depressants, and stronger drugs (Akers et al., 1979). The question also was asked separately for significant adults, peers, and religious groups. These became single-item measures (Akers et al., 1979).

The intensity of peer pressure was measured by asking each respondent to report, for each substance, the portion of his or her friends who used it (Akers et al., 1979). The proportion scale consisted of the following categories, none, almost none, less than half, more than half, and almost all (Akers, 1998). Frequency and duration of peer association was measured by asking the same question regarding the proportion of friends with whom the participant associated most often and those with whom the subject had associated with the longest (Akers et al., 1979).

Definitions were measured by items relating to one's own neutralizing definitions, law-abiding/violating definitions and positive/negative definitions (Akers et al., 1979). Three items each for drugs and alcohol measured the neutralizing definitions. These items measured the strength of the agreement with three techniques of neutralization (Akers et al., 1979). The techniques were: condemning the condemners, denial of injury, and denial of responsibility (Akers et al., 1979).

Law-abiding/violating definitions were measured by a scale of attitudes toward alcohol and drug laws and toward the law in general (Akers et al., 1979). The respondent's own personal attitude toward alcohol, marijuana, stimulants, depressants, and stronger drugs were measured by a single item which asked about their attitude toward each substance (Akers et al., 1979). The response categories ranged from approval, through mixed or ambivalent, to disapproval.

The study measured differential reinforcement (social and nonsocial) by breaking the concept down into rewards-costs of use, overall reinforcement balance, and usual effects (Akers et al., 1979). An index of rewards minus costs of use was calculated by summing the total perceived "good things" to happen from using each substance and then

subtracting the total of perceived “bad things” (Akers et al., 1979). An overall reinforcement balance was measured by respondents’ assessment of whether, on balance, “mainly good,” “mainly bad,” or “about as much good as bad” would result. The assessment for users was based on their personal experience, and for non-users on their perception of what would result (Akers, 1998).

A regression analysis indicated that differential association, differential reinforcement, definitions, and imitation combined to account for 68% of the variance of marijuana use, and 55% of the variance in alcohol use (Akers, 1998). The findings supported social learning theory and provided a model for operationalizing its central constructs (Akers, 1998; Akers et al., 1979).

Skinner and Fream (1997) also attempted to address the criticisms of social learning theory. They conducted research on the ability of the theory to explain the etiology of computer crime. The study used undergraduates from the colleges of Arts and Sciences, Business and Economics, and Engineering from a major southwestern university in the U.S. The sample size for study was 581, with 60.8% of the participants being male and 39.1% female. The survey used a self-report questionnaire to measure criminal computer activity in the last year and the

influence of differential association, imitation, definitions, and differential reinforcement.

The hypotheses for the study were:

1) The more college students associate with peers who are engaging in illegal computer activity, the greater the frequency of the behavior;
2) The operationalized neutralizing definitions will be positively related to computer crime;
3) The greater the perceived deterrent effect of being caught and severely punished, the less likely college students will engage in illegal computer activity;[2]
4) The more students learn about computer crime from family and teachers, the more they will engage in the behavior;
5) To the extent that students hear about or observe teachers engaging in or encouraging students to become involved in computer crime, they may begin to imitate this behavior;
6) Frequency of computer crime will increase as individuals are exposed to various media sources.

---

[2] Skinner and Fream (1997) were interested in two aspects of deterrence here, the perceived certainty of being caught and the severity of punishment.

The prevalence and frequency of computer crime was estimated by measuring five types of activities: knowingly used, made or given to another person a “pirated” copy of commercially sold software; tried to guess another’s password to get into his or her computer account files; accessed another’s computer account or files without his or her permission or knowledge just to look at the information or files; added, deleted, changed, or printed any information in another’s computer files without the owner’s knowledge or permission; wrote or used a program that would destroy someone’s computerized data (e.g., virus, logic bomb, or Trojan horse) (Skinner & Fream, 1997). Prevalence rates were measured from the responses (never, within the past month, within the past year, one to four years ago, and five or more years ago). Frequency was measured by asking the participants how often in the past year they had committed each of the five types of activities (Skinner & Fream, 1997). The response categories ranged from: never, 1-2 times, 3-5 times, 6-9 times, and 10 times or more. A computer crime index was calculated by summing the responses to the frequency measure.

Differential association was measured with a single item that asked the participant to indicate how many times his or her best friend had engaged in one or more of the

five computer activities (Skinner & Fream, 1997). Negative definitions were measured with a single item that asked participants to indicate their level of agreement with a statement indicating that they would not engage in illegal computer behavior because it was against the law (Skinner & Fream, 1997). Participants used a 4-point scale that ranged from: (1) strongly disagree to (4) strongly agree.

Neutralizing and negative definitions were measured by using a composite score of five items (Skinner & Fream, 1997). The items for both used a 4-point scale, and covered such statements as “people should have better security if they don’t wish to have their files viewed;” “I should be able to look at computer information without anyone’s permission;” “I would never turn a friend in for using, making, or giving another person pirated software;” “I would never turn in a friend who accessed another’s computer account or files, without the owner’s permission or knowledge;” “It is O.K. to for me to pirate commercial software because it costs too much to buy” (Skinner & Fream, 1997).

Differential reinforcement/punishment was measured with a series of items that asked participants to respond to questions on deterrence. Two questions measured apprehension of deterrence and two questions measured the

perceived severity of punishments (Skinner & Fream, 1997). The apprehension of deterrence items asked the participant to respond by indicating how likely it would be that he or she would be caught, either giving another person a pirated copy of software or accessing someone else's account without permission. The possible responses ranged from never to very likely. The perceived severity of punishment items asked the participant how severe he or she thought the punishment would be for giving someone pirated software and for accessing someone else's accounts without permission. The possible responses ranged from not severe at all to very severe (Skinner & Fream, 1997).

Imitation was measured with five items that asked the respondent to indicate how much they had learned about the five computer activities from each of the following: family, teachers, books or magazines, television or movies, and computer bulletin boards (Skinner & Fream, 1997). The respondent was required to use a 5-point scale ranging from (1) learned nothing to (5) learned everything. The study included two extra measures of imitation from teachers. Participants were asked to indicate how many times they had seen or heard their teachers (1) offer students the chance to "pirate" a copy of commercially sold software and (2)

praise students for computer activities they should not have done (Skinner & Fream, 1997).

A regression analysis supported the hypothesis that social learning theory could be applied to illegal computer behavior in college students (Skinner & Fream, 1997). When all social learning variables were included in the full regression model, 37% of the variance in software piracy was explained, 20% for guessing passwords, 16% for unauthorized access, and 40% for the computer crime index (i.e., the sum of all the reported frequencies of the five activities). When gender was entered first into the regression model and the learning variables second, the learning variables accounted for 75% of the explained variance when gender had a significant effect and 90% when gender did not.

Skinner and Fream (1997) concluded that differentially associating with friends was the strongest predictor of the computer crime index (standardized regression coefficient = .26, $p < .05$). The results also indicated that definitions had a significant influence on all types of reported computer activity (Skinner & Fream, 1997). All the hypotheses, except perceived certainty of punishment acting as a deterrent, were supported. Although certainty of punishment was not significant for predicting the crime

index (global crime rate), it did have a significant negative correlation with illegal access (Skinner & Fream, 1997).

The study provided support for the belief that social learning theory was an appropriate conceptual framework for understanding computer crime (Skinner & Fream, 1997). The study also found that the central concepts of social learning theory (differential association, differential reinforcement, imitation, and definitions) could be operationalized for measurement with a questionnaire, which corroborated the findings of Akers et al., (1979).

Other research and case studies have lent support to the findings of Skinner and Fream (1997). Both Denning (1998) and Parker (1998) concluded that differential association and differential reinforcement played a role in computer crimes and hacking. Parker also concluded that, from 25 years of case studies, it was apparent that hackers were being reinforced for their behavior and not punished. He cited cases in which convicted hackers were given high paying jobs in the computer security industry and treated as “stars” by the media and the “wanna-be” hackers (Parker, 1998).

Social learning theory can be used to explain involvement in computer crime (Akers, 1977; Akers et al.,

1979; Goldman-Pach, 1994; Hollinger, 1988; Skinner & Fream, 1997). However, it is also important to understand why individuals continue to engage in deviant activities, and the mechanisms involved in reducing self-sanctions that arise from prolonged involvement in deviant behavior (Bandura, 1990b).

Moral Disengagement

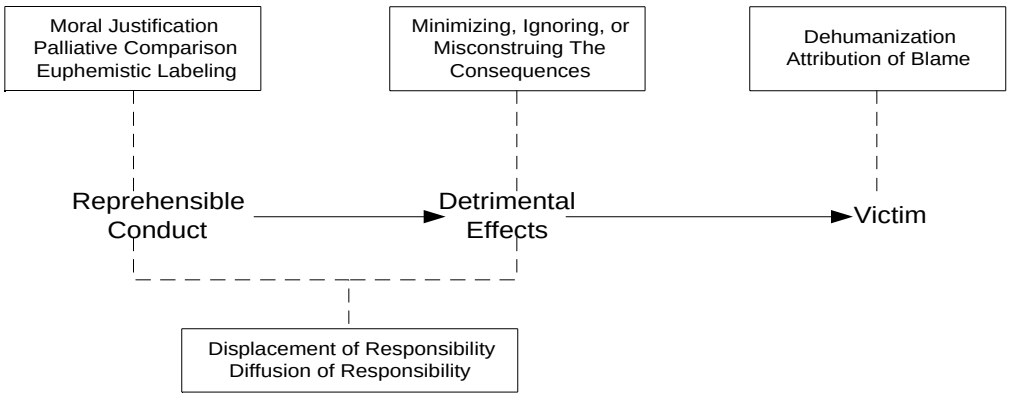
Social learning theory states that neutralizing definitions and reinforcement may interact to influence the continuation of the criminal activity (Akers, 1977, 1998; Akers et al., 1979). However, Akers (1998) stated that the concept of neutralizing definitions was similar if not identical to Bandura's model of moral disengagement. Bandura's model is a more in-depth examination of the processes involved in the rationalization and justification of deviant or aberrant behavior (Bandura, 1990a; Bandura et al., 1996).

Bandura attempted to explain how individuals who are engaged in aberrant behavior justify their activities (Bandura, 1990b; Bandura, Barbaranelli, Caprara, & Pastorelli, 1996). According to moral disengagement, people tend to refrain from engaging in behavior that violates their own moral standards (Bandura, 1990a). Such actions would lead to self-condemnation and possibly self-

sanctions. The model holds that moral standards play the role of regulating our behaviors (Bandura et al., 1996). However, these standards do not necessarily function as fixed internal controls of behavior. The self-regulatory system does not operate unless it is activated and there are several methods by which self-sanctions can be disengaged from the behavior (Bandura, 1990b). Social cognitive theory refers to these as mechanisms of moral disengagement (Bandura, 1990b; Bandura et al., 1996).

Bandura et al. (1996) stated that there were four major points in the self-regulatory system at which internal moral control can be separated from detrimental conduct (see Figure 1). An individual can disengage self-sanctions by: 1)re-construing the conduct, 2)obscuring the personal causal agency, 3)misrepresenting or disregarding the negative consequences of the action, 4)vilifying the victims, and maltreating them by blaming and devaluing them (Bandura et al., 1996; Bandura, 1990a).

Figure 1. Mechanism of Moral Disengagement



Note. From Mechanisms of Moral Disengagement in the Exercise of Moral Agency (p. 365) by A. Bandura, C. Barbaranelli, G. Caprara, and C. Pastorelli, 1996, Journal of Personality and Social Psychology, 71.

Language also plays an important role in shaping an individual's perception of his or her actions (Bandura et. al., 1996; Bandura, 1990a). Reprehensible conduct can be masked by euphemistic language and, in some cases, it can allow the conduct to be seen as respectable (Bandura, 1990a; Bandura et al., 1996).

The individual also can be relieved of a sense of personal responsibility by convoluted verbiage or by comparison to other more injurious behavior. The advantageous or palliative comparison is more effective when more flagrant activities are used in the comparison (e.g., comparing embezzling money from a large corporation to the poisoning of the environment by multinational corporations) (Bandura, 1990a; Bandura et al., 1996)

Another set of dissociative practices operates by distorting the relationship between the agent's actions and the effects of the actions (Bandura, 1990a; Bandura et al., 1996). With displacement of responsibility, individuals view their actions as arising from social pressures and, therefore, do not see themselves as responsible for their actions (Bandura, 1990a; Bandura et al., 1996). Self-censure is reduced because individuals are no longer actual agents of their actions. The action can also be ascribed to

compelling circumstances and, therefore, not construed as a personal decision (Bandura, 1990a; Bandura et al., 1996).

Personal agency can be further obscured by diffusion of responsibility. This can occur by segmentation of duties, where each segment by itself is fairly benign, although the totality is harmful. Group decisions also can be used to diffuse the responsibility (Bandura, 1990a; Bandura et al., 1996).

Another method to reduce self-censure is to disregard or distort the consequences of an action. Ignoring the detrimental consequences of the actions, as in selective inattention or through cognitive distortion, reduces the feelings of guilt (Bandura, 1990a; Bandura et al., 1996).

The last set of disengagement practices as described by Bandura et al. (1996) focuses on the recipients of the acts. Self-censure can be disengaged or weakened by stripping the victim of human attributes, or shifting the blame on to the victim. As a result of dehumanization, the victim is viewed as sub-human, not as a person with feelings. Blaming the victim or circumstances allows the perpetrators to view themselves as victims who were provoked. The perpetrator’s actions now become construed as defensive (Bandura, 1990a; Bandura et al., 1996). The

victims are blamed and accused of bringing the actions upon themselves.

Supporting Research and Criticisms.

Bandura et al. (1996) conducted a study on aggression and moral disengagement in children. The purpose of the study was to test a proposed causal structure of paths of influence through which moral disengagement affected detrimental conduct (Bandura et al., 1996). The participants in the study were 124 children in the last year of elementary school and 675 junior high school students in grades 6-8 from public schools in Rome, Italy. The mean age was 11.8 years. There were 438 males and 361 females.

The students were administered questionnaires in their classrooms by female experimenters. Data on the variables of interest also were obtained from parents, teachers, and peers of the students (Bandura et al., 1996). The scales were administered individually to the parents and teachers. Moral disengagement was measured using a multifaceted scale that measured the proneness to moral disengagement of different forms of detrimental conduct in diverse context and various interpersonal relationships (Bandura et al., 1996). Each of Bandura’s eight mechanisms of moral disengagement was represented by a subset of four items.

The social contexts encompassed by the questionnaire included educational, familial, community, and peer relations. The items were rated on a 3-point Likert-type scale, which asked children to rate their degree of acceptance of moral exoneration for certain conduct on an agree-disagree continuum (Bandura et al., 1996).

A principal-components factor analysis with varimax orthogonal rotation revealed a single factor structure that accounted for 16.2% of the variance (Bandura et al., 1996). Due to the fact that no sub-factors emerged, the responses to the items were summed to provide a composite measure of moral disengagement. Cronbach's alpha for the measure was reported at .82 (Bandura et al., 1996).

Data on the children's aggressive, prosocial, and transgressive behavior was obtained from various sources and diverse methods of assessment were used (Bandura et al., 1996). The sources included the children, their parents, teachers and peers. The methods included personality questionnaires and peer sociometric ratings. Several control items were included in each questionnaire. The children were administered two scales to measure prosocial behavior and interpersonal aggression (Bandura et al., 1996). The scales used a 3-point response format. Physical and verbal aggression was measured in 15 items

which assessed the frequency with which children fought with, or verbally disparaged others (Bandura et al., 1996). Prosocial behavior was measured by seven items that assessed the children's helpfulness, sharing, kindness, and cooperation.

The children's teachers rated the children in their classroom for physical and verbal aggression, and prosocial behavior. A shortened six-item questionnaire was developed from the children's questionnaire and it also was cast in the third person (Bandura et al., 1996). The reported Cronbach's alpha for peer ratings of prosocial behavior was .61 (Bandura et al., 1996). The Cronbach's alpha for the other three sources of data (self, parents, teachers) was all in the .80s to .90s (Bandura et al., 1996).

The study also used sociometric peer nominations as another measure of prosocial and aggressive behavior (Bandura et al., 1996). Children were given a booklet containing the names of children in their class along with 10 items. Three items measured aggressive behavior, three items measured prosocial behavior and four items measured peer popularity and aggression. For aggression, the children were asked to circle the names of three classmates who fight a lot, insult other children, and often hurt them. For prosocial behavior, the children circled the

names of three classmates who helped others, shared things, and tried to make sad people happier (Bandura et al., 1996).

Peer popularity was measured by having the children select three classmates with whom they would like to play and to study. They were also asked to select three classmates they would neither want to play with nor study with, which was considered the measure of peer rejection (Bandura et al., 1996).

The students at the junior high school level were administered two additional scales that measured the affective and cognitive aspects of aggressive and transgressive conduct relevant for older children (Bandura et al., 1996). The hostile rumination scale consisted of 15 items that assessed the level of preoccupation with personal grievances and getting even. It had a reported Cronbach's alpha of .86 (Bandura et al., 1996). The irascibility scale consisted of 14 items that assessed petulance in social transactions and weak restraints over anger with minimal provocation. The Cronbach's alpha for the irascibility scale was .84 (Bandura et al., 1996) Guilt and restitution were measured with a 15-item scale that dealt with self-regulation of transgressive conduct (causing physical injury, being destructive to property,

verbally abusive, being deceitful, or committing theft) by anticipatory self-sanctions (Bandura et al., 1996). The reported Cronbach's alpha for this scale was .79 (Bandura et al., 1996).

Delinquent behavior was measured by using relevant items from the Achenbach and Edelbrock Child Behavior Checklist (Bandura et al., 1996). The checklist covered 22 items for males and 19 items for females. Both the mothers and the children were administered the items from the checklist. The mothers and the children recorded whether they engaged in specific antisocial activities such as theft, lying, truancy, destructiveness, and the use of alcohol and drugs. The Chronbach's alpha for the parents was .77, for females .77, and .85 for males (Bandura et al., 1996).

The results indicated that disengagement was unrelated to both familial socioeconomic status and age (Bandura et al., 1996). Some interesting gender differences were found. Males had a greater readiness to provide moral justifications for detrimental conduct, to mask the conduct in euphemistic language, to minimize the conducts injurious effects, and to dehumanize and blame victims (Bandura et al., 1996).

Overall, the most commonly used disengagement mechanisms were found to be construing injurious behavior as serving righteous purposes, disowning responsibility for harmful effects, and devaluing those who are maltreated (Bandura et al., 1996).

The examination of the relationship of moral disengagement with prosocial and detrimental conduct indicated that high moral disengagers were less prosocially oriented and more likely to be rejected by peers. High moral disengagers were also found to be more likely to engage in delinquent pursuits (Bandura et al., 1996).

Bandura et al. (1996) concluded that males exhibited higher levels of moral disengagement than females. The study concluded that the male's higher levels of aggression may be influenced by the bias to disengage moral self-sanctions from injurious conduct.

Research on individuals engaged in hacking behavior indicates that they too employ mechanisms of moral disengagement as a means of reducing self-censure (Chantler, 1996; Denning, 1998; Parker, 1998). Many studies quote hackers as stating that their activities are purely an intellectual activity and that information should be freely available to everyone (Chantler, 1996; Taylor, 1997). These are clear examples of moral justification.

Other studies have found that hackers routinely minimize or misconstrue the consequences of hacking (Chantler, 1996; Parker, 1998). Participants in these studies have reported that they never intentionally damage any files, and that companies have backups of their data and systems (Chantler, 1996). Hackers also dehumanize their victims and refer to them in terms such as multi-national corporations, or networks and systems (Chantler, 1996; Parker, 1998). They usually do not comment on the impact to the end users and system administrators.

The most commonly exhibited mechanism in hackers appears to be blaming the victim. The majority of the research studies which have incorporated interviews quote the hacker participants as blaming the system administrators or programmers for lax security, and stating that the victims deserved to be attacked (Chantler, 1996; Parker, 1998).

Hacker Research

The majority of the research that has been conducted on computer crime and hackers has come from the fields of sociology and criminology. Several studies have developed categories or sub-groups of hackers (Rogers, 1999b; Skinner & Fream, 1997). This breaking down of the larger hacker

community into sub-categories is a necessary first step toward understanding these individuals (Parker, 1998; Power, 1996; Rogers, 1999a; Schwartau, 2000). By creating different hacker classifications, the studies were beginning to define operationally the term hacker (Rogers, 1999b). This is important, as the term hacker is generic and actually refers to a large heterogeneous population (Adamski, 1999; Rogers, 1999b; Taylor, 1998). Referring to someone simply as a hacker creates confusion, inaccuracies, and can lead to nominal fallacy (Denning, 1998; Parker; Rogers, 1999b).

The hacker community has been vocal about the generalizing of all individuals that fall under the hacker umbrella as criminals (Denning, 1998; Freedman & Mann, 1997; Rogers, 1999b). The hacker community claims that it maintains a loose hierarchy made up of the “elite,” “ordinary,” and “darksiders” (Adamski, 1999). The elite hackers write their own software and attack tools (e.g., automated programs designed to discover or take advantage of a vulnerability in a system or network). The ordinary hacker group consists of those individuals who use these tools (e.g., script kiddies) (Adamski, 1999). The ordinary group is also made up of individuals who focus on breaking into systems (crackers) and those who attack phone systems

(phreakers). The darksiders are involved in malicious or predatory behavior (i.e., information brokers, or using hacking for financial gain) (Adamski, 1999). Individuals within the hacker community often have discussed the hierarchy but, to date, it has not been empirically supported.

One of the earliest and most referenced studies on criminal computer behavior was conducted by Hollinger (1988). Hollinger interviewed three university students who had been convicted of gaining unauthorized access to the University of Florida's computer system and damaging files. He also interviewed eight randomly chosen computer science students. The study had the participants complete a questionnaire regarding any illegal computer activity in which they had been involved. The interviews and survey session were limited to two hours in duration (Hollinger, 1988).

Hollinger (1988) concluded that individuals were more likely to be involved in illegal computer activity if they had friends who also were engaged in the activity. The findings supported research by Sutherland (1947) and Akers (1977) on differential association and general delinquency. The study concluded that the certainty of being caught was

negatively correlated with illegal computer behavior (Hollinger, 1988).

Hollinger's study suggested that computer deviance followed a progression of involvement (Hollinger, 1988; Skinner & Fream, 1997). The involvement of the individual was fitted into three categories: "Pirates," "Browsers," and "Crackers". Each category built on the skill and loss of self-control that was necessary to commit an offence (Hollinger, 1988).

The Pirates were the least technically proficient and confined their activities to copyright violations (pirating software). The Browsers had moderate technical ability and gained unauthorized access to other people's files. They usually did not damage or copy the files (Hollinger, 1988). The Crackers had the most technical ability and were the most serious abusers (Hollinger, 1988). Their activities ranged from copying files to damaging programs and systems.

Hollinger's research has been criticized on a number of grounds. First, it has been criticized for the small number of participants and for only including two acts of computer crime in the questionnaire (Skinner & Fream, 1997). Hollinger also has been criticized for not employing a theoretical model to explain the behavior (Skinner & Fream, 1997). The study was also limited as the measure of

the prevalence and incidence of crime was restricted to only the previous four months (Rogers, 1999b; Skinner & Fream, 1997).

Chantler (1996) conducted a more in-depth investigation. The study attempted to more fully understand the profiles of hackers. The study's stated objectives were to describe the hacker environment, identify the characteristics of hackers, and generate hypotheses on the genesis of hackers (Chantler, 1996). The study was ethnographic in nature and attempted to examine the culture of hackers in a systematic fashion. The study was primarily qualitative in design and relied on interviews, both in-person and through e-mail, and an examination of artifacts (e.g., programs, notes, games, utilities, developed by the hackers). Chantler (1996) believed that qualitative-based research was an appropriate approach when attempting to discover intricate details of phenomena that are difficult to convey with quantitative methods. However, Chantler did incorporate some quantitative analyses of his surveys.

The total number of participants in the study was 164. The participants were made up of computer hackers from Australia that Chantler had known in his capacity as head of computer security for the Australian army, and other

hackers form around the world that participated via e-mail (Chantler, 1996).

The instruments for the study consisted of: observations of networks, and BBSs (computer bulletin boards), questionnaires placed online, and interviews in-person, via e-mail, telephone and fax (Chantler, 1996). The observation component used unstructured content analyses of hacker communications that Chantler had collected over a 12-year period. Two questionnaires were also placed online. The questionnaires or surveys were identical in structure and layout except for the manner in which words were spelled. In the one survey, the letter “S” was replaced with the letter “Z” as is the fad in “hacker” communiqués. Both questionnaires consisted of 90 open-ended and closed questions that addressed personal details, questions on hacking, home, school or university, work (if applicable), computing, and hacking groups.

Interviews were conducted with 23 known hackers and 41 stakeholders (i.e., computer security professionals) (Chantler, 1996). The interviews focused on hacker educational background, the genesis of a hacker (home and life environment), knowledge, motivation, information processing, threats to systems, levels of threat, and category of hackers.

The structured analysis of artifacts (games, support files, etc.) gathered the items from the following areas: open access (freely available information), underground (criminal element), hackers themselves, and hack attack victim sites. The artifacts were examined for both complexity and sophistication.

The study concluded that there were several attributes that could be used to categorize hackers (Chantler, 1996). The attributes were the hacker activities, their prowess at hacking, their knowledge, their motivation, and how long they had been hacking (Chantler, 1996). Chantler used these attributes to arrive at three categories; the elite group, neophytes, and losers and “lamers.”

The elite group displayed a high level of knowledge and was motivated by a desire to achieve, self-discovery, and by the excitement and challenge (Chantler, 1996). The neophytes displayed a sound level of knowledge, but most were still learning. They were followers and usually went where the elite group had been. The losers and lamers displayed little evidence of intellectual ability. They were motivated by a desire for profit, vengeance, theft, and espionage (Chantler, 1996). Chantler concluded that only 30% of the hacker community fell into the elite group,

60% where neophytes, and 10% percent were losers and lamers.

The study concluded that no one had forced the hackers into hacking, and that they were self-motivated and dedicated to being at the forefront of computer technology (Chantler, 1996). At the time of the study, the hacking community was just becoming organized. Chantler concluded that no real theory of their genesis was possible based on the results. The study also concluded that, although hackers had attributes that should be capitalized on by the mainstream security industry (e.g., self-motivated), their lack of ethical boundaries was problematic. Chantler (1996) warned that hackers posed a potential threat because of their intense interest in systems and curiosity about and interest in what they contained.

Chantler's (1996) study has been criticized on several fronts. One criticism was that the study relied too heavily on the participant's own classifications of hacker, with no corroborating support (e.g., crime index, convictions) (Rogers, 1999a). Other research has shown that hackers exaggerated their own importance and technical ability (Denning, 1998; Parker, 1998; Schwartau, 2000). The study has also been criticized for not using a random sample or at the least, a representative sample (Rogers, 1999a).

Furthermore, the study placed too much emphasis on e-mail interviews. With e-mail, there is no reliable method of determining who is sending the mail or if, in fact, it is from different individuals. This causes problems with the validity of the study.

However, the major criticism of Chantler's study centers on the use of the ethnographic method. Using a primarily qualitative, observational approach severely limits the possibility of empirically corroborating the findings. Also, no standard statistical procedures were followed to determine the significance of any of the findings (e.g., chi-square tests, multiple regression, path analysis)(Rogers, 1999b). Chantler (1996) acknowledged these criticisms in the conclusion but maintained that the study was exploratory and provided a foundation for future research.

Other studies have focused on a particular sub-group, the insider (Post, 1996; Shaw, Ruby, & Post, 1999). These studies have examined the personal and cultural vulnerabilities of information technology specialists who have committed computer-related crimes against their employers (Post, 1996; Shaw et al., 1999). Shaw et al. (1999), through the use of surveys and interviews, found that these individuals were prone to emotional distress,

disappointment, disgruntlement, and consequent failures of judgment. Insiders were predominantly introverted, had poor social skills, had an over-exaggerated sense of self worth, and displayed a lack of empathy (Shaw et al., 1999). The studies concluded that the information culture tends to have looser ethical boundaries and that electronic property (e.g., files, programs) is not viewed with the same ethical standards as real property (Post, 1996; Shaw et al., 1999).

Research on insiders has been criticized for being unclear on whether the characteristics of the insiders are unique to computer criminals or common to individuals who commit more general crimes such as fraud or embezzlement (Rogers, 1999b).

Psychological Profiles

From the literature reviewed it is apparent that research to date has focused on participants who have either been caught, come to the attention of officials, or who were eager to volunteer to be interviewed. These individuals make up only a small portion of the overall hacker community and, as such, the results from these studies cannot necessarily be generalized to the larger community (Denning, 1998; Parker, 1998; Rogers 1999b).

The current profile that has been developed from the research to date indicates that hackers are predominantly Caucasian, 12-28 years of age, from middle-class families. They are loners who have limited social skills and perform poorly in school (Anonymous, 1997; Chandler, 1996; Chantler, 1996; Hafner & Markoff, 1995; Littman 1997; Sterling, 1992; Wynn, 1996). They usually are not career-oriented, but show an aptitude with computers and other electronic equipment. Their families are often dysfunctional, single parent, abusive (physically and emotionally), and in some cases sexually abusive (Chantler, 1996; Freedman & Mann, 1997; Goodell, 1995; Post, Shaw, & Ruby, 1998). These individuals often display compulsive traits, such as staying online for days on end without sleep (Freedman & Mann, 1997; Goodell, 1995).

The studies suggest that the computer becomes a method for these individuals to gain control over a certain portion of their lives (Chantler, 1996; Karnow et al., 1994; Sterling, 1992). Hacking is a solitary activity, in which the individual is master over his or her machine. The computer and the Internet also provide a cloak of anonymity for these individuals. There is no face-to-face interaction on the Internet. Individuals in many of the studies reported that they could be whomever they wished to

portray. It is an opportunity to be someone with power and prestige. This is reflected in the use of nicknames often taken from science fiction or science fantasy (e.g., Analyzer, Agent Steel, Condor) (Chantler, 1996). These individuals appear unhappy with who they actually are and use the computer as a means of escapism (Chantler, 1996; Freedman & Mann, 1997; Hafner & Markoff, 1995).

Research suggests that hackers tend to be loners, yet they display a strong need to belong to a larger social group. This membership is predominantly virtual in nature (e.g., chat groups, news groups) (Hafner & Markoff, 1995; Sterling, 1992; Taylor, 1998). Individuals in several studies indicated that they attended hacker conventions and subscribed to various hacker publications (e.g., 2600 magazine) (Taylor, 1998).

Research also has concluded that individuals engaged in hacking have a tendency to brag about their exploits (Chantler, 1996; Denning, 1998; Parker, 1998). This may be due in part to their desire to be admired by their hacking peers (Freedman & Mann, 1997; Post, 1996; Sterling, 1992). However, the bragging brings them to the attention of law enforcement and consequently leads them to be arrested. The bragging and willingness to talk about their exploits often continue even while in custody and during interviews with

law enforcement officials (Hafner & Markoff, 1995; Littman, 1995).

The documented attacks that have been studied were overtly malicious in nature, which suggests that these individuals have unresolved anger, and feel a need to strike out at something or someone (Chantler, 1996; Post, 1996; Post et al., 1998; Sterling, 1992). These individuals appear to be uncomfortable with people, so they strike out at computers and networks, rationalizing that corporations are immoral and need to be taught a lesson (Post, 1996).

Studies using self-report surveys have observed that the hackers also perceive themselves as loners, under achievers, socially inept, and the products of dysfunctional families (Chantler, 1996; Post, 1996). The hackers in these studies claimed that they were motivated by the challenge, the excitement to succeed, and a desire to learn for the pure intellectual satisfaction (Post, 1996). However, some of the hackers surveyed did include vengeance, sabotage, and fraud as motivating factors (Post, 1996). The most common documented attack is directed at defacing web pages and is a type of virtual vandalism or virtual graffiti as opposed to any real learning exercise (Denning, 1998; Parker, 1998).

Present Study

Although cyber-crime and hacking have been around for nearly 30 years, research in the area has been sparse (Chantler, 1996; Denning, 1998; Parker, 1998; Rogers, 1999b; Sacco & Zureik, 1990; Skinner & Fream, 1997). Research to date has focused primarily on attempts to classify hackers into more meaningful groups. The research has been criticized for relying heavily on interviews and the subject's own self-classification as a computer criminal or hacker (Denning, 1998; Parker, 1998; Rogers, 1999b). There also have been no comparative analyses conducted between computer criminals and the general criminal population (Rogers, 1999a). Furthermore, of the studies thus far, only a few have examined a theoretical model to explain computer crime (Sherizen, 1997; Skinner & Fream, 1997).

The present study was an attempt to address some of the shortcomings of the previous research, and provide a psychological perspective for understanding individuals who engage in computer crimes. The study expanded upon the work of Skinner and Fream (1997), who studied the applicability of social learning theory as a basis for understanding computer crime. Unfortunately, Skinner & Fream (1997) did not examine the extent to which a theoretical model

explained the continuation of the hacking behavior. The study also focused solely on student participants and did not include any comparative analysis between general criminals and computer criminals (Rogers, 1999a). Without any comparisons between the two groups, it is impossible to identify the characteristics, if any, unique to computer criminals (Sherizen, 1997). The identification of unique characteristics is an important component to the development of any valid or meaningful hacker classifications (Denning, 1998; Parker, 1998; Rogers, 1999a; Sherizen, 1997).

Phase One.

Phase one of the study was exploratory and consisted of a comparison of social-demographic variables of computer criminals and general criminals. The literature reviewed indicated that there have been no prior studies that have examined this comparison. Phase one focused on a subset of the larger hacker community, namely those individuals who have actually been convicted of computer-specific criminal code offences. The phase was designed to determine if, in fact, there are any characteristics that are unique to the computer criminals specifically, rather than criminals in general.

Phase one of the study was limited to an examination of the data from individuals who had been convicted in Canada in the last five years. Prior to 1996, Canada did not have any specific computer crime offenses and no specific computer criminal data was available. The study was further limited to adult convicted general criminals, due to the fact that young offender records are sealed in Canada.

For the purpose of descriptive statistical analysis, the various social-demographic variables and arrest history data (e.g., age, sex, race, marital status, education, employment, previous arrest history, and disposition of case) were treated as dependent variables. The criminal category of the participant (i.e., general criminal population or computer criminal) was treated as an independent variable.

Phase Two.

Phase two of the study examined the differences, if any, between computer criminals, general criminals, and non-criminals on the social learning variables and moral disengagement. The dependent variables in part two of the study were differential association, differential reinforcement, imitation, definitions, and moral disengagement. Due to the fact that a self-report

questionnaire design was being used, impression management, self-deceptive enhancing and Paulhus Deception Scale totals were treated as potential control variables. The independent variables in part two were the criminal classification of the participants. The classifications were no criminal activity, computer criminal activity (including Internet and general criminal participants reporting criminal computer activity), and general criminals.

Phase Three.

In phase three the focus was on developing a foundation for predicting criminal computer activity. Phase three examined the combination of variables that provided the most efficient model for predicting computer criminal behavior. The outcome variables were the classification of the participants, and the predictor variables were dependent and control variables from phase two.

Summary of Hypotheses

The following hypotheses arise from the literature reviewed:

1) Participants who have engaged in criminal computer activity will have higher levels of differential

association and differential reinforcement than will no criminal activity participants.

2) Participants who have engaged in criminal computer activity will be more prone to moral disengagement than will no criminal activity participants.

3) The combination of the three variables of moral disengagement, differential association, and differential reinforcement will better predict criminal computer behavior than any one variable alone.

Method

Participants

Phase One

For phase one of the study, social-demographic and sentencing data from 66 convicted computer and 66 general criminals convicted over the last five years was examined (*N* = 132). The data were obtained from the British Columbia (B.C.) Department of Justice. All the provinces were canvassed, but only B.C. could provide the requested data. The other provinces indicated that they did not have the sufficient computer technology to compile the data and to do so by hand would be too time-consuming.

Inclusion of computer criminal participants was restricted to only those individuals convicted of offences that required some knowledge of computers, systems, networks, distributed computing, and their vulnerabilities. Offences such as fraud, stalking, and child pornography that involve use of the computer merely as a tool and are not directly related to vulnerabilities within computing were not considered. The applicable sections of the Criminal Code of Canada for the study were:

- 342.1(1) Unauthorized use of computer
- 342.1(1)(d) Trafficking in a password
- 342(2) Possession of unauthorized credit card data and trafficking in credit card numbers.
- 342.2 (1) Possession of a device to obtain computer service
- 326(1) Theft of telecommunication service
- 327(1) Possession of a device to obtain telecommunication facility or service
- 430(1.1) Mischief in relation to data

The inclusion criterion for the general criminal population was restricted to individuals who had been convicted of dual procedure offences (i.e., can proceed by way of summary conviction or an indictable offence)[3]. This restriction was designed to ensure that the offence severity for the "general" and "computer criminals" groups was matched, thus reducing any confounding affects that different offence severity might introduce (e.g., comparing someone convicted of mischief to data with an individual convicted of aggravated assault).

Phases Two and Three

Participation in phases two and three was voluntary. The participants consisted of 36 general criminals, and 112 Internet participants (N =148). There was a grand total of 123 Internet respondents but 10 individuals reported that they had been convicted of a criminal offense and were

---

[3] Summary offences are offences that are relatively minor in nature and carry a maximum sentence of two years less a day. The time is usually served in provincial institutions. Indictable offences are more serious and carry a sentence in excess of two years. The time is usually served in a federal institution.

excluded from the study. Another Internet respondent failed to answer more than 5% of the questions relating to the social learning measures and was excluded from the study. The total number of Internet participants used for analysis was 112. For general criminals, 37 questionnaires were returned, but one left more than 5% of the questions unanswered and was not used.

For the purposes of classifying participants, the activity of software piracy was not used. This was due to the fact that in Canada software piracy is not a criminal code offence per se, and is dealt with in civil proceedings. Software piracy was still included in the study in order to maintain consistency with other studies.

Despite extensive efforts, no convicted computer criminals volunteered to participate in the study. Out of the three provinces that participated, only Alberta indicated that there was a convicted computer criminal serving time. This individual was approached by the corrections staff and declined to participate. The participating probation services also reported that there were no computer criminals currently on probation in their jurisdictions.

General Criminals.

The inclusion criteria for general criminals limited the participants to those individuals processed at the provincial jurisdiction level. The general criminal participants were recruited by canvassing the provincial jails in British Columbia (B.C.), Alberta, and Manitoba. All the corrections departments for the provinces in Canada were contacted, but only the three listed provinces agreed to participate. Research contracts were signed with each participating province (Appendixes A-C). These contracts dictated the manner in which solicitation for participants and data collection could be undertaken.

Internet Participants.

Internet participants were recruited via the Internet. The study was advertised on several major information security sites, hacker sites, and universities throughout North America (e.g., Purdue, University of Manitoba, Simon Fraser University, www.hackernews.com, www.escape.ca, www.infosecuritymagazine.com, packetstorm.securify.com). The study was also advertised on the American Psychological Society’s Internet studies web page. The sites indicated that the study was looking at computer behaviors and attitudes in general and provided a link to the study’s web page.

Instruments

Computer Crime Index and Social Learning Questionnaire (CCISLQ).

Based on the fact that the study of computer criminals has received very little focus from the field of psychology, there were no well-validated psychological measures that combined social learning theory, moral disengagement, and illegal computer activity. This necessitated the development of a new instrument by the researcher, the Computer Crime Index and Social Learning Questionnaire (CCISLQ).

The CCISLQ was a modification of a questionnaire that had been used by Skinner and Fream (1997). The Skinner and Fream (1997) questionnaire was based on the work of Akers et al. (1979). The questionnaire operationalized the core concepts of social learning theory (i.e., differential association, differential reinforcement, definitions, imitation, and moral disengagement). The questionnaire consisted of 40 items and was designed to be used with students.

The CCISLQ modified the Skinner & Fream (1997) questionnaire to measure Canadian Criminal Code activities, to better measure the core social learning concepts as

described by Akers (1977), and to include more precise measures of Bandura's concept of moral disengagement. The CCISLQ also updated the description of activities to reflect modern terms (e.g., changing references to BBS to references to Internet).

The CCISLQ consisted of general questions to make the participant more comfortable in answering more specific questions that followed. It also included a computer crime index and expanded the number of items measuring each of the social learning constructs. Several were included that measured specific participant social-demographics (e.g., age ranges, marital status). Items in each of the scales were summed in order to arrive at a composite score on each scale (i.e., moral disengagement, differential association, etc.). The composite scores were used for data analyses.

Two versions of the CCISLQ were used in the present study. Version one consisted of 114 items and was a paper document that was provided to the general criminal participants (Appendix D). Version two consisted of 118 items and was placed on the Internet (Appendix E). Version two had four additional questions added to the end of the survey that measured knowledge and understanding of criminal computer activities and legislation, education, and occupation (items 114-118). The additional items were

included in the Internet version to better identify characteristics and social-demographics of the Internet respondents. As Krantz and Dala (2000) indicated, Internet studies suffered from the inherent problem of not knowing the characteristics/demographics of the respondents.

Other than the four additional questions, the two questionnaires were identical. The first five items of the questionnaire were designed to make the participant comfortable in answering the questionnaire and were not used to measure any particular theoretical construct. These questions were general and asked questions relating to the number of years the participant had been interested in computers, who owned the computer they used, what operating system they were most familiar with, their user level, and the number of hours per week they spent online.

Items 6-13 measured the most recent time that each participant had engaged in any of the eight types of illegal computer activities listed. The activities were software piracy, password cracking, unauthorized access to a system or account, unauthorized alteration or disclosure of data, virus or malicious computer code creation, unauthorized possession or trafficking of passwords, unauthorized possession or trafficking of credit card numbers, possession or use of a device to obtain

unauthorized telecommunications service. The possible responses ranged from: never, within the past month, within the past year, one to four years ago, and five or more years ago.

Items 14-21 measured how often in the past three years the participant had engaged in any of the illegal computer activities previously indicated. The possible responses were: A) never, B) 1-2 times, C) 3-5 times, D) 6-9 times, and E) 10 times or more. Summing the responses on these items created the crime index. For scoring purposes, the lower end of the range was used as this indicated the minimum number of times the respondents had participated in the activity (i.e., 1, 3, 6, 10). The responses to questions 15-21 were summed to determine the crime index. Question 14 pertained to software piracy and was not included. A participant with a score of zero was classified as having no self-reported criminal activity. Participants scoring higher than zero were classified as self-reporting criminal computer activity. Skinner and Fream (1997) indicated that the crime index in their study had a Cronbach's alpha = 0.60.

Items 22-29 measured the age at which the participants had first engaged in any of the previously listed illegal activities. The possible responses were: does not apply, 16

years old or less, 17-18 years old, 19-20 years old, and 21 or older.

For items 30-110 each possible response corresponded to an interval scale value (e.g., A = 1 and E = 7). These values were summed to arrive at composite total for each of the respective scales (i.e., differential association, imitation etc.).

Items 30-36 and 40-42 measured imitation. Items 30-36 measured the influence that family, peers, teachers, bosses, and the media had on participants' learning about the eight listed criminal computer activities. The possible responses included: A) learned nothing, B) learned a little, C) learned some, D) learned a lot, and E) learned nothing. Items 40-42 specifically measured how many times the participants had witnessed their teachers or their boss's overt attitudes toward illegal computer activities. The possible answers were: A) never, B) 1-2 times, C) 3-5 times, D) 6-9 times, and E) 10 times or more.

Items 37-39 were designed to measure differential association. In item 37, the participants were asked to indicate the intensity of their differential association with their friends. The possible responses were: A) none, B) just a few, C) about half D) more than half, and E) all or almost all. Items 38 and 39 measured the attitudes of

peers and family toward illegal computer activity. The possible responses included: A) strongly disapprove, B) sometimes disapprove, C) sometimes approve, and D) strongly approve.

Items 43-49 measured positive and negative definitions and required the participant to indicate their attitudes toward the listed activities. The possible responses ranged from: A) strongly disapprove, B) sometimes disapprove, C) sometimes approve, to D) strongly approve.

Items 50-96 measured differential reinforcement/punishment. Items 50-55 specifically measured deterrence and asked for the participant's perception of the likelihood of being caught for any of the eight listed criminal computer activities. The possible responses were: A) very likely, B) likely, C) somewhat likely, D) highly unlikely, and E) never.

Items 56-61 asked for the participant's perception of the severity of punishment if they did get caught being involved in the listed activities. The responses ranged from: A) very severe, B) severe, C) somewhat severe, to D) not severe at all.

Items 62-63 asked the respondent to indicate whether they or any of their friends had been caught doing

something they should not have been doing on a computer. The possible answers were: A) yes, and B) no.

Items 64-87 measured the perceived or actual balance of punishment and rewards. The items asked the participant to indicate their perception of the reactions of their friends, family, teachers or bosses, if they found out the participant was involved in the listed activities. The responses ranged from: A) turn you into authorities, B) criticize or encourage you to stop, C) do nothing, to D) encourage you to continue.

Items 88-96 measured the overall balance of desirable and undesirable outcomes of the listed activities. The possible responses were: A) mainly bad, B) about as much good as bad, and C) mainly good.

Items 96-110 measured moral disengagement. The moral disengagement scale combined the concepts of neutralizing definitions from Akers (1998) (questions 96, 98, 99, 104 – 107, and 110) and mechanisms of moral disengagement from Bandura et al. (1996) (questions 97, 100-103, 108,and 109). The items measured in the scale covered the four major points of the self-regulatory system. Questions 100, 102, 104-107, and 110, measured reconstruing the conduct. Question 109 measured obscuring personal causal agency. Questions 97-99, and 103, measured disregarding the

injurious consequences. Questions 96, 101, and 108, measured vilifying, blaming or devaluing the victim. The possible answers for the items were: A) strongly disagree, B) disagree, C) agree, D) strongly agree.

Items 111-114 were used to collect social-demographic information and asked the participants to indicate their sex, marital status, age range, and level of education.

The scales (differential association, differential reinforcement, imitation, definitions, and moral disengagement) were tested for reliability using Cronbach's alpha. For the differential association scale, $\alpha = .64$, for differential reinforcement, $\alpha = .92$, for moral disengagement, $\alpha = .87$, for imitation, $\alpha = .77$ and for definitions, $\alpha = .88$. Although the Cronbach’s alpha score of .64 for differential association was low, it was still at an acceptable level (Dunn, 1989).

The social learning construct scales had face validity and were reviewed by Akers who indicated that they were a good translation of his constructs (R. Akers, personal communication, February 2000). The scales also had content validity as they are based directly on the scales used by Akers (1998), Bandura et al. (1996), and Skinner and Fream (1997). Due to the fact that this is a new research area with little or no other research findings or scales

available, convergent and discriminant validity could not be examined.

Paulhus Deception Scales (PDS).

The Paulhus Deception Scales (PDS)(formerly known as The Balanced Inventory of Desirable Responding-7) is a 40-item questionnaire that measures an individual's tendency to provide socially desirable responses on a self-report instrument (Paulhus, 1998). Respondents are required to rate 40 statements on a 5-point scale, indicating the degree to which each statement applies to them. The scale ranges from not true to very true.

The PDS is comprised of 2 subscales: Self-Deceptive Enhancement (SDE) (items 1-20) and Impression Management (IM)(items 21-40). The SDE scale measures unconscious favorability bias, which is related to narcissism (Paulhus, 1998)[4]. Individuals scoring high on SDE are often seen as arrogant, hostile, and domineering. The questions on the SDE scale are somewhat self-reflective in nature (e.g., I

[4] Narcissism can be defined as a persistent pattern of grandiosity, lack of empathy, and an almost hypersensitivity to the evaluation of others (APA, 1994).

am not always honest with myself, I rarely appreciate criticism).

The IM scale measures the degree to which an individual is consciously self-enhancing or faking (Paulhus, 1998). Individuals are asked to rate the degree to which they perform various uncommon but socially desirable behaviors (e.g., I never swear, I have never dropped litter on the street) (Paulhus, 1998). If the individual reports an over-abundance of these behaviors, the individual may be purposely trying to impress the test administrator (Paulhus, 1998).

The PDS has been tested extensively for reliability and validity. The PDS has fair to good internal reliability, with Cronbach's alpha for college groups as: SDE = .70, IM = .81 and Total PDS = .83. Cronbach's alpha for general groups: SDE = .75, IM = .84 and Total PDS = .85. For prison entrants, the Cronbach's alphas are: SDE = .72, IM = .84 and Total PDS = .86 (Paulhus, 1998).

The PDS has been shown to be a valid instrument, with the SDE and IM scales correlated at .73 with the Marlowe-Crowne scale, and at .64 with Edward's Social Desirability Scale (Paulhus, 1998). The IM scale correlates highly with lie scales such as the Eysenck Personality Inventory (EPI) Lie Scale, and the Minnesota Multiphasic Personality

Inventory (MMPI) Lie Scale, as well as with role-playing measures such as the Wiggins Social-desirability (Sd) (Paulhus, 1998).

Procedure

Phase One

The raw data obtained for phase one covered 70 individuals convicted of computer related offences and 58,280 individuals charged with general criminal offences. Data from four of the 70 computer criminals were incomplete and they were not included in the study. To maintain a balanced design, only data from 66 randomly chosen general criminals were included in the comparison. The procedure for random assignment consisted of using the random number generation function in Microsoft Excel. A random number was assigned to each general criminal and then these were ordered by ascending numbers. Data from the first 66 general criminals were used.

Phases Two and Three

General Criminals.

For phases two and three, the directors of each of the participating facilities and probation offices in B.C., Alberta, and Manitoba were contact by phone. An e-mail was also sent outlining the research request, the fact that

signed contracts were in effect, and asking that the directors either canvass their “clients” or, in the case of B.C., ask the listed individuals to participate (Appendix F). Questionnaire packages were then compiled for handout. The packages included instructions, consent forms, CCISLQ, PDS, answer sheets and debriefing sheets (Appendixes G-I). Packages for participants on probation contained an additional self-addressed stamped envelope, and modified instructions to mail the completed questionnaires back within two weeks of obtaining them (Appendix J).

In B.C., the Department of Justice restricted access solicitation of participants to those individuals whose social-demographic and court related data had been provided in phase one of the study. These individuals were randomly chosen from an original database of 58,000 and then filtered to ensure they were either still in custody or on probation. Sixty-four questionnaire packages were forwarded to probation offices and correctional facilities in B.C. The return rate for B.C. was 0%.

In Alberta, 60 packages were delivered to the three primary correctional facilities, Calgary Correctional Center, Bow River Correctional Center, and the Calgary Remand Center. Packages were also delivered to the Alberta Department of Probation. As per the signed contract with

Alberta, each facility searched their database for individuals that met the inclusion criteria for general and computer criminals, and then canvassed these individuals. The completed sealed questionnaires were then sent by courier back to the University of Manitoba. Only one convicted computer criminal was identified, and refused to participate. The return rate for Alberta was 47% (28 returned out of 60).

In Manitoba, the probation department declined to participate despite a signed contract with the province. The probation department indicated that it could not identify the exact offence that individuals had been charged with. The Winnipeg Remand Center, and Milner Ridge Correctional Facility did agree to participate and 40 questionnaire packages were sent to these facilities. The completed sealed questionnaires were then sent by courier back to the University of Manitoba. For Manitoba, the return rate was 23% (9 returned out of 40).

At the end of the study each participating agency was provided with the results and information regarding the hypotheses and method.

Internet.

Internet participants used their web browser (Netscape, Internet Explorer), to connect to a web site

residing on a web server housed at the University of Manitoba Department of Psychology network. The web site had online versions of the CCISLQ, PDS, consent form and debriefing information (Appendixes K & L).

Once connected to the site, the participants were presented with a web page that briefly described the study and, if they consented to participate, they “clicked” on a hyper-link that took them to the CCISLQ and PDS online questionnaires. Once the participant has completed both surveys, a “submit” button posted the data to the database, and directed the browser to a debriefing page.

Once the answers from both questionnaires were posted to the database, a “cookie” was sent to the browser.[5] The submit action also assigned an unique participant ID number to the answers of both questionnaires and stored this information in the database for cross referencing the participants scores on the PDS with the CCISLQ. The data from the database was imported into Microsoft Excel and automatically scored. The PDS and CCISLQ scores were then imported into SPSS 10.0 for further statistical analysis.

---

[5] A “cookie” is small piece of code that the web server sends to the computer viewing the page. The code stays in memory and reports information back to the web server.

If a participant had successfully submitted their answers and attempted to participate again, the server would check the status of the “cookies” and if it found the “survey cookie,” would disallow them access to the site and present a message indicating they could not participate twice. The web server logs were examined to look for duplicate source IP addresses that would also indicate attempts to participate in study more than once.

No evidence was found to indicate any individuals had participated more than once. Due to the fact that the University of Manitoba Department of Psychology network did not have any monitoring software, no data relating to the number of people visiting the web page versus the total number participating was available.

Once the study was complete, the results were posted on the University of Manitoba Department of Psychology main web page.

All of the software used was open-source (non-commercial with no licensing restrictions). The various software used were: Linux Redhat 6.1 (operating system), Apache (web server), PHP 4.0 (scripting language), and MySQL (database). The server had the operating system hardened to reduce the risk of tampering.

For scoring purposes, the questionnaire answer sheets obtained from the participants were encoded with a participant number that adhered to the following coding scheme. The Internet participants were assigned a random eight-digit code, the convicted general criminals were assigned a non-random six digit code, with the first digit representing the geographical area (British Columbia=1, Alberta=2, and Manitoba=3).

Results

Data Exploration

Prior to analyses, the variables were examined through various SPSS programs for missing variables, and fit between their distributions and the assumptions of the various tests.

Phase One

Descriptive Statistics.

The first phase of the study was designed to compare various factors concerning computer and general criminals, including disposition, sentence, previous contacts, and social-demographics (i.e., age, sex, race, marital status, education). The frequency distributions for the gender, age, marital status, education, race, previous contact, and disposition are reported in Table 1.

Data were examined for 66 computer criminals (CC) and 66 general criminals (GC). The demographic data are reported in Table 2.

The general criminals (GC) and computer criminals (CC) were predominantly male (GC = 75.8%, CC = 81.8%), Caucasian (GC = 63.6%, CC = 72.7%), single (GC = 47%, CC = 56.7%), with high-school diplomas (GC = 33.3%, CC = 47.0%), and had no previous contact (GC = 31.8%, 34.8%).

Under the category of “Disposition” in Table 2, diversion refers to being diverted from the actual court system to some alternative program such as mediation services. In a conditional sentence the individual is given a specific sentence but avoids incarceration as long as they stay out of trouble for a specified period. Remand is basically time in custody. Prior to appearing before a judge or awaiting trial, an individual may be remanded into custody at an appropriate facility. During sentencing, the judge may take this time in custody into consideration. The other terms are self-explanatory.

Table 1

Social-demographic Characteristics of Computer Criminals and General Criminals

		Percentage (Frequency)	
		Computer Criminals	General Criminals
Gender	Male	81.8 (54)	75.8 (50)
	Female	18.2 (12)	24.2 (16)
	Total	100.0 (66)	100.0 (66)
Age	18-25	37.9 (25)	30.3 (20)
	26-35	31.8 (21)	36.4 (24)
	36-45	18.2 (12)	22.7 (15)
	Over 45	10.6 (7)	10.6 (7)
	Total	100.0 (66)	100.0 (66)
Marital Status	Single	56.1 (37)	47.0 (31)
	Married/ commonlaw	18.2 (12)	33.3 (22)
	Divorced/ Separated	13.6 (9)	15.0 (10)
	Widowed	1.5 (1)	0.0 (0)
	Unknown	10.6 (7)	4.5 (3)
	Total	100.0 (66)	100.0 (66)
Education	Elementary	1.5 (1)	6.1 (4)
	Grade 7-9	7.6 (5)	6.1 (4)
	Grade 10-11	18.2 (12)	30.3 (20)
	Grade 12	47.0 (31)	33.3 (22)
	Vocational	3.0 (2)	9.1 (6)
	University	4.5 (3)	1.5 (1)
	Unknown	18.2 (12)	13.6 (9)
	Total	100.0 (66)	100.0 (66)
Race	Caucasian	72.7 (48)	63.6 (42)
	Black	1.5 (1)	0.0 (0)
	Asian	10.6 (7)	1.5 (1)
	East Indian	0.0 (0)	1.5 (1)
	Native people	4.5 (3)	22.7 (15)
	Not Stated	10.6 (7)	10.6 (7)
	Total	100.0 (66)	100.0 (66)
Previous Criminal Contact	No Previous	34.8 (23)	31.8 (21)
	No previous time in Jail	10.6 (7)	19.7 (13)
	No Previous Jail Sentence	7.6 (5)	9.1 (6)
	Previous jail >2 yrs ago	12.1 (8)	15.2 (10)
	Previous Jail within 2 yrs	34.8 (23)	24.2 (16)
	Total	100.0 (66)	100.0 (66)
Disposition	Incarceration	21.2 (14)	24.2 (16)
	Probation	21.2 (14)	57.6 (38)
	Diversion	1.5 (1)	4.5 (3)
	Conditional Sentence	3.0 (2)	4.5 (3)
	Community Work	7.6 (5)	7.6 (5)
	Restitution	4.5 (3)	1.5 (1)
	Bail	9.1 (6)	0.0 (0)
	Remand	25.8 (17)	0.0 (0)
	Default Fine	6.1 (4)	0.0 (0)
	Total	100.0 (66)	100.0 (66)

Table 2

Descriptive Statistics: Age by Criminal Category

	Criminal Category	M	SD	N
Age	Computer	31.29	11.97	66
	General	32.20	10.23	66
Sentence (in days)	Computer	123.50	223.30	66
	General	265.76	220.67	66

Computer Criminal and General Criminal Comparison.

Gender by criminal category was examined for any significant differences using Fisher's Exact test. (The use of Fisher's exact test was necessary, as the comparison was on a 2 x 2 table with cell counts below 5 (Agresti & Finlay, 1997). No significant difference was found between CC and GC.

Race by criminal category, marital status by criminal category, education by criminal category, previous contact by criminal category, and disposition by criminal category, were analyzed using the Likelihood Ratio Chi Square test (see Table 3). The use of the Likelihood Ratio Chi Square was necessary as the computed tables had some cell counts less than five (Agresti & Finlay, 1997).

Table 3

Likelihood Ratio Chi-Square Tests: Social-demographics by Criminal Category

	Value	df
Race x Criminal Category[a]	13.06*	3
Marital Status x Criminal Category	5.95	4
Education x Criminal category	8.65	5
Previous Contact x Criminal Category	3.50	4
Disposition x Criminal Category[b]	6.91	5

[a]Black and East Indian groups combined to satisfy conditions of no cells having a count of 0.

[b]Bail, Remand, and Defaulted Fine removed as these relate to pre-sentencing.

*$p < .05$.

The analysis of disposition by criminal category did not use the categories of bail, defaulted fine, and remand. The cell counts with these categories was zero for GCs. These categories also related to pre-sentencing, which was not in the scope of this study. The categories of Black and East Indian were also combined to ensure that no expected cell counts equaled zero (Agresti & Finley, 1996).

The results indicated that race by Criminal Category (2 x 4 table) was significantly different between computer and general criminals, χ^2=(3, N = 132) = 13.06, p < .05 (see Table 4). The table indicated that there were significantly fewer Native people CCs, (adjusted residual = -2.9). The table also indicated that there were significantly more Asian CCs, (adjusted residual = 2.2). Cramer's phi was computed for the table, phi= .32. The shared variance was r^2 = .10 and the power of the test was .82.

Table 4

Cross Tabulation: Race by Criminal Category

			Criminal Category		
			Computer Criminal	General Criminal	Total
Race	Caucasian	Count	48.0	43.0	91.0
		Expected Count	45.5	45.5	91.0
		Adjusted Residual	1.1	-1.1	
	Black-East Indian	Count	1.0	1.0	2.0
		Expected Count	1.0	1.0	2.0
		Adjusted Residual	0.0	0.0	
	Asian	Count	7.0	1.0	8.0
		Expected Count	4.0	4.0	8.0
		Adjusted Residual	2.2*	-2.2*	
	Native People	Count	3.0	14.0	17.0
		Expected Count	8.5	8.5	17.0
		Adjusted Residual	-2.9*	2.9*	
Total		Count	59.0	59.0	118.0
		Expected Count	59.0	59.0	118.0

*p < .05.

Age by criminal category and sentence by criminal category data met the assumptions of homogeneity but did not meet the assumption of normality. Therefore, a 2-sample, non-parametric, Mann-Whitney test was conducted. The 2-tailed test showed a significant difference for sentence by criminal category, with general criminals receiving longer sentences than computer criminals (z = -4.90, p < .001) (See Table 5). The power of the t-test was .83.

Phases Two and Three

Missing Data.

Missing data on the PDS were corrected using adjusted means as per the PDS scoring guide (Paulhus, 1998). Twenty-four (15%) PDS questionnaires out of a total of 161 had missing data. There were 72 missing data points out of 11,840 on the social learning scales portion of the CCISLQ. Missing data were adjusted using the series mean technique contained in SPSS 10.0 (Tabachnick & Fidell, 1996; SPSS, 2000).[6]

---

[6] This technique replaces missing values with the mean for the entire series.

Table 5

Non-parametric Test: Age and Sentence by Criminal Category

	Mann-Whitney U	Wilcoxon W	Z
Age	1967.00	4178.00	-.96
Sentence in Days	1112.00	3323.00	-4.90**

**p < .001.

Descriptive Statistics.

The demographics of the Internet and GC participants' age, gender, marital status, and education are presented in Table 6.

With respect to gender, 74.1% of Internet subjects were males, and 24.1% females, while for GC, 91.7% were males and 5.6% females. The majority of the Internet and GC respondents were single (Internet = 55.4%, GC = 47.2%). Almost two-thirds (62.5%) of the Internet participants had an undergraduate or graduate degree, and 75% of the GCs had high school education. Just over one-third (35.7%) of the Internet participants and 47.2% of the GCs were between 18-25 years of age.

Some additional demographic information was collected for the Internet participants. More than half (58.9%) of the Internet participants indicated their knowledge of the Internet was at the expert level, and 58.0% reported they had a moderate knowledge of computer crime laws. 57.1% of the Internet participants reported they worked in the IT field. The second most reported occupation was student or academic at 31.3%.

Table 6

Demographics: Internet and General Criminals

		Percentage (Frequency)	
		Internet	General Criminals
Gender	Male	74.1 (83)	91.7(33)
	Female	24.1 (27)	5.6 (2)
	Missing	1.6 (2)	2.8 (1)
	Total	100.0(112)	100.0(36)
Age	Under 18	7.1 (8)	5.6 (2)
	18-25	35.7 (40)	47.2(17)
	26-35	31.3 (35)	19.4 (7)
	Over 35	25.0 (28)	25.0 (9)
	Missing	0.9 (1)	2.8 (1)
	Total	100.0(112)	100.0(36)
Marital Status	Single	55.4 (62)	47.2(17)
	Married/ commonlaw	36.6 (41)	41.7(15)
	Divorced/ Separated	7.1 (8)	5.6 (2)
	Widowed	0.0 (0)	2.8 (1)
	Missing	0.9 (1)	2.8 (1)
	Total	100.0(112)	100.0(36)
Education	Some High school	4.5 (5)	38.2(13)
	High School	17.0 (19)	41.2(14)
	Diploma-Cert	15.2 (17)	17.6 (6)
	Degree	36.6 (41)	0.0 (0)
	Graduate Degree	25.9 (29)	2.9 (1)
	Missing	0.9 (1)	5.6 (2)
	Total	100.0(112)	100.0(36)
Internet Knowledge	Beginner	2.7 (3)	
	Intermediate	38.4 (43)	
	Expert	58.9 (66)	
	Total	100.0(112)	
Law Knowledge	Limited	16.1 (18)	
	Moderate	58.0 (65)	
	Expert	25.9 (29)	
	Total	100.0(112)	
Occupation	Not Stated	2.7 (3)	
	IT Field	57.1 (64)	
	General Business	4.5 (5)	
	Student/Academic	31.3 (35)	
	Student High school	2.7 (3)	
	Legal	0.9 (1)	
	Other	0.9 (1)	
	Total	100.0(112)	

Demographics: Sample vs. Population.

The sample to population demographics for both the Internet and general criminals indicated that they were similar, suggesting that the participants in the study were a representative sample (see Table 7).

Demographics: Criminal Computer Activity and No-criminal Activity.

The participants were further categorized based on their scores on the crime index scale. General criminal and Internet participants who reported any criminal computer behavior other than piracy on the Crime Index scale (score > 0) were categorized as criminal computer activity (CCA). If no criminal activity was reported (score = 0), the participant remained classified as Internet no criminal activity (NCA) or General Criminal (GC). Demographics of the CCA and NCA participants are reported in Table 8.

Table 7

Sample vs. Population Demographics

	General Criminal		Internet	
Category	Population[b]	Sample	Population[c]	Sample
Male	97.0	91.7	64.0	74.1
Female	3.0	5.6	36.0	24.1
Age 20-34[a]	49.0	66.0	45.0	67.0

Note. Numbers represent percentages.

[a]Approximate number for sample as this encompassed 2 ranges 18-25 and 26-35.

[b]Source: Corrections Canada (1999).

[c]Source: CommerceNet (CN) Research Center (2000). CN is a not-for-profit research organization that tracks Internet demographics. CN's affiliates include Stanford University, MIT, and University of California, Berkley.

Table 8

Demographics: Computer Criminal Activity by No Criminal Activity

		Percentage (Frequency)	
		CCA	NCA
Gender	Male	59.6(53)	75.0(30)
	Female	19.1(17)	25.0(10)
	Missing	21.3(19)	0.0 (0)
	Total	100.0(89)	100.0(40)
Age	Under 18	9.0 (8)	0.0 (0)
	18-25	33.7(30)	25.0(10)
	26-35	27.0(24)	27.5(11)
	Over 35	11.2(10)	45.0(18)
	Missing	19.1(17)	2.5 (1)
	Total	100.0(89)	100.0(40)
Marital Status	Single	51.7(46)	40.0(16)
	Married/ commonlaw	24.7(22)	47.5(19)
	Divorced/ Separated	3.4 (3)	12.5 (5)
	Widowed	0.0 (0)	0.0 (0)
	Missing	20.2(18)	0.0 (0)
	Total	100.0(89)	100.0(40)
Education	Some High school	5.6 (5)	0.0 (0)
	High School	16.9(15)	10.0 (4)
	Diploma-Cert	9.0 (8)	22.5 (9)
	Degree	29.2(26)	37.5(15)
	Graduate Degree	20.2(18)	27.5(11)
	Missing	19.1(17)	2.5 (1)
	Total	100.0(89)	100.0(40)

Note. CCA = Criminal Computer Activity, NCA = No Criminal Activity.

Over half (59.6%) of the CCA participants and 75% of the NCA that reported their gender were males, while 19.1% of the CCA and 25% of the NCA were females. Half (51.7%) of the CCA were single and 47.5% of NCA were married/commonlaw. 49.4% of the CCA and 65% of the NCA had undergraduate or just over one-third (33.7%) of the CCA were between 18-25 years of age, and 45% of the NCA were over 35 years of age.

The frequency distributions of the participants' number of years interested in computers, ownership, operating system, experience, and online hours are reported in Table 9. In general, the majority of the participants had been interested in computers for four or more years, owned their own computer, used Windows as an operating system, were experienced users, and were online more than 15 hours per week.

Table 9

Additional Demographics: Criminal Computer Activity and No Criminal Activity

		Percentage (Frequency)	
		CCA	NCA
Interested	NA	3.4 (3)	0.0 (0)
	1yr	2.2 (2)	2.5 (1)
	2 yrs	2.2 (2)	5.0 (2)
	3 yrs	10.1 (9)	7.5 (3)
	More than 4	82.0(73)	82.5(33)
	Missing	0.0 (0)	2.5 (1)
	Total	100.0(89)	100.0(40)
Ownership	Self or Family	56.2 (50)	47.5(19)
	Friend	3.4 (3)	0.0 (0)
	School	7.9 (7)	7.5 (3)
	Employer	29.2(26)	45.0(18)
	Other	3.4 (3)	0.0 (0)
	Total	100.0(89)	100(40)
Operating System	NA	4.5 (4)	0.0 (0)
	DOS	5.6 (5)	5.0 (2)
	Windows/NT	50.6(45)	62.5(25)
	Macintosh	7.9 (7)	2.5 (1)
	Unix-Linux-BSD	30.3(27)	30.0(12)
	Missing	1.1 (1)	0.0 (0)
	Total	100.0(89)	100.0(40)
Experience	Novice	2.2 (2)	5.0 (2)
	Intermediate	44.9(40)	40.0(16)
	Expert	52.8(47)	55.0(22)
	Total	100.0(89)	100.0(40)
Online Hours	Less than 5	22.5(20)	22.5 (9)
	5-10 hrs	20.2(18)	20.0 (8)
	10-15 hrs	12.4(11)	15.0 (6)
	More than 15	44.9(40)	40.0(16)
	Missing	0.0 (0)	2.5 (1)
	Total	100.0(89)	100.0(40)

Note. CCA = Criminal Computer Activity, NCA = No Criminal Activity.

Frequency and Prevalence of Computer Crime.

Approximately 60% of all the participants admitted to engaging in some form of criminal computer behavior (89 out of 148 participants). The specific frequencies of each of the categories admitted to is reported in Table 10. In general, the frequency of criminal activities engaged in over the last three years decreased as the seriousness of the activity increased. The most frequent activity was piracy (a minimum of 495 incidents), and the next most frequent was password guessing (379). The least frequent activity was possession of, or obtaining credit card numbers (54).

The prevalence of criminal computer activity is presented in Table 11. The most prevalent criminal computer activity over the lifetime period was browsing someone else's files without permission (75% admitted to having engaged in this activity), software piracy was second (70%), and obtaining credit card numbers was least prevalent (17%).

Table 10

Frequency and Incidence of Computer Activity in the Past Three Years

	Never	1-2 Times	3-5 Times	6-9 Times	10 Times or more	Minimum No. of incidents
Piracy	41.9 (62)	14.2 (21)	13.5(20)	6.1 (9)	24.3 (36)	(495.0)
Password Guessing	53.4 (79)	15.5 (23)	8.1(12)	3.4 (5)	19.6 (29)	(379.0)
Browse	52.7 (78)	16.2 (24)	10.8(16)	4.1 (6)	16.2 (24)	(348.0)
Change files	73.6(109)	11.5 (17)	2.7 (4)	1.4 (2)	10.8 (16)	(201.0)
Passwords Use-Traffic	76.4(113)	9.5 (14)	5.4 (8)	0.7 (1)	8.1 (12)	(164.0)
Virus	81.8(121)	8.8 (13)	4.1 (6)	2.7 (4)	2.7 (4)	(95.0)
Phone	85.1(126)	6.8 (10)	5.4 (8)	0.7 (1)	2.0 (3)	(70.0)
Credit Card	88.5(131)	6.8 (10)	1.4 (2)	2.0 (3)	1.4 (2)	(54.0)

Note. Number of cases in parentheses.

Table 11

Prevalence of Criminal Computer Activities

	Never	Past Month	Past Year	1-4 yrs ago	5yrs or more	Lifetime
Browse	15.7 (14)	37.1 (33)	22.5 (20)	21.3 (19)	3.4 (3)	84.3 (75)
Piracy	21.3 (19)	34.8 (31)	23.6 (21)	12.4 (11)	7.9 (7)	78.7 (70)
Password Guessing	24.7 (22)	38.2 (34)	27.0 (4)	9.0 (8)	1.1 (1)	75.3 (67)
Change files	55.1 (49)	18.0 (16)	12.4 (11)	11.2 (10)	3.4 (3)	44.9 (40)
Passwords Use-Traffic	58.4 (52)	16.9 (15)	12.4 (11)	7.9 (7)	4.5 (4)	41.6 (37)
Virus	66.3 (59)	7.9 (7)	11.2 (10)	12.4 (11)	2.2 (2)	33.7 (30)
Phone	66.3 (59)	4.5 (4)	11.2 (10)	5.6 (5)	12.4 (11)	33.7 (30)
Credit Card	80.9 (72)	5.6 (5)	4.5 (4)	6.7 (6)	2.2 (2)	19.1 (17)

Note. Number of cases in parentheses.

An examination of the instances of criminal computer behavior and age indicated that for all eight categories, the majority of the criminal activity occurred at 16 years or less (see Table 12).

Formal Hypotheses Testing

Hypothesis One: Differential Association and Differential Reinforcement.

Hypothesis one was tested by multivariate analysis of variance (MANOVA) performed on the two dependent variables (DV) (differential association scores-DA and differential reinforcement scores-DR). The Independent variable (IV) was criminal category (criminal computer activity-CCA, and non-criminal-NCA).

SPSS MANOVA was used for the analysis. The total *N* was 129. Results of the evaluation of assumptions of normality, homogeneity of variance-covariance matrices, linearity and multicollinearity were satisfactory.

Scores on the IM, SDE and Total of the PDS were examined as possible covariates, but did not meet the criteria of being sufficiently correlated with the two DVs ($r > .20$) (Keppel & Zedeck, 1989) (See Table 13). The descriptive statistics are reported in Table 14.

Table 12

Criminal Activity by Age

	Never	16yrs or less	17-18 yrs	19-20 yrs	21 yrs or older
Piracy	15.7 (14)	44.9 (40)	11.2 (10)	2.2 (2)	25.8 (23)
Password Guessing	20.2 (18)	30.3 (27)	13.5 (12)	7.9 (7)	28.1 (25)
Password Use-Traffic	55.1 (49)	15.7 (14)	10.1 (9)	4.5 (4)	14.6 (13)
Browse	20.2 (18)	24.7 (22)	12.4 (11)	10.1 (9)	32.6 (29)
Change Files	52.8 (47)	19.1 (17)	7.9 (7)	5.6 (5)	14.6 (13)
Virus	61.8 (55)	14.6 (13)	6.7 (6)	3.4 (4)	7.9 (7)
Credit Card	79.8 (71)	10.1 (9)	3.4 (3)	1.1 (1)	5.6 (5)
Phone	65.2 (58)	15.7 (14)	7.9 (7)	5.6 (5)	5.6 (5)

Note. Number of cases in parentheses.

Table 13

Pearson Correlation: PDS by Category by Social Learning Measures

	Criminal Category	DA	DR	MD	IM	SDE	PDS Total
Criminal Category	1.00	.53	.20	.41	-.11	-.39	-.31
DA		1.00	.56	.36	-.04	-.30	-.12
DR			1.00	.45	.03	.15	-.10
MD				1.00	-.00	.30	-.20
IM					1.00	.33	.78
SDE						1.00	.85
PDS Total							1.00

Note. DA = Differential Association, DR = Differential Reinforcement, MD = Moral Disengagement, SDE = Self-deceptive Enhancing, PDS Total = Paulhus Deception Scale total

Table 14

Descriptive: Social Learning Measures by Criminal Category

	Criminal Category	M	SD	n
Differential Association	NCA	4.90	1.69	40
	CCA	6.48	2.24	89
	Total	5.99	2.21	129
Differential Reinforcement	NCA	96.69	15.73	40
	CCA	104.18	17.18	89
	Total	101.86	17.04	129

Note. CCA = Criminal Computer Activity, NCA = No Criminal Activity.

With the use of Wilks' criterion, the combined dependent variables of DA and DR were significantly affected by category of offender $F(2, 126) = 7.85$, $p < .001$. The power of the test was determined to be .95. The results reflect a medium association between criminal category and the combined DVs, $\eta^2 = .11$ (see Table 15).

To investigate the impact of each main affect on the individual DVs, post hoc univariate analyses were performed (see Table 16). The analysis revealed that the CCA group showed significantly higher scores on DA than the NCA group ($M = 6.47$ vs. $M = 4.90$), $F(1, 127) = 15.75$, $p < .001$). There was a medium association between criminal category and DA, $\eta^2 = .11$, and the reported power was .98. The analysis further indicated that the CCA group showed significantly higher scores on DR than the NCA group ($M = 104.19$ vs. $M = 96.69$, $F(1, 127) = 5.53$, $p < .05$). There was a small association between criminal category and DR, $\eta^2 = .04$, with the reported power being .65.

Table 15

Mulivariate Tests: Criminal Category by Social Learning Measures

	Value	*df*	*F*	η^2
Wilks' Lambda	.89	2, 126	7.85**	.11
Hotelling's trace	.13	2, 126	7.85**	.11

**$p < .001$.

Table 16

Comparison of Social Learning Measures by Criminal Category

Source		df	SS	MS	F	η^2
DA	Between Groups	1	68.75	68.75	15.75**	.11
	Within Groups	127	554.42	4.37		
DR	Between Groups	1	1550.69	1550.69	5.53*	.04
	Within Groups	127	35604.46	(280.35)		

*p < .05. ** p < .001.

Hypothesis Two: Moral Disengagement.

Hypothesis two was tested using an analysis of covariance (ANCOVA) on one DV (moral disengagement measure-MD), one concomitant DV (SDE), and one IV (criminal computer activity-CCA, and non-criminal-NCA). The data met the assumptions of normality, independence, equality of variance, correlations, and homogeneity of regression.

SDE was found to be negatively correlated with moral disengagement, r = -.30, and the criminal category, r = -.39. According to Keppel & Zedeck (1989), the correlations were sufficient to allow SDE to be considered as a covariate. SDE was also examined for its affects as a mediator-moderator, but did not meet the criteria (Baron & Kenny, 1986).

The descriptive statistics for the moral disengagement measure and criminal category are reported in Table 17. The results of the analysis of MD and criminal category are reported in Table 18.

Table 17

Descriptive: Moral Disengagement by Criminal Category

	Criminal Category	M	Adjusted M[a]	SD	n
Moral Disengagement	NCA	28.00	28.76	6.33	40
	CCA	35.03	34.69	7.63	89
	Total	32.85		7.93	129

Note. CCA = Criminal Computer Activity, NCA = No Criminal Activity.

[a]Evaluated as covariates appeared in the model:

SDE = 7.28.

Table 18

Analysis of Covariance Self-deceptive Enhancing by Moral Disengagement by Criminal Category Between Subjects Effects

Source	df	Adjusted SS	MS	F
Between Groups	1	826.04	826.04	16.00**
Within Groups	126	6504.04	51.2	

**p < .001.

The analysis revealed that the CCA group showed significantly higher scores on the MD measure than the NCA group (M = 34.69 vs. M = 28.76, $F(1, 126) = 16.00$, $p < .001$). The effect size was considered medium, R^2 = .11, and the observed power of the test was .98.

Hypothesis Three: Predictive Model.

Hypothesis three was tested using a binomial logistic regression analysis with one DV, criminal category (criminal computer activity-CCA, and no criminal computer activity-NCA), and three IVs (differential association-DA, differential reinforcement-DR, and moral disengagement-MD).

Due to the fact that the study is exploratory, a backward stepwise Wald procedure was used (see Table 18)(Menard, 1996). The data were explored, and met the assumptions for the test. The results indicated that only two variables out of the three tested were significant, DA, (W = 6.73, $p < .05$), and MD, (W = 12.76, $p < .001$) (see Table 20).

Table 19

Backward Stepwise (Wald) Omnibus Tests of Model Coefficients and Model Summary

		χ^2	*df*	-2 Log Likelihood
Step 1	Step	32.75**	3	
	Block	32.75**	3	
	Model	32.75**	3	126.99
Step 2	Step	-1.34	1	
	Block	31.42**	2	
	Model	31.42**	2	128.33

**$p < .001$.

Table 20

Variables in Equation: Backward Stepwise Wald Procedure

							95% C.I for Exp(B)	
		B	S.E	Wald	df	Exp(B)	Lower	Upper
Step 1	DA	.39	.14	7.70*	1	1.48	1.12	1.96
	DR	-.02	.02	1.31	1	.98	.95	1.01
	MD	.13	.04	13.18**	1	1.14	1.06	1.22
	Constant	-3.60	1.44	6.22*	1	.03		
Step 2	DA	.32	.12	6.73*	1	1.38	1.08	1.75
	MD	.12	.03	12.76*	1	1.12	1.05	1.20
	Constant	-4.63	1.15	16.38**	1	.01		

Note. DA = Differential Association, DR = Differential Reinforcement, MD = Moral Disengagement.

*p < .05. **p < .001.

The analysis further indicated that the model including only the two variables of DA and MD fit the data well as the Hosmer and Lemeshow test was non-significant at α = .05. The model DA & MD, reduced the error of classification by 40%, (τ_p = .40). The model also had good prediction at 74.4% (see Table 21).

Additional Data Analyses

Multiple Regression Correlation Analysis of Crime Index and Social Learning Measures.

To explore the data further, a multiple regression correlation analysis (MRC) was conducted. The choice of an MRC was based on Keppel & Zedeck (1986), who concluded that MRC might be a more appropriate analysis method for non-experimental designs than ANOVA based methods.

There were six social learning measure IVs (imitation-IMT, differential association-DA, differential reinforcement-DR, moral disengagement-MD, and definitions-DF), and one PDS IV (Total-PDS Tot). PDS total was chosen over SDE because it captured both IM and SDE scores. The DV was raw crime index scores. Raw scores were used to explore any possible effects that the degree of criminal

Table 21

Classification Table

Observed		Predicted		
		Criminal Category		Percentage Correct
		NCA	CCA	
Criminal Category	NCA	19	21	47.5
	CCA	12	77	86.5
Overall Percentage				74.4

Note. NCA = No Criminal Activity, CCA = Criminal Computer Activity.

involvement of the participants might have. Data from all the criminal categories were included. The total N was 148.

The descriptive statistics are reported in Table 22. The analysis indicated that the model containing definitions and differential association formed the best predictive model, $F(2, 145) = 68.08$, $p < .001$. This model accounted for 48% of the variability, $R^2 = .48$ (see Table 23).

MANCOVA Criminal Categories by Social Learning Measures.

Further analysis was conducted to examine the differences if any between CC and GC. The data were tested by multivariate analysis of covariance (MANCOVA) performed on the three dependent variables (DV) (differential association scores-DA, differential reinforcement scores-DR, and moral disengagement scores -MD) and one covariate (DV) SDE. The Independent variable (IV) was criminal category (criminal computer activity-CCA, non-criminal-NCA, and general criminal-GC). The total N was 148.

The data were evaluated for assumptions of normality, homogeneity of variance-covariance matrices, linearity and multicollinearity. The assumption of homogeneity of

Table 22

Descriptive: Crime Index and CCISLQ Measures

	M	SD
Crime Index	12.20	15.77
Imitation	12.65	4.61
Differential Association	5.77	2.20
Differential Reinforcement	100.50	18.47
Moral Disengagement	32.47	8.36
Definitions	12.30	5.25
PDS-Tot	10.96	6.22

Note. PDS-Tot = Paulhus Deception Scale total score.

Table 23

Stepwise Multiple Regression Analysis: Variables Predicting Crime Index Scores

Variable	*B*	*SE B*	*β*
Step 1			
Definitions	2.01	.18	.67**
Step 2			
Definitions	1.62	.22	.54**
Differential Association	1.61	.52	.23*

Note. R^2 = .45 after step 1; R^2 = .48 after step 2 ($p < .05$).

*$p < .05$. **$p < .001$.

variance was violated at the α = .05 level for DR. There were also unequal sample sizes (CCA = 89, NCA = 40, and GC = 19), but the ratio between the largest and the smallest variance was smaller than the limitation of 10:1. Two-tailed MANCOVA is fairly robust to violations of homogeneity of variance, but due to the fact that the GC sample was both the smallest and displayed the greatest variance, α = .001 was used to control for Type I error (Tabachnick & Fidell, 1996). According to Tabachnick & Fidell (1996), adjusting the α also was necessary as the ratio of smallest sample to largest sample was greater than 4:1. The descriptive statistics are reported in table 24.

With the use of Wilks' criterion, the combined dependent variables of DA, DR, and MD were significantly affected by category of offender $F(6, 284) = 6.29$, $p < .001$. The power of the test was determined to be .96. The results reflect a medium association between criminal category and the combined DVs, $\eta^2 = .12$ (see Table 25).

Table 24

Descriptive: Social Learning Measures by All Criminal Categories

	Criminal Category	M	Adjusted M[a]	SD	n
Differential Association	NCA	4.90	4.87	1.69	40
	CCA	6.48	6.49	2.24	89
	GC	4.32	4.34	1.57	19
	Total	5.77		2.20	148
Differential Reinforcement	NCA	96.69	98.00	15.73	40
	CCA	104.18	103.81	17.18	89
	GC	91.24	90.22	24.85	19
	Total	100.50		18.47	148
Moral Disengagement	NCA	28.00	29.04	6.33	40
	CCA	35.03	34.74	7.63	89
	GC	29.85	29.04	10.72	19
	Total	32.47		8.36	148

Note. NCA = No Criminal Activity, CCA = Criminal Computer Activity, GC = General Criminal.

[a]Evaluated as covariates appeared in the model:

SDE = 6.98.

Table 25

Mulivariate Tests: All Criminal Categories by Social Learning Measures

	Value	*df*	*F*	η^2
Wilks' Lambda	.78	6, 284	6.29**	.12
Hotelling's trace	.28	6, 282	6.55**	.12

**$p < .001$.

The univariate tests indicated that there was a main effect for DA, ($F(2, 144) = 13.70$, $p < .001$, $\eta^2 = .16$, power = .93), and for MD, ($F(2, 144) = 9.33$, $p < .001$, $\eta^2 = .12$, power = .74). DR showed no significant main effect at $\alpha = .001$ level (see Table 26).

A post hoc multiple comparison procedure (MCP) was conducted using a Bonferroni correction for Type I error. The MCP indicated that for differential association-DA, CCA scored significantly higher than the NCA group ($M = 6.49$ vs. $M = 4.87$, CI = -3.15, -8.20E-02, $p < .001$) and the GC group ($M = 6.49$ vs. $M = 4.34$, CI = .24, 4.06, $p < .001$). There was no significant difference between NCA and GC. There was also no significant difference at $\alpha = .001$ level between the categories on DR or MD.

Table 26

Univariate Tests: All Criminal Categories by Social Learning Measures

Source		df	Adjusted SS	MS	F	η^2
Differential Association	Between Group	2	113.85	56.93	13.70**	.16
	Within Group	144	598.30	(4.16)		
Differential Reinforcement	Between Group	2	3233.25	1616.62	5.04	.07
	Within Group	144	46214.85	320.94		
Moral Disengagement	Between Group	2	1093.50	546.75	9.33**	.12
	Within Group	144	8437.68	58.60		

**$p < .001$.

Discussion

The present study attempted to shed light on criminal computer behavior in today's society. The current study included participants from several different populations: convicted computer criminals, general criminals, and the Internet based general public. Because of a lack of previous research using these populations together, this study was exploratory and only scratched the surface of this research area. The primary areas of focus of the study were the identification of social-demographic variables unique to computer criminals as opposed to criminals in general, and the identification of variables that might influence the initial involvement in and subsequent continuation of criminal computer behavior.

Two of the three hypotheses were supported by the results. The first hypothesis that individuals who had engaged in criminal computer activity would have higher levels of differential association and differential reinforcement than the individuals who had no criminal activity was supported. The second hypothesis that individuals who had engaged in criminal computer activity would have higher rates of moral disengagement than individuals who had no criminal activity was also

supported. The third hypothesis that the combination of the three variables of moral disengagement, differential association, and differential reinforcement would better predict illicit computer behavior than any one variable alone was not supported.

The current study incorporated a web-based approach both for recruiting some of the participants and for actual participation. This design had several advantages. Psychology has been criticized, perhaps unfairly, as being the study of white North American college sophomores (Krantz & Dalal, 2000). Web-based studies using the Internet overcome this criticism, as the study is now potentially open to the world, or at least that segment of the population that has access to the Internet (Krantz & Dalal, 2000). Another advantage is that the demographics of Internet users are very quickly approaching the demographics of the general population, which may allow for more accurate generalization of findings from research (Reips, 2000).

However, with the use of web-based research, questions regarding validity arise. Studies which have looked at the validity of web based psychological research have focused on the validity of the method. The two primary ways to establish this type of validity are: comparison of results

from web-based research to laboratory-based research, and examining the research to determine whether the results follow theoretically predicted trends (Krantz & Dalal, 2000). Several studies following these criteria have concluded that, in general, web-based studies have sufficient validity to be a viable research tool (Krantz & Dalal, 2000; Reips, 2000). Other research also has concluded that web-based studies access the same psychological variables as laboratory studies (Krantz & Dalal, 2000; Reips, 2000). Krantz and Dalal (2000) indicated that in their research, lab and Internet samples correlated at .94. Despite these findings, the web remains a powerful tool for research that tends to be under-used by psychological researchers.

Birnbaum (2000) identified two additional pitfalls of web-based studies, sampling and control. The current study was sensitive to these problems and included extra social-demographic questions for the Internet participants. The Internet participant social-demographics were then compared to the known demographics of the Internet population. These participants were considered to be representative. For the present study, control of conditions was not a significant problem since it was survey-based with no experimental manipulation.

Social-demographics

The social demographic comparison of convicted computer and general criminals indicated that, apart from race, there were no significant differences between the two groups. The fact that Native People were under-represented in the criminal computer group is not surprising. One of the unique aspects of criminal computer behavior is access to or availability of the technology. Social economic status (SES) is a possible factor in this type of crime, as computers and access to the Internet can be costly (Sacco & Zuriek, 1990). Although efforts have been made in both Canada and the United States to provide Internet access to all citizens through public terminals, these efforts have met with minimal success. Native People in Canada tend to aggregate in the lower to middle sector of the SES continuum, and would have less access to the technology required to commit these types of crimes.

The social-demographics comparison also indicated that Asians were over-represented. Here again, SES may play a role. However, caution should be exercised in making any sweeping generalizations as the data were obtained from the province of B.C. only and may not be representative of all of Canada.

The finding that age, education, or marital status was not significantly different is interesting. The common profile of computer criminals is that they are Caucasian, male, and 12-28 years old (Denning, 1998; Parker, 1998; Rogers, 1999a). This profile appears to be more of a generic criminal profile and, as the current results indicate, it tells us nothing unique about computer criminals (Rogers, 1999a). It is speculated that the inclusion of young offenders (ages 11-18) in subsequent studies will more clearly identify any differences in age. Young offenders were not part of the present study due to legal restrictions on young offender data in Canada.

It was observed that general criminals received significantly longer sentences than computer criminals, despite the fact that they are both dual procedure offences (i.e., the Crown can proceed by way of summary conviction or indictable offence). The sentencing guidelines are similar for these offences, yet general criminals tended to receive more severe punishments than computer criminals. This may be related to the fact that judges and Crown attorneys (dual procedure cases are rarely heard by a jury) still see computer crimes as less severe and less harmful to victims than traditional crimes (e.g., theft, assault,

break and enter) (Davis & Hutchinson, 1999; Parker, 1998; Schwartau, 1994).

Computer Crime Activities

The finding that 60% of all the participants admitted to engaging in criminal computer activities illustrates the extent of this criminal behavior. The prevalence may be due in part to the unique morality surrounding this type of criminal activity. As both Spafford (1997) and Denning (1998) indicated, the ethical boundaries of technology seem to be at odds with ethical standards found in the real physical world. Many people feel that because they are not dealing with tangible items (e.g., virtual files as opposed to real property), the ethical considerations relating to personal property and privacy in the “real” world do not apply in the “cyber” world. This flexible morality allows people to engage in behaviors in the “cyber” world that they probably would avoid in the real world (e.g., invasion of privacy, break and enter, theft).

Ethics, or an apparent lack thereof, has become such a concern that there have been several heated debates surrounding this issue in the information technology sector. These debates have centered around the inclusion of

courses on ethics as a requirement in the curriculum of computer science and engineering programs (Spafford, 1997).

The present study found that, as the perceived severity of the criminal activity increased, the frequency of these activities decreased. Both the current study and Skinner and Fream (1997) found that the most frequent activity was software piracy, and that the second most frequent was password guessing. Most people consider software piracy and password guessing as relatively harmless activities (Denning, 1998; Parker, 1998). In the current study, obtaining or possessing credit card numbers (the most severe of the listed activities) was the least frequent activity and had the lowest lifetime prevalence rate.

The observed severity trend may be influenced by moral disengagement. According to Bandura (1990b), it would take less effort for people to rationalize and justify perceived minor deviant behavior than more serious behavior. As the perceived severity of the behavior increases, the individual would have to exert more effort to rationalize engaging in the behavior. Thus, the frequency of behaviors perceived as more severe would be lower (Bandura, 1990b).

The fact that most of the criminal computer activity occurred when the participants were 16 years of age or less appears to support the theory that criminal computer

activity is more common among youths and young adults than with older people (Parker, 1998; Sacco & Zuriek, 1990). This may be due to the fact that the Internet and the personal computer are artifacts of the last decade or so. The World Wide Web, which has popularized the Internet, has only been in existence since approximately 1990, and public access to the Internet has only been practically available for the last five years. As a result, members of the younger generation tend to be more familiar and more comfortable with the technology and the medium. This familiarity and understanding may result in the younger generation being more active in deviant behavior that relies on technology (Parker, 1998; Skinner & Fream, 1997).

Although not the focus of the current study, the operating system preferences and perceived level of computing expertise of the participants provided some interesting observations. The study found that Microsoft Windows/NT was the most used operating system for all participants and that the majority considered themselves to be at the expert level of experience with computers. This is contrary to the stereotype of computer criminals as “super users” with more expertise in Unix or Unix-like operating systems than typical users (Denning, 1998). It appears that, at least for the current study, operating

system preference and level of expertise are not significant factors.

Based on the results, there appeared to be no significant difference between the criminal computer activity and no criminal activity groups with regard to the number of hours spent online. The majority of all the participants spent in excess of 15 hours per week online. Caution should be exercised when interpreting the results here, as the maximum category of more than 15 hours may represent too low a number for meaningful comparison (i.e., a ceiling effect). Before any conclusions can be drawn, it would be necessary to include additional categories (e.g., 16-20, 21-25, 26-30). Studying the amount of hours an individual is online is important. Excessive online hours may indicate problems associated with an addiction, which has been hypothesized as a causal factor for some computer related crimes (Duff & Gardener, 1996).

Differential Association and Differential Reinforcement

Studies have found that differential association and differential reinforcement were positively correlated with certain types of deviant behavior (e.g., drugs, alcohol abuse, computer deviance)(Akers, 1977; Akers, 1998; Akers et al., 1979; Skinner & Fream, 1997). The present study

supported these findings. The results indicated that individuals who self-report criminal computer activity had significantly higher rates of differential association and differential reinforcement than participants who had never engaged in criminal activity.

The structure of the computer underground itself may be partially responsible for the high rates of differential association and differential reinforcement. Studies have indicated that individuals involved in criminal computer behavior associate with other computer criminals either virtually through chat channels or news groups, or physically by way of conferences and conventions (Chandler, 1996; Taylor, 1997). The high degree of association may be due to the fact that these individuals rely on their membership in the “hacker” community in order to hone their skills and to keep abreast of new techniques and potential targets (Adamski, 1999; Taylor, 1997).

Mentoring is common within the hacking community and encouraged within the computer underground (Adamski, 1999; Taylor, 1997). Older, more experienced individuals share with novices their knowledge, techniques, views, and definitions of what is appropriate and inappropriate. This mentoring environment is the type of social learning environment that Akers described in his theory, as the

foundation upon which the other social learning variables interact (Akers, 1998).

Moral Disengagement

The moral disengagement questionnaire that the current scale was derived from was originally designed to be used with studies on aggression with the child participants and had never been tested on adults (A. Bandura, personal communications, February 2000). For the current study the questionnaire had been adapted for use with criminal behavior and adult participants. As such the focus was on measuring only the four major points in the self-regulatory system (e.g., reconstruing the conduct, obscuring personal causal agency, misrepresenting or disregarding the injurious consequences, and vilifying the victims). It did not include a comprehensive measure of each of the eight sub-concepts that Bandura et al. (1996) posited as operating under these four major points (e.g., diffusion of responsibility). The sample size for the current study was small which could have negatively impacted on the power of the tests to accurately identify significant small to medium effects. Due to these constraints a more detailed analyses of moral disengagement was not conducted.

In the present study, participants who self-reported computer criminal behavior had significantly higher rates of moral disengagement than non-criminal participants. This finding supported the results of studies on deviance, terrorism and aggression. Bandura (1990b) indicated that moral disengagement is an important mechanism for certain criminal actors such as terrorists to possess. Individuals who use moral disengagement are more able to justify and rationalize their deviant activities, thus continuing the behavior (Bandura, 1990b). However, the fact that we are dealing with a criminal activity would in and of itself lead us to expect a significant difference on moral disengagement (Sherizen, 1997). Without further study it is impossible to determine if the difference is a result of computer activity as well.

Self-deceptive enhancing (SDE) was initially believed to have some impact on the CCISLQ scores. The data analysis confirmed that SDE was associated with moral disengagement and therefore had to be controlled. The correlation of SDE to moral disengagement makes intuitive sense. SDE represents an unconscious bias that is related to narcissism (Paulhus, 1998). Narcissistic individuals tend to believe the world revolves around them and are often unaware of, or are not interested in, the impact their

actions have on anyone else (Emmons, 1987). This characteristic is also one of the mechanisms of moral disengagement, namely the disregarding of consequences (Bandura et al., 1996). Individuals who score high on SDE also have a pervasive lack of insight and are self-deceiving (Paulhus, 1998). Self-deception is an aspect of moral disengagement as well (Bandura, 1990b). The process of rationalizing and justifying deviant behavior requires that people deceive themselves about certain aspects of their actions (e.g., impact on the victim, seriousness of the activity). However, Bandura (1990a) did caution about whether deception could ever truly be completely unconscious.

Predictive Model

Although exploratory, the present study was concerned with developing a foundation for determining which variables, or combinations of variables, might be significant in predicting criminal computer behavior. Since no previous research had looked at this question, a logical model to begin with incorporated the variables that had been hypothesized as significant (i.e., differential association, differential reinforcement, and moral disengagement). The results indicated that of the

variables tested, only differential association and moral disengagement were significant for predicting who engaged in criminal computer activity. Differential reinforcement was not a significant variable. The finding is contrary to the conclusions of both Skinner & Fream (1997) and Hollinger et al. (1988). These studies supported the idea that the complex schedule of reinforcement and punishment that occurs with criminal computer activity is an important factor in explaining the continuation of the offense (Skinner & Fream, 1997).

The contradiction found in the current study may be explained by the difference between participants in the current study and those involved in the previous studies. Skinner & Fream (1997) and Hollinger et al. (1988) used students as their participants. The current study used general criminals and the public as participants. Although speculative, there may be a difference in the perception of what constitutes negative and positive reinforcement between students and non-students. In the student studies, the negative reinforcement centered on academic sanctions. To non-students, the negative reinforcement would center around criminal as opposed to academic sanctions. As discussed in the literature review, actual criminal

sanctions apparently occur infrequently, thus reducing the perceived negative reinforcement or punishment.

Another possible explanation is the small number of participants in the present study. Although the power of the logistic regression test was adequate, a larger n would have allowed the test to be more sensitive to small and medium effects. This may have resulted in a differential reinforcement being identified as significant (Tabachnick & Fidell, 1996).

Exploration

The current study provided an opportunity to explore many facets of criminal computer activity and to provide some insight into differences not only between computer criminals and the public but also between computer criminals and general criminals. Differences between computer criminals and the non-criminal public would be expected based solely on the fact that we are dealing with criminals. Therefore, it was important that the study examined how computer criminals and general criminals differed.

There is a rush within the law enforcement community to develop profiles of different offender categories (e.g., predatory offenders, mass murders, pedophiles, terrorists).

However, in order to develop useful profiles, a large amount of data is required (Douglas, Resler, Burgess, & Hartman, 1986). This allows researchers to more accurately identify whether or not any unique patterns and characteristics actually exist. Unfortunately, a large amount of data is not yet available for computer criminals.

Definitions and Differential Association.

The multiple regression analysis examined the variables to identify any that were significantly correlated with the degree of criminality of the participant. The raw crime index scores reflected the amount of criminal activity in which the participant had engaged (Skinner & Fream, 1997). It was necessary to explore this as the main study had dichotomized the participants as criminal computer activity and no criminal computer activity.

The results of the multiple regression analysis indicated that only the model comprised of the variables of definitions and differential association was significant for raw crime index scores. This further supports the some of the findings of Skinner & Fream (1997), and Hollinger (1988). Both of the studies indicated that differential association was positively correlated with illegal computer acts and was the strongest predictor of computer crime.

The finding that definitions also were significant supports social learning theory in general. According to social learning theory, definitions (i.e., norms, and attitude orientation) are a type of cognitive behavior that can be reinforced and can act as discriminative stimuli for other behavior (Akers et al., 1979).

A model consisting of differential association and definitions makes intuitive sense. The more the individual defines the behavior as positive or justified, and associates with individuals holding similar views, the higher the probability that he or she will engage in the behavior.

All Categories by Social Learning Measures.

The exploration of differences between all the categories of participants (criminal computer activity, no-criminal activity, and general criminals) revealed that there was a significant difference between the groups. Criminal computer activity participants not only had higher rates of differential association than the no criminal activity participants, they also had higher rates than the general criminals. The fact that no other significant differences were identified was probably due to the restrictions that were placed on the tests due to the small

n for general criminals and the resulting violations of the test assumptions (Tabachnik & Fidell, 1996). These restrictions made the tests conservative ($\alpha = .001$).

The finding of a higher rate of differential association needs to be viewed with caution. It should be stressed that the study focused on criminal computer activity and not general criminal behavior. This fact is important, as it is not surprising that individuals who specialize in a particular criminal area have higher differential association with that area. Without further exploration of computer versus general criminal behavior, the importance of the finding is somewhat obscured. In order to more fully explore the question, one would have to study the rates of differential association of those who are involved in criminal computer activity and those involved in general crimes, relative to their specific activities.

However, it has been speculated that criminal computer behavior may in fact be more dependent on differential association than general criminal behavior (Chantler, 1996). This dependence is for not just the social environment aspect of shaping their belief systems, but also for the required technical acumen to engage in the behavior. The unique technical requirements of criminal computer behavior as opposed to general criminal behavior

(e.g., theft, assault) would dictate that individuals wanting to engage in the behavior would have to learn the skills (Chantler, 1996; Denning, 1998). These skills are not routinely taught in universities or trade schools, and must be acquired by associating with others who already have the knowledge and skills, namely the criminal or deviant community (Chantler, 1996).

Limitations of the Study

As with most studies that are exploratory in nature, there are certain limitations that should be taken into consideration when examining the results and drawing any conclusions.

The empirical findings of this study were somewhat compromised by the methodological limitations of self-report surveys. Also, the current study was not experimental in design, which limits the ability to reach any causal inferences regarding the findings (Keppel & Zedeck, 1989). In general, non-experimental studies are criticized for not using random sampling techniques. The current study, while not using random sampling, did obtain representative samples of participants. The comparison of the sample participants to their corresponding populations (i.e., general criminal population, and Internet population), support this conclusion.

In phase one, the comparative analysis was somewhat limited due to the fact that no data were obtained on young offenders (12-18 years of age). Canada is very protective of young offenders and severely restricts access to any data relating to them. This hampers exploratory research of this nature, as other studies have indicated that young offenders may make up the bulk of the criminal computer population (Chantler, 1996; Parker, 1998).

The findings of phases two and three were also limited as there were no convicted computer criminal participants. It was unfortunate that this population was not represented, despite extensive efforts to locate convicted computer criminals in Canada. In Canada, the majority of computer criminals receive sentences that are served in the community. They usually do not spend time in correctional institutions. This makes their recruitment very difficult. Computer crime is also a relatively recent criminal phenomenon and there are not a large number of individuals who have actually been convicted of these offences in Canada. The combination of these factors may have contributed to their absence from the study.

The lack of convicted computer criminals was anticipated. The use of the “Meta category” of criminal computer activity, that included anyone self-reporting

criminal computer activity, was specifically designed to reduce the impact of no convicted computer criminal participants. Although the individuals self-reporting criminal computer activity had never been convicted, they still had committed the criminal act. The use of this Meta category is justified as the ultimate focus of the study was not on whether or not someone had been convicted, but on characteristics of individuals who had or were currently engaged in criminal computer behavior.

The relatively small number of general criminal participants who had never engaged in criminal computer behaviors was also problematic. Several of the provinces' probation services were uncooperative or declined to participate, or refused to help locate potential participants. The small n severely limited the type of exploratory analysis that could be conducted as it led to violations of normality and other test assumptions. To overcome these violations, some of the statistical tests were adjusted to be very conservative, but unfortunately the power was reduced. As a result of the low power, potential small to medium effects would not have been identified by these tests.

The questionnaire used in this study, the CCISLQ, was a new instrument. Although it was based on questionnaires

used by other researchers in this area, it had not undergone any reliability or validity testing prior to its usage. However, input was obtained from the researchers from whose scales the CCISLQ had been developed (Dr. Skinner, Dr. Akers, and Dr. Bandura).

The post hoc reliability tests on the CCISLQ indicated that the scales had sufficient reliability to be of use. The differential association scale did have a lower reliability score than the other scales $\alpha = .64$. This lower reliability score could have been due to the fact that only three questions were used for this scale. Using such a small number of items negatively affects unidimensionality, resulting in a low reliability score (Dunn, 1989). No thorough validity testing of the CCISLQ was possible. As criminal computer research is an immature field with a lack of established instruments, the CCISLQ was only tested for construct validity, which was considered sufficient.

Summary

Research in the area of criminal computer behavior has been sparse. Because of the lack of previous research and the lack of conceptual development into the study of computer crime, this study was exploratory. The findings of this study are preliminary and require corroborating support of further studies. The CCISLQ is also a new

instrument that will require future work to verify and improve its reliability, validity, and the actual structure of the scales.

Although there were some limitations with the study, the findings and their implications are important and add to the growing body of knowledge in this area. The results indicated that: 1) Criminal computer activity is relatively common. 2) There were few social demographic differences between convicted computer and general criminals. Although race was identified as significant (with more computer criminals being Asian and fewer being Native People than would be expected by their relative numbers), based on speculation, this may be due to the influence of socio-economic status (SES), 3) The courts in Canada sentence computer criminals to significantly shorter sentences than general criminals, 4) Criminal computer behavior is influenced by differential association, differential reinforcement, and moral disengagement, 5) A predictive model for criminal computer behavior should include moral disengagement and differential association.

Future researchers in this area should be aware of the various logistical problems encountered when dealing with several provincial agencies. It would be prudent for researchers to include some sort of incentive for the

criminal participants to return the surveys within a certain time (e.g., small monetary reward if questionnaire is useable and returned within two weeks).

From a design perspective, subsequent studies should expand their comparative analyses of computer criminals, general criminals, and members of the non-criminal public to include personality traits (e.g. extraversion, introversion). The use of instruments such as the MBTI or NEO-PI should also be considered.

Subsequent studies need to include young offenders as part of their sample. This could be difficult in Canada due the current Young Offenders Act, but obtaining a representative sample across all age categories would be beneficial.

Another important area to focus upon in future studies would be the individual differences if any, between the various computer criminal activity categories (i.e., piracy, viruses, credit cards). To date, these differences have not been studied.

As Canada has a relatively small convicted computer criminal population, it would be advisable for subsequent studies to include criminal participants from the U.S. The U.S. appears to be more active in pursuing computer criminals and should have a larger pool to draw upon. This

would dramatically increase the sample sizes and thus increase the power of the tests used to analyze the data. An increase in power would assist in identifying any true differences that may exist between computer criminals, general criminals, and the general public.

In general, future research needs to focus on comparisons of computer to general criminals in order to ascertain whether criminal computer activity is unique or merely part of the larger criminal continuum (Sherizen, 1997).

As we enter the twenty-first century, computer crime appears to be on the rise. As society becomes more and more dependent on technology, the need to understand the computer criminal also becomes increasingly important.

References

Adamski, A. (1999). Crimes related to the computer network. Threats and opportunities: A criminological perspective. Retrieved June 1, 1999 from the World Wide Web: http://www.infowar.com/new.

Agnew, R. (1993). Why do they do it? An examination of the intervening mechanisms between social control and delinquency. Journal of Research in Crime and Delinquency, 3, 245-266.

Agresti, A., & Finlay, B. (1997). Statistical methods for the social sciences. New Jersey: Prentice Hall

Akers, R. (1977). Deviant behavior: A social learning approach. Belmont: Wadsworth.

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

Akers, R., Krohn, M., Lanza-Kaduce, L., & Radosevich, M. (1979). Social learning and deviant behavior: A specific test of a general theory. American Sociological Review, 44, 636-655.

Albanese, J. (1984). Corporate criminology: Explaining deviance of business and political organizations. Journal of Criminal Justice, 12, 11-19.

American Psychiatric Association. (1994). Diagnostic and statistical manual of mental disorders (4th ed.). Washington, DC: Author.

Anonymous. (1997). A hackers guide to protecting your internet site and network: Maximum security. New York: Sams.net Publishing.

Bandura, A. (1990a). Mechanisms of moral disengagement. In Reich (Ed.). Origins of Terrorism; Psychologies, Ideologies, Theologies, States of Mind. (pp. 161-191). New York: Cambridge University Press.

Bandura, A. (1990b). Selective activation and disengagement of moral control. Journal of Social Issues, 46, 27-46.

Bandura, A., Barbaranelli, C., Caprara, G., & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. Journal of Personality and Social Psychology, 71, 364-374.

Blackburn, R. (1993). The psychology of criminal conduct: Theory, research and practice. Toronto: John Wiley & Sons.

Baron, R., & Kenny, D. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations.

Journal of Personality and Social Psychology, 52, 1173-1182.

Birnbaum, M. (2000). Decision making in the lab and on the web. In Birnbaum (Eds.). Psychological experiments on the internet. (pp. 3-34). San Diego: Academic Press.

Burgess, R., & Akers, R. (1966). A differential association-reinforcement theory of criminal behavior. Social Problems, 14, 128-147.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. International Journal of the Sociology of Law, 24, 229-251.

Chantler, N. (1996). Profile of a computer hacker. Florida: Infowar.

Davis, R., & Hutchison, S. (1999). Computer crime in canada. Toronto: Carswell.

Davis, L., & Offord, K. (1997). Logistic regression. Journal of Personality Assessment, 68, 497-507.

Denning, D. (1998). Information Warfare and Security. Reading: Addison-Wesley.

Douglas, J., Resler, R., Burgess, A., & Hartman, C. (1986). Criminal profiling from crime scene analysis. Behavioral Sciences and the Law, 4, 401-421.

Duff, L., & Gardiner, S. (1996). Computer crime in the global village: Strategies for control and regulation- in

defence of the hacker. International Journal of the Sociology of Law, 24, 221-228.

Dunn, G. (1989). Design and analysis of reliability studies. New York: Halsted Press.

Emmons, R. (1987). Narcissim: Theory and measurement. Journal of Personality and Social Psychology, 52, 11-17.

Ewen, R. (1980). An introduction to theories of personality. New York: Academic Press.

Feldman, P. (1993). The psychology of crime a social science textbook. Cambridge: Cambridge University Press.

Flohr, U. (1995). Bank robbers go electric. Retrieved March 5, 1998 from the World Wide Web: http://www.byte.com/news.

Freedman, D., & Mann, C. (1997). At large. New York: Touchstone.

Garfinkel, S., & Spafford, G. (1996). Practical unix and internet security. New York: O'reilly & Associates Inc.

Gattiker, U., & Kelley, H. (1997). Techno-crime and terror against tomorrow's organization: What about cyberpunks? Retrieved February 5, 1999 from the World Wide Web: http://www.ncsa.com/library.

Goldman-Pach, J. (1994). An investigation of the applicability of a general theory of crime to computer crime. Unpublished paper.

Goodell, J.(1996). The cyber thief and the samurai. New York: Dell Publishing.

Government of Canada. (1996). Criminal Law Improvement Act, 1996. Retrieved March 1, 1999 from the World Wide Web: http://www.parl.gc.ca/government/C-17.

Hafner, K., & Markoff, J. (1995). Cyberpunks: Outlaws and hackers on the computer frontier. Toronto: Simon and Schuster.

Hirschi, T. (1969). Causes of delinquency. Berkley: Free Press.

Hollin, C. (1989). Psychology and crime: An introduction to criminological psychology. New York: Routledge.

Hollinger, R. (1988). Computer hackers follow a guttman-like progression. Social Sciences Review, 72, 199-200.

Hosmer, D., & Lemeshow, S. (1989). Applied logistic regression. Toronto: John Wiley & Sons.

Howard, J. (1997). Analysis of security incidents on the internet. Unpublished doctoral dissertation, Carnegie Mellon University, Pennsylvania.

Karnow, C., Landels, R., & Landels, D. (1994). Recombinant culture: crime in the digital network.

Retrieved February 5, 1999 from the World Wide Web: http://www.cpsr.org/privacy.

Keppel, G., & Zedeck, S. (1989) Data analysis for research designs: Analysis of variance and multiple regression correlation approach. New York: W.H. Freeman and Company.

Kleinbaum, D. (1996). Logistic regression: A self-learning text. New York: Springer-Verlag

Krantz, J., & Dalal, R. (2000). Validity of web-based pyschological research. In Birnbaum (Eds.). Psychological experiments on the internet. (pp. 35-60). San Diego: Academic Press.

Levy, S. (1985). Hackers. New York: Dell

Littman, J. (1997). The Watchman: The twisted life and crimes of serial hacker kevin poulsen. Toronto: Little Brown & Company.

Littman, J. (1995). The fugitive game: online with Kevin Mitnick. Toronto: Little Brown & Company.

Matseuda, R. (1988). The current state of differential association. Crime and Delinquency, 34, 277-306.

Maxwell, S., Delaney, H., & Dill, C. (1984). Another look at ANCOVA versus blocking. Psychological Bulletin, 95, 136-147.

McCarthy, B. (1994). The attitudes and actions of others: Tutelage and sutherland's theory of differential association. British Journal of Criminology, 36, 135-147.

Michalowski, R., & Pfuhl, E. (1991). Technology, property and law: The case of computer crime. Crime, Law and Social Change, 15, 255-275.

Mizrach, S. (1997). Is there a hacker ethic for the 90s? Retrieved February 5, 1999 from the World Wide Web: http://www.infowar.com.

Parker, D. (1998). Fighting computer crime: A new framework for protecting information. New York: John Wiley & Sons, Inc.

Paulhus, D. (1998). Paulhus deception scales (PDS): The balanced inventory of desirable responding-7, user's manual. Toronto: Multi-Health Systems Inc.

Post, J. (1996). The dangerous information system insider: Psychological perspectives. Retrieved February 5, 1999 from the World Wide Web: http://www.infowar.com

Post, J., Shaw, E., & Ruby, K. (1998). Information terrorism and the dangerous insider. Paper presented at the meeting of InfowarCon'98, Washington, DC.

Power, R. (1996). Testimony before the permanent subcommittee on investigations. Retrieved January 5, 1999 from the World Wide Web: http://www.gocsi.com/preleas2.

Power, R. (1998). Current and future danger. Computer Security Institute.

Power, R. (1999). CSI/FBI 1999 computer security survey. Computer Security Institute.

Power, R. (2000). CSI/FBI 2000 computer security survey. Computer Security Institute.

Rapalus, P. (1997). 1997 Computer crime and security survey. Available: www.gocsi.com/preleas.

Rasch, M. (1996). Criminal law and the internet. The Internet and Business: A Lawyer's Guide to the Emerging Legal issues. Retrieved February 5, 1999 from the World Wide Web: http:// www.cla.org/RuhBook/chp11.htm

Reips, U. (2000). The web experiment method: Advantages, disadvantages, and solutions. In Birnbaum (Eds.). Psychological experiments on the internet. (pp. 89-117). San Diego: Academic Press.

Rogers, M. (1999a). Psychology of hackers: Steps toward a new taxonomy. Retrieved May 5, 1999 from the World Wide Web: http://www.infowar.com

Rogers, M. (1999b). Psychology of computer criminals. Paper presented at the annual Computer Security Institute Conference, St. Louis, Missouri.

Rubinstein, G. (1997). Computer abuse act. Retrieved February 5, 1999 from the World Wide Web: http://www.digitalcentury.com/encyclopedia.

Sacco, V., & Zureik, E. (1990). Correlates of computer misuse: Data from a self-reporting sample. Behaviour and Information Technology, 9, 353-369

Schwartau, W. (1994). Information Warfare. New York: Thunder Mouth Press.

Schwartau, W. (2000). Cybershock: Surviving hackers, phreakers, identity thieves, internet terrorists and weapons of mass destruction. New York: Thunder Mouth Press.

Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. Security Awareness Bulletin, 2, 1-10.

Sherizen, S. (1997). Criminological concepts and research findings relevant for improving computer crime control. In Hollinger (Ed.). Crime Deviance and the Computer. (pp. 298-305). Aldershot: Dartmouth.

Skinner, W., & Fream, A. (1997). A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency, 34, 495-518.

Spafford, E. (1997). Are hacker break-ins ethical? In, Ermann, M., Williams, M. & Shauf, M. (Eds.) Computers, ethics, and society. (pp. 77-88). New York: Oxford.

SPSS. (2000). Guide to data analysis. New Jersey: Prentice Hall.

Sterling, B. (1992). The Hacker crackdown: Law and disorder on the electronic frontier. Toronto: Bantam Books.

Stoll, C. (1985). The cuckoo's egg: Tracking a spy through the maze of computer espionage. New York: Mass Market Paperback.

Sutherland, E. (1947). Principles of criminology (4th ed.). Philadelphia: Lippincott.

Tabachnick, B., & Fidell, S. (1996). Using multivariate statistics (3rd ed.). New York: HarperCollins College Publishers.

Taylor, P. (1998). Hackers: the hawks and the doves-enemies & friends. Unpublished manuscript.

United Nations (1999). International review of criminal policy – United nations manual on the prevention and control of computer-related crime. Retrieved June 14, 1999 from the World Wide Web: http://www.ifs.univie.ac.at/~pr2gq1.

Unrau, Y., & Coleman, H. (1998). Understanding and interpreting polytomous logistic regression: Applications to research on social work practice. Research on Social Work Practice, 8, 223-235.

West, D. (1988). Psychological contributions to criminology. British Journal of Criminology, 28, 77-92.

Wynn, G. (1996). Cyberculture and differential association: The net effect of juvenile delinquency. Unpublished paper.

Appendix A

Research Agreement: Province of British Columbia

Appendix B

Research Agreement: Province of Alberta

Appendix C

Research Agreement: Province of Manitoba

Appendix D

Computer Crime Index and Social Learning Questionnaire:

Handout Version

C.C.I.S.L.Q.

CONFIDENTIAL QUESTIONNAIRE

NOTE: Your participation in this study is greatly appreciated, and steps have been taken to ensure your anonymity. Please make sure that you do not indicate your name on this questionnaire or on the answer sheet.

PLEASE USE THE ACCOMPANYING ANSWER SHEET TO ANSWER THE QUESTIONS. DO NOT MARK THE QUESTION SHEET.

1) How long have you been interested in computers?

(A)= Does not apply (B)= 1yrs (C)= 2yrs (D)= 3yrs
(E)=4 or more years

2) The computer you use most often is owned by:

(A) = you or your family (B) = a friend (C) = a school
(D) = your employer (E) = other

3) What operating systems are you familiar with?

(A) = Does not apply (B) = DOS (C) = Windows 95-98
(D) = Windows NT/2000 (E) = Macintosh (F) =Unix (including Linux/FreeBSD)

4) What level of a user would you rate yourself as?

(A) = Novice (B) = Intermediate (C) = Expert

5) Aside from work or school, how many hours per week do you spend on computers (including Internet usage)?

(A) = Less than 5 (B) = between 5 –10 (C) = between 10-15 (D) = more than 15

WHEN WAS THE MOST RECENT TIME THAT *YOU:*

(Use the response codes below for answers to questions 6-13)

(A) = never (B) = within the past month (C) = within the past year (D) = 1-4 years ago (E) = 5+ years ago

6) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

7) Tried to guess another's password to get into his/her computer account or files?

8) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

9) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

10) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?

11) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

12) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

13) Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?

HOW OFTEN IN THE PAST 3 YEARS HAVE YOU;

(Use the response codes below for answers to questions 14-21)

(A) = never (B) = 1 -2 times (C) = 3-5 times
(D) = 6-9 times (E) = 10 times or more

14) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

15) Tried to guess another's password to get into his/her computer account or files?

16) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

17) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

18) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?

19) Knowingly used or gave to another person someone else’s password without the owner of the password’s knowledge or permission?

20) Electronically obtained or possessed someone’s credit card number without his/her knowledge or permission?

21) Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?

HOW OLD WERE YOU THE FIRST TIME YOU:

(Use the response codes *below for answers to questions 22-29)*

(A) = does not apply (B) = 16 years old or less
(C) = 17-18 years old (D) = 19-20 years old
(E) = 21 or older

22) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

23) Tried to guess another's password to get into his/her computer account or files?

24) Accessed another's computer account or files without his/her knowledge or permission *just to look* at the information or files?

25) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

26) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

27) Knowingly used or gave to another person someone else’s password without the owner of the password’s knowledge or permission?

28) Electronically obtained or possessed someone’s credit card number without his/her knowledge or permission?

29) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

HOW MUCH HAVE YOU LEARNED ABOUT THE ACIVITIES IN QUESTIONS 6-13 FROM:

(Use the response *codes below* for answers *to questions 30-36)*

(A) = learned nothing (B) = learned a little
(C) = learned some (D) = learned a lot
(E) = learned everything

30) Reading books or magazines?

31) Seeing family do them?

32) Seeing friends do them?

33) Seeing teachers do them?

34) Watching television, movies, or videos?

35) Seeing bosses or supervisors do them?

36) Accessing the Internet?

37) How many of your best friends have done one or more of the activities listed in questions 6-13

(A) = none (B) = just *a* few (C) = about half
(D) = more *than half (E) = all or almost all*

(*Use*, *the response* codes *below for answers* to questions 38-39)

(A) = strongly disapprove (B) = sometimes disapprove
(C) = sometimes approve (D) = strongly approve

38) What is the general attitude of your friends toward illegal computer activity?

39) What is the general attitude of your family toward illegal computer activity?

HOW MANY TIMES HAVE YOU SEEN OR HEARD ANY OF YOUR COLLEGE, HIGH SCHOOL TEACHERS, OR BOSS:

(Use the response codes below for answers to questions 40-42)

(A) = never (B) = 1-2 times (C) = 3-5 times (D) = 6-9 times (E) = 10 times or more

40) Mention that certain computer activities are unethical or illegal?

41) Praise or encourage students or employees who have done computer activities you thought they should not be doing?

42) Offer students or employees the chance to "pirate" a copy of commercially sold computer software?

WHAT IS YOUR ATTITUDE TOWARD:

(*Use, the response* codes *below for answers* to questions 43-49)

(A) = strongly disapprove (B) = sometimes disapprove (C) = sometimes approve (D) = strongly approve

43) Using, making, or giving to another person a "pirated' copy of software.

44) Trying to guess another's password to get into his/her computer account or files.

45) Accessing another's computer account or files without his/her knowledge or permission just to look at the information or files.

46) Using, or giving to another person someone else’s password without the owner of the password’s knowledge or permission.

47) Defacing a web page to make a point or deliver a political message.

48) Electronically obtaining or possessing someone's credit card number without his/her knowledge or permission?

49) Using, making, or giving to another person a device to obtain free long distance phone calls.

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN OR WOULD ENGAGE IN THE LISTED ACTIVITY, HOW LIKELY IS IT THAT IF DID YOU WOULD BE CAUGHT:

(Use the response codes below for answers to questions 50-55)

(A) = very likely (B) = likely (C) = somewhat likely
(D) = highly unlikely (E) = never

50) Using, making, or giving to another person a "pirated" copy of software?

51) Accessing or trying to access another's computer account or files without his/her knowledge or permission?

52) Writing or using a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

53) Using, or giving to another person someone else's password without the owner of the password's knowledge or permission?

54) Electronically obtaining or possessing someone's credit card number without his/her knowledge or permission?

55) Caught using, making, or giving to another person a device to obtain free long distance phone calls?

(Use the response codes below for answers to questions 56-61)

(A) = very severe (B)= severe (C) = somewhat severe
(D) = not severe at all

56) How severe do you think the punishment would be if you got caught using, making, or giving to another person a "pirated" copy of software?

57) How severe do you think the punishment would be it you got caught accessing another's computer account or files without his/her knowledge or permission?

58) How severe do you think the punishment would be if you got caught writing or using a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?

59) How severe do you think the punishment would be if you got caught using, or giving to another person someone else's password without the owner of the password's knowledge or permission?

60) How severe do you think the punishment would be if you got caught electronically obtaining or possessing someone's credit card number without his/her knowledge or permission?

61) How severe do you think the punishment would be if you got caught using, making, or giving to another person a device to obtain free long distance phone calls?

(Use the response codes below for answers to questions 62-63)

(A) = yes (B) = no

62) Have you ever been caught doing something that you should not have been doing on a computer?

63) Have any of your friends ever been caught doing something that they should not have been doing on a computer?

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, HOW DO YOU THINK YOUR FRIENDS WOULD LIKELY REACT IF THEY FOUND OUT THAT YOU:

(Use the response codes below for answers to questions 64-71)

(A) = turn you in to authorities (B) = criticize you or encourage you to stop (C) = do nothing
(D) = encourage you to continue

64) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

65) Tried to guess another's password to get into his/her computer account or files?

66) Accessed another's computer account or files without his/her knowledge or permission *just to look* at the information or files?

67) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

68) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

69) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

70) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

71) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, HOW DO YOU THINK YOUR FAMILY WOULD LIKELY REACT IF THEY FOUND OUT THAT YOU:

(Use the response codes below for answers to questions 72-79)

(A) = turn you in to authorities (B) = criticize you or encourage you to stop (C) = do nothing (D) = encourage you to continue

72) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

73) Tried to guess another's password to get into his/her computer account or files?

74) Accessed another's computer account or files without his/her knowledge or permission *just to look* at the information or files?

75) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

76) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

77) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

78) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

79) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

<u>WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, HOW DO YOU THINK YOUR TEACHERS OR IF APPLICABLE , BOSSES WOULD LIKELY REACT IF THEY FOUND OUT THAT YOU:</u>

(Use the response codes below for answers to questions 80-87)

(A) = turn you in to authorities (B) = criticize you or encourage you to stop (C) = do nothing (D) = encourage you to continue

80) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

81) Tried to guess another's password to get into his/her computer account or files?

82) Accessed another's computer account or files without his/her knowledge or permission *just to look* at the information or files?

83) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

84) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

85) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

86) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

87) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, IF YOU WERE TO ENGAGE IN IT, WHAT WOULD THE MOST LIKELY OUTCOME BE?

(Use the response codes below for answers to questions 88-95)

(A) = mainly bad (B) = about as much good as bad
(C) = mainly good

88) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

89) Tried to guess another's password to get into his/her computer account or files?

90) Accessed another's computer account or files without his/her knowledge or permission *just to look* at the information or files?

91) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

92) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

93) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

94) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

95) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

(Use the response codes below for answers to questions 96-110)

(A) = strongly disagree (B) = disagree (C) = agree
(D) = strongly agree

96) If people do not want me to access their computer or computer systems they should have better security.

97) It is O.K. to use someone else's credit card number since the credit card company pays not the person.

98) I should be able to look at any computer information the government, a school, business or individual has on me even if they do not let me have *access.*

99) I should be able to look at any information on any computer system even without authorization.

100) Compared with other illegal things people do gaining unauthorized access to a computer system or someone's account is not very serious.

101) It is O.K. to treat someone badly who was obnoxious in the past.

102) People who break into computer systems are actually helping society.

103) It is O.K. to tell small lies because they don’t really do any harm.

104) I would never turn in a friend who used, made or gave to another person a "pirated" copy of software.

105) It is o.k. to use a computer to get revenge on an individual, business or institution who wronged me (gave me an unfair grade, fired me, ruined my credit, broke into my computer account, etc.).

106) It is o.k. for me to pirate commercially sold software because it costs too much for me to buy it.

107) I would never turn in a friend who accessed another's computer account or files without the owner's knowledge or permission.

108) Some people deserve to be treated like animals.

109) A person in a gang should not be blamed for the trouble the gang causes.

110) I would never turn in a friend who wrote or used a program that would destroy someone’s computerized data (i.e. a virus, logic bomb or trojan horse).

111) Please indicate your sex.

(A) = female (B) = male

112) Please indicate your marital status.

(A) = single (B) = married\commonlaw (C) = divorced\separated (D) = widowed

113) Please indicate your age range.

(A) = under 18 (B) = 18-25 (C) = 26-35 (D) = over 35

114) Please indicate the highest level of education obtained

(A)= high school- partial (B) = high school/GED (C) = Technical school or community college diploma\certificate (D) = Under Graduate Degree (E) = Graduate Degree

Appendix E

Computer Crime Index and Social Learning Questionnaire:

WEB BASED VERSION

SURVEY 2

Thank you for participating in this study. Your response will be kept completely confidential. Please answer the survey only once. There are 118 questions. Please answer all questions before submitting your answers.

---

1) How long have you been interested in computers?

__ **Does not Apply**

__ **1year**

__ **2 Years**

__ **3 Years**

__ **4 Years or more**

2) The computer you use most often is owned by:

__ **You or your Family**

__ **A friend**

__ **A School**

__ **Your Employer**

__ **Other**

3) What operating system are you most familiar with?

Does not Apply

DOS

Windows (95/98/NT/2000)

Macintosh

Unix (including Linux/FreeBSD etc.)

4) What level of a user would you rate yourself as?

Novice

Intermediate

Expert

5) Aside from work or school, how many hours per week do you spend on computers (including Internet usage)?

Less than 5

Between 5 -10

Between 10-15

More than 15

WHEN WAS THE MOST RECENT TIME THAT *YOU*:

6) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

Never

Within the past month

Within the past year

1-4 years ago

5+ years ago

7) Tried to guess another's password to get into his/her computer account or files?

Never

Within the past month

Within the past year

1-4 years ago

5+ years ago

8) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

Never

Within the past month

Within the past year

1-4 years ago

5+ years ago

9) Added, deleted, changed or printed any information in another's computer files without the owner's

knowledge or permission?

Never

Within the past month

Within the past year

1-4 years ago

5+ years ago

10) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?

Never

Within the past month

Within the past year

1-4 years ago

5+ years ago

11) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

Never

Within the past month

Within the past year

1-4 years ago

○ **5+ years ago**

12) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

○ **Never**

○ **Within the past month**

○ **Within the past year**

○ **1-4 years ago**

○ **5+ years ago**

13) Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?

○ **Never**

○ **Within the past month**

○ **Within the past year**

○ **1-4 years ago**

○ **5+ years ago**

HOW OFTEN IN THE PAST 3 YEARS HAVE YOU;

14) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

○ **Never**

1-2 times

3-5 times

6-9 times

10 or more times

15) Tried to guess another's password to get into his/her computer account or files?

Never

1-2 times

3-5 times

6-9 times

10 or more times

16) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

Never

1-2 times

3-5 times

6-9 times

10 or more times

17) Added, deleted, changed or printed any information in another's computer files without the

owner's knowledge or permission?

Never

1-2 times

3-5 times

6-9 times

10 or more times

18) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?

Never

1-2 times

3-5 times

6-9 times

10 or more times

19) Knowingly used or gave to another person someone else’s password without the owner of the password’s knowledge or permission?

Never

1-2 times

3-5 times

6-9 times

○ **10 or more times**

20) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

○ **Never**

○ **1-2 times**

○ **3-5 times**

○ **6-9 times**

○ **10 or more times**

21) Knowingly used, made, or gave to another person a device to obtain free long distance phone calls?

○ **Never**

○ **1-2 times**

○ **3-5 times**

○ **6-9 times**

○ **10 or more times**

HOW OLD WERE YOU THE FIRST TIME YOU:

22) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

○ **Does not apply**

○ **16 years old or less**

○ **17-18 years old**

○ **19-20 years old**

○ **21 or older**

23) Tried to guess another's password to get into his/her computer account or files?

○ **Does not apply**

○ **16 years old or less**

○ **17-18 years old**

○ **19-20 years old**

○ **21 or older**

24) Accessed another's computer account or files without his/her knowledge or permission ***just to look*** at the information or files?

○ **Does not apply**

○ **16 years old or less**

○ **17-18 years old**

○ **19-20 years old**

○ **21 or older**

25) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

Does not apply

16 years old or less

17-18 years old

19-20 years old

21 or older

26) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

Does not apply

16 years old or less

17-18 years old

19-20 years old

21 or older

27) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

Does not apply

16 years old or less

17-18 years old

19-20 years old

○ **21 or older**

28) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

○ **Does not apply**

○ **16 years old or less**

○ **17-18 years old**

○ **19-20 years old**

○ **21 or older**

29) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

○ **Does not apply**

○ **16 years old or less**

○ **17-18 years old**

○ **19-20 years old**

○ **21 or older**

HOW MUCH HAVE YOU LEARNED ABOUT THE ACIVITIES IN QUESTIONS

6-13 FROM:

30) Reading Books or magazines ?

○ **learned nothing**

learned a little

learned some

learned a lot

learned everything

31) Seeing family do them?

learned nothing

learned a little

learned some

learned a lot

learned everything

32) Seeing friends do them?

learned nothing

learned a little

learned some

learned a lot

learned everything

33) Seeing teachers do them?

learned nothing

learned a little

learned some

learned a lot

learned everything

34) Watching television, movies, or videos?

learned nothing

learned a little

learned some

learned a lot

learned everything

35) Seeing bosses or supervisors do them?

learned nothing

learned a little

learned some

learned a lot

learned everything

36) Accessing the Internet?

learned nothing

learned a little

learned some

learned a lot

learned everything

---

37) How many of your best friends have done one or more of the activities listed in questions 6-13

None

Just a few

About half

More than half

All or almost all

38) What is the general attitude of your friends toward illegal computer activity?

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

39) What is the general attitude of your family toward illegal computer activity?

__ **Strongly disapprove**

__ **Sometimes disapprove**

__ **Sometimes approve**

__ **Strongly approve**

-

HOW MANY TIMES HAVE YOU SEEN OR HEARD ANY OF YOUR COLLEGE, HIGH SCHOOL TEACHERS, OR BOSS:

40) Mention that certain computer activities are unethical or illegal?

__ **Never**

__ **1-2 times**

__ **3-5 times**

__ **6-9 times**

__ **10 times or more**

41) Praise or encourage students or employees who have done computer activities you thought they should not be doing?

__ **Never**

__ **1-2 times**

__ **3-5 times**

6-9 times

10 times or more

42) Offer students or employees the chance to "pirate" a copy of commercially sold computer software?

Never

1-2 times

3-5 times

6-9 times

10 times or more

WHAT IS YOUR ATTITUDE TOWARD:

43) Using, making, or giving to another person a "pirated' copy of software.

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

44) Trying to guess another's password to get into his/her computer account or files.?

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

45) Accessing another's computer account or files without his/her knowledge or permission just to look at the information or files.

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

46) Using, or giving to another person someone else's password without the owner of the password's knowledge or permission.

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

47) Defacing a web page to make a point or deliver a political message.

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

48) Electronically obtaining or possessing someone's credit card number without his/her knowledge or permission?

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

49) Using, making, or giving to another person a device to obtain free long distance phone calls.

Strongly disapprove

Sometimes disapprove

Sometimes approve

Strongly approve

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN OR WOULD ENGAGE IN THE LISTED ACTIVITY, HOW LIKELY IS IT THAT IF YOU DID, YOU WOULD BE CAUGHT:

50) Using, making, or giving to another person a "pirated" copy of software?

Very likely

Likely

Somewhat likely

Highly unlikely

Never

51) Accessing or trying to access another's computer account or files without his/her knowledge or permission?

Very likely

Likely

Somewhat likely

Highly unlikely

Never

52) Writing or using a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

Very likely

Likely

Somewhat likely

Highly unlikely

Never

53) Using, or giving to another person someone else's password without the owner of the password's knowledge or permission?

○ **Very likely**

○ **Likely**

○ **Somewhat likely**

○ **Highly unlikely**

○ **Never**

54) Electronically obtaining or possessing someone's credit card number without his/her knowledge or permission?

○ **Very likely**

○ **Likely**

○ **Somewhat likely**

○ **Highly unlikely**

○ **Never**

55) Caught using, making, or giving to another person a device to obtain free long distance phone calls?

○ **Very likely**

○ **Likely**

○ **Somewhat likely**

○ **Highly unlikely**

○ **Never**

56) How severe do you think the punishment would be if you got caught using, making, or giving to another person a "pirated" copy of software?

Very severe

Severe

Somewhat severe

Not severe at all

57) How severe do you think the punishment would be it you got caught accessing another's computer account or files without his/her knowledge or permission?

Very severe

Severe

Somewhat severe

Not severe at all

58) How severe do you think the punishment would be if you got caught writing or using a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse)?

Very severe

Severe

Somewhat severe

Not severe at all

59) How severe do you think the punishment would be if you got caught using, or giving to another person someone else’s password without the owner of the password’s knowledge or permission?

Very severe

Severe

Somewhat severe

Not severe at all

60) How severe do you think the punishment would be if you got caught electronically obtaining or possessing someone's credit card number without his/her knowledge or permission?

Very severe

Severe

Somewhat severe

Not severe at all

61) How severe do you think the punishment would be if you got caught using, making,or giving to another person a device to obtain free long distance phone calls?

Very severe

Severe

Somewhat severe

Not severe at all

---

62) Have you ever been caught doing something that you should not have been doing on a computer?

No

○ **Yes**

63) Have any of your friends ever been caught doing something that they should not have been doing on a computer?

○ **No**

○ **Yes**

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, HOW DO YOU THINK YOUR FRIENDS WOULD LIKELY REACT IF THEY FOUND OUT THAT YOU:

64) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

○ **Turn you into the authorities**

○ **Criticize you or encourage you to stop**

○ **Do nothing**

○ **Encourage you to continue**

65) Tried to guess another's password to get into his/her computer account or files?

○ **Turn you into the authorities**

○ **Criticize you or encourage you to stop**

○ **Do nothing**

○ **Encourage you to continue**

66) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

__ **Turn you into the authorities**

__ **Criticize you or encourage you to stop**

__ **Do nothing**

__ **Encourage you to continue**

67) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

__ **Turn you into the authorities**

__ **Criticize you or encourage you to stop**

__ **Do nothing**

__ **Encourage you to continue**

68) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

__ **Turn you into the authorities**

__ **Criticize you or encourage you to stop**

__ **Do nothing**

__ **Encourage you to continue**

69) Knowingly used or gave to another person someone else’s password without the owner of the password’s knowledge or permission?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

70) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

71) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, HOW DO YOU THINK YOUR FAMILY WOULD LIKELY REACT IF THEY FOUND OUT THAT YOU:

72) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold

computer software?

__ **Turn you into the authorities**

__ **Criticize you or encourage you to stop**

__ **Do nothing**

__ **Encourage you to continue**

73) Tried to guess another's password to get into his/her computer account or files?

__ **Turn you into the authorities**

__ **Criticize you or encourage you to stop**

__ **Do nothing**

__ **Encourage you to continue**

74) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

__ **Turn you into the authorities**

__ **Criticize you or encourage you to stop**

__ **Do nothing**

__ **Encourage you to continue**

75) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

__ **Turn you into the authorities**

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

76) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

77) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

78) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

79) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, HOW DO YOU THINK YOUR TEACHERS OR IF APPLICABLE , BOSSES WOULD LIKELY REACT IF THEY FOUND OUT THAT YOU:

80) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

81) Tried to guess another's password to get into his/her computer account or files?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

82) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

83) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

Turn you into the authorities

Criticize you or encourage you to stop

Do nothing

Encourage you to continue

84) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

Turn you into the authorities

Criticize you or encourage you to stop

○ **Do nothing**

○ **Encourage you to continue**

85) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

○ **Turn you into the authorities**

○ **Criticize you or encourage you to stop**

○ **Do nothing**

○ **Encourage you to continue**

86) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

○ **Turn you into the authorities**

○ **Criticize you or encourage you to stop**

○ **Do nothing**

○ **Encourage you to continue**

87) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

○ **Turn you into the authorities**

○ **Criticize you or encourage you to stop**

○ **Do nothing**

Encourage you to continue

WHETHER OR NOT YOU HAVE ACTUALLY ENGAGED IN THE LISTED ACTIVITY, IF YOU WERE TO ENGAGE IN IT, WHAT WOULD THE MOST LIKELY OUTCOME BE?

88) Knowingly used, made, or gave to another person a "pirated" copy of commercially-sold computer software?

Mainly bad

About as much good as bad

Mainly good

89) Tried to guess another's password to get into his/her computer account or files?

Mainly bad

About as much good as bad

Mainly good

90) Accessed another's computer account or files without his/her knowledge or permission just to look at the information or files?

Mainly bad

About as much good as bad

Mainly good

91) Added, deleted, changed or printed any information in another's computer files without the owner's knowledge or permission?

Mainly bad

About as much good as bad

Mainly good

92) Written or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or Trojan horse)?

Mainly bad

About as much good as bad

Mainly good

93) Knowingly used or gave to another person someone else's password without the owner of the password's knowledge or permission?

Mainly bad

About as much good as bad

Mainly bad

94) Electronically obtained or possessed someone's credit card number without his/her knowledge or permission?

Mainly bad

About as much good as bad

Mainly good

95) Knowingly used, made, or gave to another person a device to obtain free long distance calling?

Mainly bad

About as much good as bad

Mainly good

96) If people do not want me to access their computer or computer systems they should have better security.

Strongly disagree

Disagree

Agree

Strongly agree

97) It is O.K. to use someone else's credit card number since the credit card company pays not the person.

Strongly disagree

Disagree

Agree

Strongly agree

98) I should be able to look at any computer information the government, a school, business or individual has on me even if they do not let me have ***access.***

Strongly disagree

Disagree

Agree

○ **Strongly agree**

99) I should be able to look at any information on any computer system even without authorization.

○ **Strongly disagree**

○ **Disagree**

○ **Agree**

○ **Strongly agree**

100) Compared with other illegal things people do, gaining unauthorized access to a computer system or someone's account is not very serious.

○ **Strongly disagree**

○ **Disagree**

○ **Agree**

○ **Strongly agree**

101) It is O.K. to treat someone badly who was obnoxious in the past.

○ **Strongly disagree**

○ **Disagree**

○ **Agree**

○ **Strongly agree**

102) People who break into computer systems are actually helping society.

__ **Strongly disagree**

__ **Disagree**

__ **Agree**

__ **Strongly agree**

103)? It is O.K. to tell small lies because they don't really do any harm.

__ **Strongly disagree**

__ **Disagree**

__ **Agree**

__ **Strongly agree**

104) I would never turn in a friend who used, made or gave to another person a "pirated" copy of software.

__ **Strongly disagree**

__ **Disagree**

__ **Agree**

__ **Strongly agree**

105) It is o.k. to use a computer to get revenge on an individual, business or institution who wronged me (gave me an unfair grade, fired me, ruined my credit, broke into my computer account, etc.).

__ **Strongly disagree**

Disagree

Agree

Strongly agree

106) It is o.k. for me to pirate commercially sold software because it costs too much for me to buy it.

Strongly disagree

Disagree

Agree

Strongly agree

107) I would never turn in a friend who accessed another's computer account or files without the owner's knowledge or permission.

Strongly disagree

Disagree

Agree

Strongly agree

108) Some people deserve to be treated like animals.

Strongly disagree

Disagree

Agree

Strongly agree

109)A person in a gang should not be blamed for the trouble the gang causes.

Strongly disagree

Disagree

Agree

Strongly agree

110) I would never turn in a friend who wrote or used a program that would destroy someone's computerized data (i.e. a virus, logic bomb or trojan horse).

Strongly disagree

Disagree

Agree

Strongly agree

---

111) How would you rate yourself based on your knowledge of computers and the Internet ?

Beginner

Intermediate

Expert

112) How would you rate your knowledge of computer related laws and computer related crimes?

Limited

Moderate

Expert

113) Please indicate your gender.

Female

Male

114) Please indicate your marital status.

Single

Married or Commonlaw

Divorced or Separated

Widowed

115) Please indicate your age range.

Under 18

18-25

26-35

Over 35

116) Have you ever been convicted of a criminal offence?

Yes

No

117) Please indicate the highest level of education obtained

High school - partial (did not graduate)

High school or G.E.D

Technical school or community college (diploma or certifcate)

University - Under Graduate

Graduate Degree (Masters or Doctorate)

118) Please list your occupation (e.g., IT professional, student). If you are a student please indicate the level and program of study (e.g. University, 1st year, Engineering)

Click here to submit your answers

Please view the debfriefing information

Appendix F

E-mail Correspondence

Please be advised that I am conducting a study as part of a doctoral program at the University of Manitoba. The study is under the supervision of Dr. James Ogloff from Simon Fraser University. The study has received ethics approval from the University of Manitoba, and the Corrections Branch of the Province of BC. Robert Watts of the corrections branch has also approved the study and a research contract has been signed.

The study is designed to examine illicit computer behavior. As part of the study I wish to have individuals who have been convicted under certain sections of the Criminal Code of Canada answer two questionnaires. The following individual(s) who report to your office, have been identified as meeting the inclusion criteria:

CS # Name

I ask that the appropriate probation officer inquire if the individual(s) are willing to take part in the study. It takes about 45 minutes in total to complete the questionnaires. If they agree, please provide a questionnaire package to them, and have them mail the completed questionnaires back, using the self addressed, stamped envelope.

I will be forwarding questionnaire packages to the probation offices in the next week. The packages will contain the questionnaires, consent form, debriefing sheet, instructions, and a self addressed, stamped envelope.

I thank you in advance for your cooperation in this matter, and greatly appreciate your assistance. If you have any questions or concerns please feel free to contact me.

Marc Rogers
Graduate Studies
Dept. of Psychology
P240 Duff Roblin Bldg.
University of Manitoba
Winnipeg Manitoba
Canada
R3T 2N2
(204)294-4447
mkr@escape.ca

Appendix G

Questionnaire Instructions: Jail

Thank you for agreeing to participate in this research study. The questionnaire package you have received should contain the following documents:

- Consent form
- PDS questionnaire
- CCISLQ questionnaire
- Computer score sheet
- Participant debriefing sheet

Please **sign** the consent form and have it **witnessed**. Please **do not** indicate your name, age, gender, or the date on the PDS questionnaire.

Please answer the PDS by circling the appropriate number on the form itself.

Please **do not** enter any personal information on the computer score sheet. Please use the computer score sheet to answer the questions on the CCISLQ.

Please answer all questions.

Please **complete the questionnaires within 1 day**. Once you have completed the questionnaires please place all the documents back into the envelope and seal it.

Please return the envelope to a staff member.

Appendix H

Consent Form

Thank-you for taking the time to participate in this research. If you agree to participate in this study, you will be asked to complete two brief questionnaires. The questionnaires are designed to measure various psychological and social factors of specific computer related behaviors. At the end of your participation, you will be provided with information regarding the general nature and design of the study. A more detailed explanation of the study will be provided when the entire study has been completed.

We would like to emphasize that your participation will be completely anonymous. Only your participant number will record your responses on all measures.

The session should take approximately 60 minutes. Your participation in this study is voluntary. You have nothing to gain nor lose at any time from participation in this study. You can withdraw from the study at any time without penalty.

By signing below you, acknowledge that you have read and understand the above statements and have given your consent to participate in this study.

_____	_____	_____
Signature	Witness	Date

Appendix I

Participant Debriefing Report

I would like to thank you for participating in the research. The study you took part in is exploratory in nature. It is designed to investigate the psychological and social factors that influence a person's involvement in and continuation of illegal computer activities. Please be assured that the study has been designed so that your participation is completely anonymous, and there is no method of identifying you or any institution you are affiliated with.

Due to the nature of the study a detailed explanation of the hypotheses and the method used will not be made available until the study has been completed, which should take several months. Once the study has been completed the results will be made available and can be obtained from your administration. Again thank you for your participation.

Appendix J

Questionnaire Instructions: Probation

Thank you for agreeing to participate in this research study. The questionnaire package you have received should contain the following documents:

- Consent form
- PDS questionnaire
- CISSLQ questionnaire
- Computer score sheet
- Participant debriefing sheet
- Self addressed, stamped envelope

Please **sign** the consent form and have it **witnessed**. Please **do not** indicate your name, age, gender or the date on the PDS questionnaire.

Please answer the PDS by circling the appropriate number on the form itself.

Please **do not** enter any personal information on the computer score sheet. Please use the computer score sheet to answer the questions on the CISSLQ.

Please answer all questions.

Please complete and return the questionnaires within 1 week of receiving them. Once you have completed the questionnaires, please place all the documents into the self addressed stamped envelope and place in the mail.

Appendix K

Web Consent

Welcome

Thank you for taking an interest in this research project. Please read all instructions carefully. It should take you about 60 minutes to answer the 2 questionnaires. Please ensure that you have sufficient time before starting. Steps have been taken to ensure your anonymity.

Consent

If you agree to participate in this study, you will be asked to complete 2 questionnaires. The questionnaires are designed to measure various psychological and social factors of specific computer related behaviors. At the end of your participation, you will be provided with information regarding the general nature and design of the study. A more detailed explanation of the study will be provided when the entire study has been completed.

We would like to emphasize that your participation will be completely confidential and anonymous. Only your participant number will record your responses on all measures.

Your participation in this study is voluntary. You can withdraw from the study at any time.

By clicking on the link below, you acknowledge that you have read and understand the above statements and have given your consent to participate in this study.

Click here to answer Survey 1

Appendix L

Web Participant Debriefing

I would like to thank you for participating in the research. The study you took part in is exploratory in nature. It is designed to investigate the psychological and social factors that influence a person's involvement in and continuation of illegal computer activities. Please be assured that the study has been designed so that your participation is completely confidential.

Due to the nature of the study a detailed explanation of the hypotheses and the method used will not be made available until the study has been completed, which should take several months. Once the study has been completed the results will be made available on-line at this site.

Again thank you for your participation.