2006

Recommendations for a comprehensive identity theft victimization survey framework and information technology prevention strategies

Sara Berg

Recommendations for a Comprehensive Identity Theft Victimization Survey Framework and Information Technology Prevention Strategies

By

Sara E. Berg

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Technology

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

April 7, 2006

ACKNOWLEDGEMENTS

This thesis could not have been made possible without the guidance and support of numerous folks along the way --

The Information Technology department: a home away from home while in graduate school.

The Criminal Justice department: who treated me as one of their own even without having a CJ graduate program.

Java Wally's, Panera Bread, and Spot Coffee: caffeine, food, and free wireless Internet.

The Old Toad and MacGregors: beer, food, and free wireless Internet.

Everyone involved with Interlibrary Loan: web-based article delivery A+

My committee:
Steve Jacobs, for stepping in when there was a need and bringing his fresh perspective into the area of high tech crime.

Charlie Border, for always knowing I could do it and kicking my butt to get this thing finished.

Sam McQuade, my mentor for two years and beyond, who invited me onto a fabulous research project and told me when I was wrong.

My friends and family, neglected for long periods here and there in the name of education.

And last (but never least), my husband, Eric: for always being there, even when he thought my drafts were boring to read!

ABSTRACT

While steps have been undertaken in the last five years to better understand the problem of identity theft, there has been little research done in the areas of high tech crime victim profiling and prevention. Most studies focus on victim demographics without examining ways in which the victimization may have been facilitated technologically. Attempts to look at precipitating behaviors in the context of victimization are limited. As such, a weak empirical base exists on which to generate additional research and potential solutions to identity theft victimization. This thesis bridges previous identity theft research with other empirical studies in order to offer recommendations for a comprehensive survey framework in which to study identity theft victimization and for information technology strategies to enhance prevention efforts.

TABLE OF CONTENTS

Acknowledgements iii

Abstract iv

Table of Contents v

List of Tables vii

List of Figures vii

I. Introduction and Literature Review 1
- A. What is Crime? 1
  - Labeling of Deviance 1
  - Human Values and Crime 2
- B. What is High Tech Crime? 3
  - Technology-Enabled Crime 3
  - Definition of High Tech Crime 4
  - Types of High Tech Crime 5
- C. Victims and Victimization 6
  - High Tech Victimization 7
  - Victimless Crime 8
- D. Effects of Victimization 8
- E. Theories of Victimization 10
  - Lifestyle-Exposure Theory 11
  - Routine Activities Theory 11
- F. What is Identity Theft? 12
  - History of Identity Theft in the United States: Banking 13
  - History of Identity Theft in the United States: Social Security 15
  - Types of Identity Theft 17
  - Methods of Committing Identity Theft 19
- G. Identity Theft Victimization 20
  - Identity Theft Data Clearinghouse 20
  - FTC's Identity Theft Survey Report (Synovate) 21
  - FTC's Identity Theft Survey Report (Javelin/BBB) 22
  - National Crime Victimization Survey 24
  - Empirical Studies 24

A. Methodology and Findings ……..…… 27
A. Comparative Survey Analysis ……...… 27
B. Findings ……. 30
The profile of an identity theft victim needs to be enhanced. ……. 31
The methodologies used for previous survey administration are problematic. ……. 32
There are deficiencies in the current survey instruments used. ……... 35

B. Recommendations ……..…… 38
A. Changes for Future Surveys …….. 38
More demographic information in should be obtained from survey findings. ……... 38
A number of improvements to methodologies for national surveys can be made. …… 40
Questions asking about offline preventative behaviors should be enhanced. ……. 41
Questions asking about computer security techniques should be enhanced. ……. 43
B. Prevention and Treatment Policies …… 46
There is a need for improved organizational accountability. …….. 48
Financial companies require improved regulation. ……. 50
There is a need for improved individual accountability. ……. 51
Victim treatment policies should be improved. ……... 53
C. Information Technology Prevention Strategies ……. 53
More employee and consumer training is needed. …….. 53
Improved computer security techniques should be used. …… 55
Personal identity should be better validated. ……... 55
Database modification should reduce or eliminate the use of Social Security numbers. …… 57
Law enforcement resources should be improved. ……... 58

IV. Conclusion: Does “IT” Matter? ……... 61

V. References ……... 64

Appendix A: Model Identity Theft Victimization Survey Instrument Description ……. 72

Appendix B: Model Identity Theft Victimization Survey Instrument …… 75

Appendix C: Use of Previously Written Material ……... 85

LIST OF TABLES

Table 1: Types of Identity Theft Fraud-related Victimization …… 17

Table 2: Age of FTC Identity Theft Victims ……... 21

Table 3: Offline Methods of Access to Victim Information ……... 23

Table 4: Online Methods of Access to Victim Information …… 23

LIST OF FIGURES

Figure 1: Combining Previous Research ……. 29

Figure 2: Survey Comparisons ……..……... 29

Figure 3: Thesis Research …… 30

I. Introduction and Literature Review

A. What is Crime?

In order to examine high tech crime, such as identity theft, and its corresponding victimization, it is important to understand what overall crime and criminal victimization comprise. Crime, simply, is any act or omission of act which is forbidden by public law and whose actor is subject to punishment for engaging in the act. A criminal act has been labeled as being deviant and thus is contrary to standards of expected behavior. Labeling is the "process by which deviants are defined by the rest of society" (Becker, 1964, p. 2). Deviance is a shift from social norms – "expectations of conduct in certain situations [which] regulate human social relations and behavior" (Clinard & Meier, 2001, p. 10). What is considered by society to be criminal will change over time. For example, before prohibition the making, selling, and drinking of alcohol was legal, during prohibition it became illegal, and after prohibition it returned to legal status.

Labeling of Deviance

Behaviors themselves are not "inherently criminal or deviant"; this only comes through the label that society confers upon it, not because it incurs harm (Lilly, Cullen, & Ball, 2002, p. 106). The reality that certain acts do cause harm may be a factor in the state or society labeling behavior as criminal, however. This label of "crime" will not occur until there is an "organized social-legal reaction against some form of behavior" (Pfohl, 1981, p. 69). An act will not automatically be deviant in any society or situation; instead it depends on the context and circumstance in which the act occurs. When a certain behavior is new, it will not be deviant or non-deviant – it merely is. Until it happens again, and happens more frequently, it cannot be

understood. Once society is aware of its existence, then labels may be applied in order to name or explain it. For example, when the innovative act of automobile theft became deviant, it was considered to be the crime of "auto banditry" – long before the ordinary crime of "carjacking" ever existed (McQuade, 2001).

Human Values and Crime

At the core of any act, criminal or not, are human values – what does an individual find important? Most people would generally want security, privacy, and protection of their self and their assets. Other people desire assets not theirs and will take whatever steps necessary to get them, or they may not have respect for the safety of others. Offenders are driven by their desires, often independent of criminal laws prohibiting behaviors for acquiring assets or protecting personal security. Thus it is the belief of need that motivates individuals to commit crimes, though actual needs are not as important as the offender's perception of need. (Braithwaite, 1997). Similarly, an offender's greed for financial gains may also be the motivating factor.

One such crime that may occur in order to illegally acquire assets is fraud. Identity theft is fraud. So are multitudes of other crimes, regardless of what form it takes (i.e., credit card fraud, bank fraud, loan fraud, mail fraud, wire fraud, telephone fraud, etc.). These types of fraudulent acts are accomplished using deceit or trickery. The offender misrepresents himself or herself as another person, typically for financial or material gain. Over the years there have been numerous definitions offered for fraud, with assorted terms for these criminal acts used interchangeably. As Dick Johnston (1996), former Director of the National White Collar Crime Center noted, "if I say fraud, you may say economic crime, while somebody else says corporate crime or business crime and others say white collar crime" (p. 1). Over the years there has been a steady stream of evolving labels attached to these sorts of acts, especially once computing

technology became involved: from fraud, to white-collar crime, to financial crime, to computer abuse, to computer crime, to computer related crime. Further spin-offs include economic crime, corporate crime, and cybercrime, as well as the more recent high tech crime (McQuade, 2005).

B. What is High Tech Crime?

Technology-Enabled Crime

Technology[1] may help people protect themselves and what is theirs, but it will also help the people who want to commit acts against others. According to the theory of technology-enabled crime, as technology – tools and techniques – become more complex, criminals may adopt these in order to perform innovative and increasingly complex forms of illicit acts (McQuade, 1998). The consequence is three phases of technology-enabled impacts, namely: "ordinary crime", "adaptive crime", and "new crime". Ordinary crimes are the common crimes that are well known and understood, adaptive crimes are variations of ordinary crime which manifest themselves through innovative use of technology, and new crimes are typically not well-understood and involve radically innovative use of technology to commit (*Ibid*., 1998). This theory also reveals that understanding and managing relatively complex crimes is initially quite difficult, and that there is continual competition between the criminals and law enforcement for technological advantage. As criminals do something new and innovative, law enforcement must catch up in order to avert, control, deter, and prevent new forms of crime. Until the new forms of criminality are understood, there is a policy lag before statutes are passed to criminalize the behavior, after which the act becomes considered as common and ordinary (*Ibid*., 1998).

[1] I accept McQuade's (1998) definition of technology as simple-to-complex tools and techniques. However, for the purposes for this thesis, the frequently used word "technology" refers to telecommunications and computing technologies, also specified as information technology or IT.

Definition of High Tech Crime

As crime has evolved over time, due to the addition of technology used in new and innovative ways, the names and definitions have changed as well. We have seen a shift from computer abuse to computer crime, to computer-related crime, to high tech crime, as well as to the more recent cybercrime (McQuade, 2005). Computer abuse was defined in the late 1970's as "any intentional act involving where one or more perpetrators made or could have made a gain and one or more victims suffered or could have suffered a loss" (U. S. Department of Justice, 1979, p. 3-4). This definition used Parker's (1976) early work, in which he categorized computers as the subject of attack, as the environment of the attack, as a tool of the attack, and as a symbol. McEwen (as cited in McQuade, 1997) conceived of computer crime as an offense committed using knowledge of computer technology. Parker (1998) later operationalized computer crime as "a crime in which the perpetrator uses special knowledge about computer technology", while a cybercrime perpetrator "uses special knowledge of cyberspace" (p. 72).

These previous conceptualizations can then be used to generate a definition for high tech crime. I define this as: any criminal act or omission 1) which is facilitated by information technology, 2) which requires technology on the server-side, or 3) which physically targets technology, which causes any harm – including, but not limited to, financial/monetary or emotional/psychological – to either an individual or a commercial victim. While this definition is encompassing enough to cover a multitude of computer-based or computer-related offenses, it would not cover an act such as homicide – for example, if someone hit another person with their computer and caused death. While the computer would certainly be a tool of the crime in this case, the technology was not a key element for the crime to be able to occur.

Types of High Tech Crimes

What we now label as a high tech crime is, in many cases, a new form of a traditional crime. Using McQuade's (1998) theory of technology-enabled crime, we can understand that many of these traditional crimes have evolved through radical and innovative use of technology. In this manner, a crime such as stalking, which always previously occurred in physical space, could then evolve to use the Internet as the medium of the offense. Similarly, a fraud scheme which previously operated through the U.S. mail system could shift to delivery via electronic mail. However, this theory also helps us understand truly innovative and high tech forms of crime, which do not have an origin in traditional crime. For example, hacking could not exist without a computer, since the crime entails the unauthorized access of a computing system. The definition of high tech crime given in the previous section is extremely broad and recognizes that there are a number of offenses that meet the criteria; these include both new ways of committing traditional crimes and radically innovative crimes. Below are examples of many of these crimes, though it is certainly not an all-inclusive list.

Identity theft is perhaps the most well known crime, due to its prevalence in the media over the last ten years. Internet fraud, notably auction fraud (such as what occurs on eBay) is also infamous. Cyberstalking is a potentially hybrid crime, which may begin online and lead to offline stalking behaviors or vice versa; it may also occur in tandem with traditional stalking. "Phishing" schemes, typically sent through electronic mail, lure victims to fake web sites where they are instructed to enter personal information. The originator of an advance fee, or "419", scam often purports to be a high level African government official or other professional businessperson who is looking for individuals to handle large sums of money, in exchange for a percentage of it. Computers may be used in the facilitation of a number of white-collar crimes,

including fraud, embezzlement, and theft. Unsolicited, or spam, e-mails are typically used to sell goods or services, which may or may not be genuine. Today, file sharing and piracy of music, movies, and software is a large problem, potentially in part because those who engage in those behaviors do not feel that they are criminal.

C. Victims and Victimization

The term "victimology" – the study of victims and victimization – was first coined by Beniamin Mendolsohn, who began gathering victim information for his law practice in 1937 and later did a 1940 study on rape victims (Fattah, 1991). Criminal victimization, using an objective, legal criterion, is defined as negative impacts to victims "caused by, or resulting from, a criminal offense, which is an act committed in violation of the criminal law" (*Ibid*., 1991, p.10). A victim, thus, is "the person who suffers the harmful consequences of the act or omission" (*Ibid*., 1991, p. 89). As a whole, the concept of "victim" is a social construction (Quinney, 1974, p. 107). This can be seen in the shift of the definition of victim over the years, looking at whom exactly would be considered as such. It is only as our understanding of victimization deepens that we can attach the terms of harm to an act and label someone as a victim of that act. However, these understandings and conceptions will always be different based on the individual or group, further varying it across different segments of society (*Ibid*., 1974). In addition, in the criminological view of the label "victim", there is a stigma attached, just as a stigma is attached to the label of "criminal" (Fattah, 1991). These perceptions shape the social reality of the offender-victim relationship, which may not always be as clear-cut as "bad guy" versus "good guy".

High Tech Victimization

As crimes become more complex and high tech, victimization also shifts from traditional into more complex forms. Since the onset of computerization beginning in the 1980's, modernized societies have experienced increasingly complex forms of crime involving non-physical activities via cyberspace. There is a move from physical victimization, as seen in the "ordinary" crimes of burglary, robbery, rape, and homicide, to the emotional and monetary victimization that stems from the more complex financial and computer-based crimes. This is not to say that victims of burglary, robbery, rape, and homicide do not suffer from emotional or monetary victimization; however, it is rare to find victims suffering from offender-inflicted physical harms that result from high tech crimes. In addition, while burglary, robbery, rape, and homicide are usually considered ordinary, they are subject to technological innovations and could, in certain cases, result in more complex victimization and investigation.

Throughout the history of the criminal-victim relationship, society has always recognized the "harm, injury, or other damages caused by the criminal to his victim" (Schafer, 1968, p. 7). However, it has only been in the last thirty years that the consideration that someone harmed by a non-violent crime is still a victim has existed. Quinney (1974) remarks that "criminologists are reluctant to admit that victims are present in less dramatic offenses", and alternative criminal-victim relationships, aside from those "limited to a narrow range of crimes", "have thus been ignored" (p. 105). This could, in part, stem from difficulties in specifying who is a crime victim. Crimes such as rape and murder have clearly defined victims, but this is not so clear for forms of fraud, embezzlement, and other financially-based or technological-based offenses. It may not be an individual, but instead may be businesses, banks, or taxpayers who absorb the losses stemming from the criminal act (Fattah, 1991). In addition, victims of high tech crimes may not

learn of their victimization until well after the act has occurred, if at all – a definite difference from a crime involving a physical, interpersonal connection between offender and victim.

Victimless Crime

However, when it comes to so-called victimless crime, it may become difficult or impossible to define a victim. Victimless crime occurs when "the persons involved in exchanging (illicit) goods or services do not see themselves as victims" (Schur & Bedau, 1974, p. 7). The most frequently cited crimes of this sort include prostitution, drug use, gambling, and homosexuality, while other less mentioned crimes include suicide, private fighting, and vagrancy (Fletcher, 2003, p. 311). While certain behaviors are viewed as *mala in se*, such as murder, these victimless crimes are often issues of morality. Statutes that criminalize these acts are not universal and instead held to local, state, or federal standards. In today's society, file sharing may be viewed as victimless (*Ibid*., 2003). While this sort of piracy is indeed a crime, many individuals do not feel that downloading mp3 files, for example, hurts anyone and so this act has become culturally acceptable. Similar sentiments may be held in other sorts of high tech crimes as well. Due to the lack of interpersonal domain and the use of computer-mediated communication, offenders may not feel that they are causing others harms by their illicit actions.

D. Effects of Victimization

Because criminal victimization so violates a victim's senses of self, trust, and autonomy, it results in emotional harm to the victim (Kennedy, 1983). This "violation of self" is a commonality regardless of the type of attack that has occurred (Bard & Sangrey, 1979, p. 10). Bard and Sangrey (1979) identified three phases of victimization: 1) impact, where the victim

suffers internal distress and seeks reassurance from others; 2) recoil, where the victim must deal with resulting emotions in an attempt towards recovery; and 3) reorganization, where the victim's emotions no longer overwhelm them and they can move on in life. Many victims believe that they are the only ones who feel this way, which compounds the pain of victimization (*Ibid.,* 1979).

Monetary victimization may stem from a number of acts, not solely those that are financial-based. Victims may have direct financial loss due to damaged property and indirect losses due to medical costs to care for physical injuries or from temporary or permanent loss of work (Elias, 1986, p. 108). Violent crimes often result in physical harms suffered. About one-third of all crimes will result in a financial loss in addition to physical injury (*Ibid*., 1986, p. 108). Victims may receive temporary injuries that will heal or permanent injuries that result in scarring, disfigurement, or impaired use, if not death.

Additionally, victims will often experience secondary victimization on the part of the criminal justice system, by being re-victimized due to the treatment they receive. This can be due to a number of reasons, including: insensitive police questioning, lack of information about the status or outcome of their case, attitudes by the police or prosecutors which suggest that the victim contributed to their investigation, lost wages due to time spent testifying in court, difficulties in finding transportation or childcare or getting time off work to go to work, or anxiety about testifying in court (Tomz & McGillis, 1997, p. 16). As Gulotta (1984) notes, "a victim of crime, more often than not, also becomes the victim of the criminal justice system" (p. 87). Individuals against whom the offense was not originally perpetrated often experience suffer from the criminal violation, resulting in indirect victimization (Shichor, 1989). If a victim is

suffering from negative, emotional impacts, their friends and family – the typical support network – will also be affected by their victimization.

E. Theories of Victimization

Criminologists developed a stronger interest in victims in the 1960's, and theories of victimization were developed beginning in the 1970's, the two most widely accepted ones being lifestyle-exposure and routine activities (Miethe & Meier, 1994). The historical foundation for these theories has its origins in the late 1950's when Marvin Wolfgang introduced the term "victim precipitation", which became a "popular descriptor for all direct-contact predatory crime (e.g. murder, assault, forcible rape, robbery)" (Meier & Miethe, 1997, p. 227). The supposition was that victims somehow provoked the offender into committing a criminal act, resulting in the cause of their victimization. This view has been modified over the last fifty years to reflect the changing nature of crime, suggesting that victim precipitation may also be a component of non-violent, especially financial, crimes. Even when no provocation occurs, the victim's own conduct may be a factor in its perpetration. Individuals who display negligent, careless, imprudent, or reckless attitudes or behaviors may open themselves up to opportunistic behavior on the part of the offender (Fattah, 1991). For example, a person who keeps their Social Security card in their purse or wallet is essentially handing their Social Security number to the criminal who pickpockets them. Similarly, a system administrator who does not protect their company servers behind a firewall could unwittingly be allowing malicious hackers to gain access to the system.

Lifestyle-Exposure Theory

In the lifestyle-exposure theory, the basic premise is that "demographic differences in the likelihood of victimization can be attributed to differences in the personal lifestyles of victims" (Meier & Miethe, 1997, p. 232). Thus, variations in lifestyle – a person's occupation, education, residence, age, gender, marital status, and family income and race – all factor into the likelihood that they will become a victim of crime. Because victimization occurs disproportionately as opposed to uniformly, certain lifestyles may increase the risk (Hindelang, Gottfredson, & Garofalo, 1978).

Routine Activities Theory

The routine activities theory has similarities to the lifestyle-exposure theory. Developed by Cohen and Felson (1979), it is based on the premise that "structural changes in routine activity patterns influence crime rates by affecting the convergence in time and space of three elements of direct-contact predatory crimes: motivated offenders, suitable targets, and the absence of capable guardians against a violation" (p. 589). If an individual, in the course of their daily routine or schedule, is in a location that contains someone who has the motive and opportunity to commit a crime, especially if barriers are not present, then the likelihood of victimization may increase. In other words, normal everyday life provides a setting for criminal activity to occur. Capable guardianship could be a person or object and is usually conceptualized either as social/interpersonal (e.g., friends, neighbors, law enforcement) or physical (e.g., burglar alarms, guard dogs, street lighting, Neighborhood Watch programs) (*Ibid*., 1979). Today it could also be virtual or logical, utilizing various forms of digital computer technology to prevent victimization (e.g., Access Control Lists implemented on a network device to limit access,

passwords, and anti-virus software). Such barriers do not exist in any kind of physical or tangible form, and are composed merely of binary 1's and 0's.

This theory, while originally designed to explain direct-contact predatory crimes, may also help to explain high tech crime[2]. The gym a victim frequents may have a receptionist who later harasses him or her online. A victim's wallet may be stolen from outside of their favorite grocery store and the credit card contained within used to commit identity theft. An individual may click on an e-mail attachment that causes them to catch a computer virus. A laptop left unattended in a college library could be stolen.

Additionally, if victimization does occur, an individual's routine may change following the event in order to prevent the same situation from recurring. After someone becomes victimized, they might change their behaviors so they will not be re-victimized. This could include running anti-virus software, changing a computer login password, shredding sensitive documents before throwing them in the trash, not giving out a Social Security number over the phone, using one-time use credit card numbers when shopping online, etc.

F. What is Identity Theft?

Identity theft is one of the fastest growing high tech crimes in the United States today. Also known as identity fraud, these two labels are interchangeable terms which refer to the commission of several types of fraud in the United States and in other nations, although naming conventions vary in crime statutes and in practice throughout the world. Identity theft is committed through the use of obtaining (unique) personal information and then using that

[2] Based on my analysis of identity theft victims from the RIT Computer Use and Ethics, it was not shown that victims were more likely to engage in certain online activities than non-victims. However, further examination is needed of other types of high tech victims in order to say with any certainty if routine activities would or would not apply.

information to impersonate one or more victims, in one or more locations, and across time spanning hours to years. Various methods are used in order to gain access to information for identity theft purposes, of which a key piece of data is a person's Social Security Number. This crime causes both financial and emotional harm to its victims, making this computer-based offense just as dangerous to consumers as traditional "offline" crimes, including violent ones.

In order to understand how identity theft could become so prevalent in the United States, it is important to recognize two major advances. First, we have electronic banking and credit cards, which have made modern life convenient. Second, we have Social Security numbers, which have become an easy way to keep track of an individual. The theft of an individual's "identity" is not a new phenomenon; this form of fraud where someone socially misrepresents themselves as another has always existed. However, the misuse of credit card numbers and Social Security numbers – an individual's key pieces of personal information – has resulted in the growth of the financial fraud that we today call identity theft.

History of Identity Theft in the United States: Banking

Prior to the availability of unified currency system in the United States, each state printed its own notes to act as money in conjunction with gold and silver coins (Evans & Schmalensee, 2003). The first commercial bank in America was chartered on January 7, 1782 in Philadelphia, with the first federal bank chartered in 1791 (Klebaner, 1974). States operated their own banks throughout the 1700's, which involved printing individual currencies. Following the Civil War, the National Bank Act of 1863 authorized the federal government to grant charters to "national banks" – privately owned commercial banks who could then create circulating paper money (Degen, 1987, p. 1). Paper money was lighter and easier to transport than coins, but in the early days there were no limits as to how much was printed, even if no gold or silver existed to back

up its value (Evans & Schmalensee, 2003). During the 1900's the use of paper money increased, which led to the growth of consumer banking and the development of formal credit systems.

The existence of various technologies surrounding the banking industry provided a framework in which identity theft was able to evolve and grow. Prior to the use of "plastic", exchanges made often relied on trust. This was especially true in a small town setting where people knew each other. Customers might have had a credit account at the local store and use this to buy items and pay for them later. The transaction would be recorded in a ledger, and no cash, check, or credit card was required at the time of purchase. Payment cards began to originate at the beginning of the twentieth century, with hotels, oil companies, and department stores issuing them to customers to identify that they had a charge account at that business (*Ibid.,* 2003). However they were only good at that particular company and were not networked together in any fashion.

In 1950, the Diners' Club was the first organization to offer a charge card, which required that the balance be paid in full every month (Wikipedia Group Author, 2005a). Between 1953 and 1954, almost 100 U.S. banks began offering charge cards to their customers (Evans & Schmalensee, 2003). By 1958, American Express and Carte Blanche were also offering charge cards for payment services, but it was Bank of America and Chase Manhattan Bank who issued the first actual credit cards, which could either be paid in full every month or used until a credit limit was reached (*Ibid.,* 2003). Bank of America was the first to do a mass mailing of credit cards in September 1958, sending them to nearly every household in Fresno, California; one year later, they had racked up $59 million in purchases on their cards ($350 million in 2004 dollars) (Brooker & Levinstein, 2004). Barclay's Bank operated the first cash-dispensing machine in the world on June 27, 1967, in Enfield, North London (Wikipedia Group Author, 2005b). The first

American-cash dispensing machine was opened by Chemical Bank on September 2, 1969 in Rockwell Centre, Long Island and also allowed customers to cash checks (Florian, Burke, & Mero, 2004). By the mid-1970's, these Automated Teller Machines (ATMs) could also perform additional banking functions, including taking deposits and performing balance inquiries (*Ibid.,* 2004). As computing technologies became more powerful, ATM's from different banks could be networked together, then different networks connected. Banking had shifted from local commerce to a transnational affair, paving the way for the dependence on interconnected financial databases and the ease of accessing this information for illicit purposes.

History of Identity Theft in the United States: Social Security

In the midst of the Great Depression, there was a need in the United States to improve the economic security of its citizens. President Franklin D. Roosevelt, elected in 1932, felt that "social insurance" as opposed to welfare assistance was the key – a plan where workers would contribute through taxes while employed and later on receive benefits as retirees (Social Security Administration [SSA], 2003). A year after its initial promotion, the Social Security Act was signed into law on August 14, 1935, creating general welfare programs and providing for a system by which retired workers over age 65 could be paid a continuing income after retirement (*Ibid.,* 2003). To implement the Act, every worker would be assigned a Social Security number (SSN) so they could begin acquiring credits towards retirement.[3] While the original intent was that this unique identifier would solely be used within the Social Security Administration, this proved not to be the case.

[3] Social Security turned into a family-based program following a 1939 amendment, which added payments to a retired worker's spouse and children under age 18 and survivor benefits for the family of a worker killed before retirement (SSA, 2003).

In 1943 President F.D. Roosevelt authorized the use of the SSN as a primary key for other government databases (Berghel, 2000). Fueled by this decision, between 1961 and 1973:

- the Civil Service Commission adopted the SSN as an official Federal employee number;
- the Internal Revenue Service adopted the SSN as the official taxpayer identification number;
- the Treasury Department required buyers of Series H savings bonds to furnish their SSN;
- citizens over age 65 needed a SSN for Medicare;
- the Veterans Administration began using SSNs as a hospital admissions number and for patient record keeping;
- the Department of Defense adopted the SSN to replace the military services number to identify Armed Forces personnel;
- the Bank Records and Transactions Act required a SSN to be obtained from all bank, credit union, savings and loan association, and securities brokers/dealers customers; and
- the Treasury Department required buyers of Series E savings bonds to furnish their SSN (SSA, 2000).

The Privacy Act of 1974 made it easier for citizens to refuse providing their SSN by requiring government agencies to obtain authorization before using it, though agencies already using SSNs prior January 1, 1975 were exempt (Hibbert, 2001). The Tax Evasion Act of 1976 allowed state and local agencies handling taxes, welfare, or driver's licenses to use a SSN as a unique identifier (*Ibid.,* 2001). In 1987, a project was initiated for parents to automatically obtain SSNs for their newborn infants when the state registered their birth (SSA, 2000). These steps led the way for non-government organizations, including medical offices, utility companies, insurance companies, and schools, to use the SSN, especially once nearly everyone in the United States had

one. The widespread usage of the SSN as an everyday form of personal identification was inevitable, which set conditions for its misuse and easy availability.

Types of Identity Theft

Corresponding to every form of identity theft are forms of victimization, which may include credit card fraud, unauthorized phone or utility services, bank fraud, etc. Recent data provided by the Federal Trade Commission (FTC) indicate relatively high rates of fraud-related victimization. As listed in Table 1 below these range from a high of twenty-six percent from credit card fraud to five percent for fraudulent loans.

Table 1: Types of Identity Theft Fraud-related Victimization

Credit Card Fraud	26%
Unauthorized Phone or Utility Services	18%
Bank Fraud	17%
Employment-Related Fraud	12%
Government Document or Benefits Fraud	9%
Fraudulent Loans	5%
Other Assorted Incidents	25%

Source: Federal Trade Commission [FTC], 2006

Another six percent of complainants reported an attempted identity theft incident.

Data from Table 1 above are explained as follows:

- Credit card fraud: This is the most common incident. The offender uses their victim's identity in order to apply for and obtain credit cards, either through a major bank or from department stores. They might also fraudulently use an existing card belonging to the victim.
- Unauthorized phone or utility service: The offender uses the stolen identity to obtain such services as a cell phone, landline phone, or other utility.

- Bank fraud: The offender opens an account using the victim's information, makes fraudulent withdrawals against the victim's account, or writes fraudulent checks (First National Bank of Sullivan, n.d.). There might also be an electronic funds transfer between the victim's account and the offender's account (U. S. House of Representatives, Broder, 2000a[4]).
- Employment fraud: The offender obtains employment in the victim's name.
- Fraudulent loan applications: These can easily be made with victim information, with amounts getting approved for sometimes thousands, if not tens of thousands, of dollars. One thief in California was even able to purchase a $500,000 house through this method and was about to close on an $800,000 residence before he was caught (Lin-Fisher, 2001).
- Government identification or benefits fraud: Offenders can use a victim's identity to obtain a driver's license or other government-issued identification papers.
- Other assorted incidents: These can include obtaining medical services, signing lease agreements, or evading legal sanction or criminal warrants (FTC, 2001a). More recently, organized crime rings have begun to prey on consumers by perpetrating scams that involve requests for personal information, including the "Slave Reparations Act" (National Center for Victims of Crime [NCVC], 2001) and the "Nigerian Bank Transfer" hoax (U. S. Secret Service, 2002).

Many victims will experience multiple types of identity theft together in a single victimization incident (FTC, 2001a), such as when an offender obtains both credit cards and loans in the victim's name.

[4] The first citation given for any Congressional Hearing witness testimony will be given in the form: Branch of Congress, Witness Name, Date. Subsequent references to the same witness will be cited as: Witness Name, Date.

Methods of Committing Identity Theft

Although some victims are not aware of how an offender obtained their personal identification information, there are a number of different methods that enable the theft to occur. Stealing the victim's purse or wallet (NCVC, 2001) provides access to a great deal of data, including name, address, date of birth, driver's license, phone number, credit cards, and most importantly, Social Security number (SSN). If a SSN can not be immediately found, it can be purchased through online information brokers when details such as name and birth date are given. These information brokers, alternatively, can sell SSNs as well, getting the numbers from headers of credit reports (U. S. Senate, Givens, 2000). Using a technique known as "dumpster diving", offenders search trash cans of individuals or businesses for papers or other documents that might contain SSNs or other data (Givens, 2000; NCVC, 2001). Related to this is mail theft, where the documents, such as pre-approved credit card applications, are stolen directly from a mailbox (Givens, 2000; NCVC, 2001). A change-of-address form can be used to divert a victim's mail, potentially containing personal information, to the offender. Personal and credit information can be taken from insecure online (Internet-based) shopping sites (NCVC, 2001). Within a company, dishonest employees with access to sensitive data can obtain SSNs and other records (Givens, 2000). Using "pretexting", a method to obtain personal information under false pretenses (FTC, 2001b), an offender could pose as a telemarketer, a financial representative, etc., to get the victim to disclose key pieces of information. Especially in recent times, "phishing" schemes are being used more often, where offenders seek to direct consumers to a fake web site designed to look like the site for a legitimate business, such as eBay or Paypal. Finally, it could be a relative, friend, or someone else with a personal relationship with the victim who may divulge and/or use their information to perpetrate identity theft.

Clearly, even though identity theft has been identified as a high tech crime, not all of the methods used in order to acquire personal information are technology-based. This is especially true of such techniques as purse or wallet theft, dumpster diving, or mail theft. However, these sorts of "offline" measures are a means to an end. Because of the interconnectedness of financial databases, information technology is used once an offender uses the SSN or credit card number, for example, that is taken from the victim. Additionally, the addition of IT has it made possible to commit identity theft on a large scale, thus changing the dynamics of both offending and victimization. As one article puts it, identity theft is the "neoteric crime of the information technology era" (Saunders & Zucker, 1999, p. 184).

G. Identity Theft Victimization

Identity Theft Data Clearinghouse

Since the late 1990's, statistics have been kept on consumer victims of identity theft[5]. The Federal Trade Commission (FTC) began the Consumer Sentinel database for consumer complaints in 1997 (FTC, 2006). In November 1999, the FTC launched the Identity Theft Data Clearinghouse, as part of a provision in 1998's Identity Theft and Assumption Deterrence Act. The ITADA, which made identity theft a federal crime against consumer victims, also called for the FTC to begin tracking victim complaints. By the end of 2005, the Clearinghouse contained

[5] The Internet Crime Complaint Center (IC3), a joint venture between the Federal Bureau of Investigation and the National White Collar Crime Center, began tracking Internet fraud complaints in 2000. However only 0.3% of the 207,449 complainants in 2004 reported being victimized by identity theft (National White Collar Crime Center and the Federal Bureau of Investigation [NWCC & FBI], 2005, p. 4, 6). As such, these victims are not incorporated into this study.

almost three million complaints on both identity theft and consumer fraud, including Internet fraud (*Ibid*., 2006).

The Identity Theft Data Clearinghouse and Consumer Sentinel track information including the age of complainants/victims, victim reporting behaviors, and time between victimization and discovery. Out of the 686,683 complaints received between January 1 and December 31, 2005, thirty-seven percent were categorized as identity theft (*Ibid*., 2006, p. 6).

The 239,277 identity theft complaints in 2005 where age was reported break into the following age groups, as seen in Table 2 below:

Table 2: Age of FTC Identity Theft Victims

Under 18	5%
18-29	29%
30-39	24%
40-49	20%
50-59	13%
60-64	3%
65 and over	6%

Source: FTC, 2006, p. 11

There was an average of 12 months between the initial identity theft incident and the discovery of victimization for victims in 2002, which was the last year this information was recorded (FTC, 2003). Out of the 81,444 victims, forty-eight percent discovered the victimization in less than one month, while five percent took over sixty months (*Ibid*., 2003, p. 7).

FTC's Identity Theft Survey Report (Synovate)

In early 2003 the Federal Trade Commission sponsored a phone survey of American households to look at the topic of identity theft and the experience of victims (Synovate, 2003).

This survey, the most comprehensive study of identity theft victimization to date, had 4,037 respondents, of which 12.7% reported having been a victim – implying that between 1998 and 2003, approximately 27.3 million Americans had been victimized (*Ibid*., 2003, p. 12). Only twenty-five percent of victims reported the crime to law enforcement, and victims over age fifty-five were the least likely to report; similarly only twenty-two percent of victims said they contacted one or more CRA's (*Ibid*., 2003, pp. 9, 12). Victims spent an average of thirty hours for recovery efforts and suffered an average of $500 in monetary loss over all forms of identity theft, but they spent an average of sixty hours and suffered an average of $1,180 in monetary loss when the offender opened new accounts in their name (*Ibid*., 2003, pp. 6-7).

FTC's Identity Theft Survey Report (Javelin/BBB)

A longitudinal update to the 2003 survey was released by Javelin Strategy & Research ([Javelin], 2005a) and the Better Business Bureau (BBB) in January 2005, using a similar methodology and employing many of the same questions as Synovate (2003). Of their sample (n=4,000), 509 indicated that they had been a victim of identity fraud; this generalizes to 9.3 million Americans in total, a statistically insignificant (at $\alpha = .05$) 7.9% drop from the 10.1 million estimated victims in 2003. Per victim, the median total cost was $750, mean out-of-pocket losses were $652, and an average of twenty-eight hours was spent to resolve credit and financial problems caused by victimization (*Ibid*., 2005a, p. 3). Though most victims' information was obtained by offenders using offline means (68.2%), 11.6% had information taken from online; specific methods of information access are found in Tables 3 and 4 on the following page:

Table 3: Offline Methods of Access to Victim Information

	Percentage
Lost or stolen wallet, checkbook, or credit card	28.8%
Friends/acquaintances/relatives with access to information	11.4%
Accessed as part of an offline transaction	8.7%
Corrupt employee who had access to the information	8.7%
Stolen paper mail/fraudulent change of address	8.0%
Taken from the garbage	2.6%
Total	***68.2%***

(Source: Javelin, 2005a, p. 8)

Table 4: Online Methods of Access to Victim Information

	Percentage
Computer Spyware	5.2%
Accessed as part of an online transaction	2.5%
Computer virus/hacker	2.2%
Emails sent by criminals posing as legitimate business ("phishing")	1.7%
Total	***11.6%***

(Source: Javelin, 2005a, p. 8)

The method of access has implications for time between initial victimization and discovery, as victims whose friends or family took their information were more likely to take three months or more to detect the crime, while those who lost their wallet or check card often discovered the incident within a day. It is also relevant to mean dollar losses, as online methods generally cost victims less than offline methods. For example, phishing schemes resulted in mean losses of $2,320, as opposed to mean losses of $15,607 when information was taken by family or friends or $9,243 from the theft of paper mail.

This survey, which asked questions about victims' behaviors prior to and after victimization, did find that behaviors changed afterwards; prior to an incident, the least used prevention methods were "reviewing statements monthly, shredding documents before discarding and retrieving mail promptly", while post-incident, more victims reviewed both their

paper-based and online statements on a monthly basis and more often monitored their billing cycles (*Ibid*., 2005a, p. 4). This is notable that the increase in prevention activity was "to the point where victims' prevention behaviors in these areas surpassed average U.S. adults' behaviors" (*Ibid*, 2005a, p. 4). Recommendations for consumers included updating their computer anti-virus and firewall software as a measure to thwart "online criminal activities".

National Crime Victimization Survey

Since 1973, the Bureau of Justice Statistics under the United States Department of Justice has sponsored the National Crime Victimization Survey. Beginning in July 2004, questions on identity theft were incorporated into the traditionally physical crime-focused structure. However, as of this writing[6], the data has not been released on these victims.

Empirical Studies

In one of the few empirical studies on identity theft specifically, thirty-seven victims completed a victim questionnaire, with thirty of them also completing a Brief Symptom Inventory (Sharp, Shreve-Neiger, Fremouw, Kane, & Hutton, 2004). It was found that the victims suffered a number of strong emotional responses two weeks after learning of their victimization, including irritability and anger, fear and anxiety, and frustration. By twenty-six weeks after, participants felt distressed and desperate. Victims also suffered from a number of physical or health (somatic) symptoms two weeks after, including difficulties sleeping, anxiety, and appetite problems; at twenty-six weeks after, anxiety was the most reported problem.

[6] Initial findings were released on April 3, 2006 and indicated that age, income, and residential location may be factors involved in determining the likelihood of victimization.

Coping methods found included calling government agencies, contacting credit bureaus, and contacting vendors.

Finally, while not specifically an identity theft victimization study, the Rochester Institute of Technology's (RIT) Computer Use and Ethics Survey (McQuade et al., 2004) led to the development of a victim profile of college students. Administered to 873 undergraduate students in the spring of 2004, respondents were asked over 160 questions that included their use and abuse of computers, their associates' perceptions on computer abuse, and their rates of high tech crime victimization. For this survey, identity theft was defined as "someone used personal information about you in order to pretend they were you"; fifty-five students indicated that they had been victimized by this misuse of information (Berg, 2005a). Based on these survey results, it was found that victims were more often male, but it was highly possible that they are female (ratio 1.3 females to 1 male), and they would probably be a White/Caucasian who was aged eighteen to twenty-three. In the area of computer proficiency, victims would generally own or control at least two devices and run Windows on their computers; had a computer in the house while growing up and have been using computers since about age ten; are generally self-taught with regards to computing knowledge; and had parents who did not provide extensive supervision of computing activities but gave them a lot of support. In the realm of computer security, most victims: used anti-virus software, though less than a third updated their virus definitions on a regular basis; would avoid opening unsolicited e-mail attachments; and used a personal firewall. Additionally, many victims also restricted their Internet browser/cooking settings. However, victims generally did not have strong passwords and did not change their passwords; even if they shared their password in the past, which they probably have done, it was not changed after. Though victims thought that computer-based incidents were on the increase at

RIT, they were not worried about RIT's computing safety. Even after having been victimized, they were not worried that they would be victimized and did not think their friends worried either (*Ibid*., 2005a).

Overall, this RIT identity theft victim profile was exactly the same profile as a non-victim, with two minor differences. First, victims perceived that more of their friends/peers commit plagiarism, engage in online harassment, and do not view sending spam as being very wrong. This would seem to indicate that victims' friends are not necessarily the most ethical people. Taking a closer look at the seventeen victims who indicated that they knew who the offender was in their case, four indicated it was an acquaintance while five said it was a friend; though the survey does not measure this, it is possible that the types of friends/peers who have positive feelings towards offending behaviors may be the types more likely to commit identity theft against fellow friends in their group. Second, there were different rates of firewall usage and the avoidance of opening e-mail attachments; more victims responded that they used a firewall than non-victims, but victims would more frequently open e-mail attachments (*Ibid*., 2005a). However, the survey instrument did not include a measure asking how victims' information may have been taken, so it cannot be determined if opening e-mail attachments was a precipitating factor in an identity theft incident. Similarly, the survey also did not ask about changed behaviors post-victimization, so it can also not be determined if the improved firewall usage came about before or after the victim's experience with identity theft.

Clearly, while steps have been undertaken in the last five years to better understand the problem of identity theft, there has been little research done in the areas of high tech crime victim profiling and prevention. Most studies, whether one-time or ongoing, focus on victim

demographics without examining ways in which their victimization may have been facilitated technologically. The attempts to look at precipitating behaviors in the context of victimization are limited. As such, a weak empirical base exists on which to generate additional research on and potential solutions to identity theft victimization. Thus, my thesis is: identity theft victimization surveys can be substantially improved by addressing a broader range of issues on the basis of existing criminological theory and previous survey findings. Similarly, my primary research questions are: in what specific ways can identity theft survey instruments be improved, what policies can be made to improve identity theft victimization prevention and treatment, and what information technology strategies can be recommended to enhance prevention efforts?

II. Methodology and Findings

A. Comparative Survey Analysis

Ultimately the value of any research will be determined by the amount and quality of data collected and analyzed, which simply means that a researcher's methodology is crucial. Generally speaking there are two basic approaches to research, namely, quantitative and qualitative, which derive their labels from the types of data collected and analyzed and the way in which research is done (Tesch, 1990). Quantitative data gathering and analysis is appropriate when researching a known or understood phenomenon, while a qualitative approach is better for the study of phenomenon which are unknown or not well understood (Creswell, 1994). This thesis draws upon these dual approaches, building upon both qualitative and quantitative research that I completed previously.

In preparation for this thesis, I undertook two independent research courses. The first produced a qualitative content analysis of 577 newspaper articles relating to identity theft that were published between 1985 and 2003. For this analysis, I developed models that visualized key variables involved in an identity theft incident, from initial theft/acquisition of the data through punishment of a convicted offender, and also identified characteristics of identity theft victims. My second independent study, previously referred to in the literature review, was a quantitative analysis of RIT Computer Use and Ethics survey data. This study examined the rates of identity theft victimization on a college campus and the traits of those victimized.

For this thesis, I undertook further in-depth analysis of the FTC, Synovate, Javelin/BBB, and NCVS survey instruments, along with my own independent research findings that profile identify theft victims, in order to develop model survey instrument questions for future research into this form of high tech fraud[7]. Specifically my thesis compares findings from previous independent studies with the Synovate and Javelin reports in order to identify gaps in each and to propose a new comprehensive framework in which to study identity theft and its corresponding victimization. Prior identity theft victimization survey instruments were examined to see what questions are currently asked of victims. The information obtained from these surveys were compared to the existing identity theft profile in order to identify weaknesses in the data gathered and make recommendations for future survey questions in order to gain further information about the victim experience.

The following figures visualize how my previous independent research (Figure 1) combines with previous surveys (Figure 2) to examine what we know and what needs to be asked in the future, while Figure 3 shows how I address the latter:

[7] Survey recommendations can be found in the Recommendations section. A model survey instrument can be found in Appendix B and its description in Appendix A.

Figure 1: Combining Previous Research

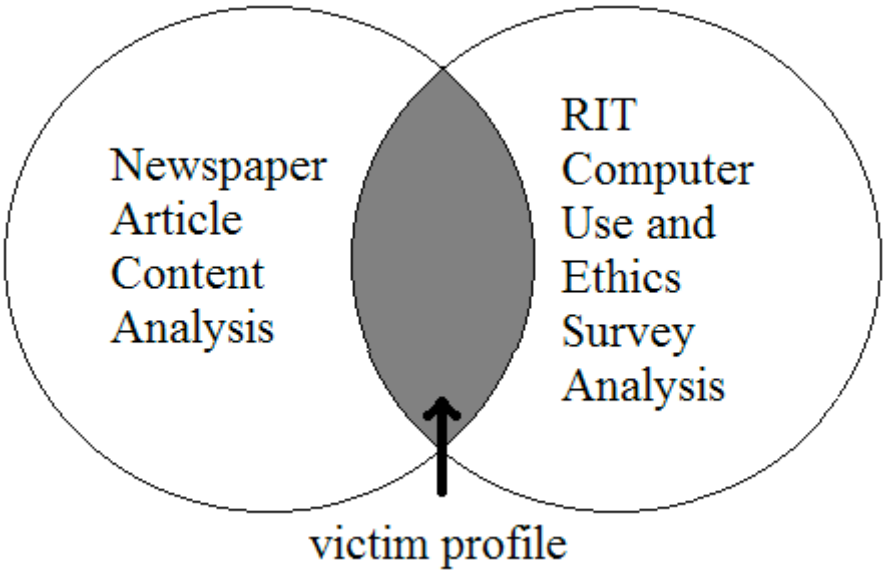


Figure 2: Survey Comparisons

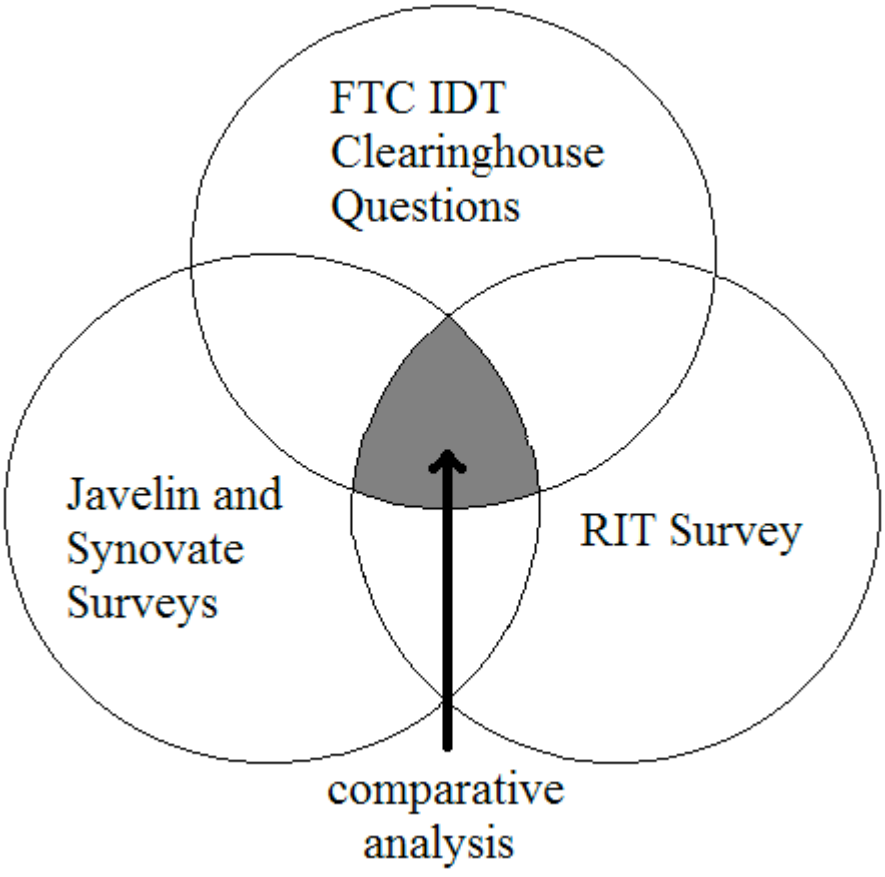
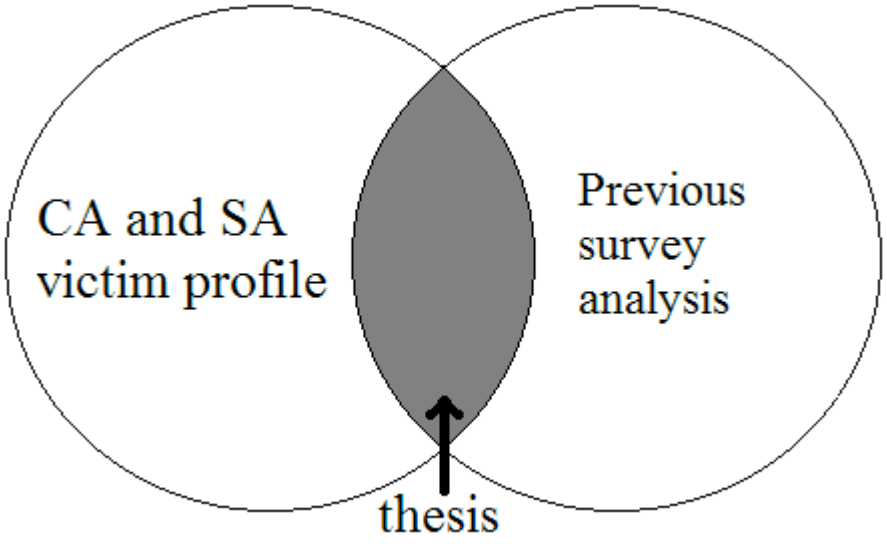


Figure 3: Thesis Research



Finally, I examined a number of information technology approaches to the prevention of identity theft. Some of these have been suggested by victims as ways in which their victimization may have been prevented or discovered more quickly. Others were discovered through my prior content analysis research as methods in which IT is either currently being used with regards to identity theft or as proposed measures to be undertaken in the future.

B. Findings

This section of my thesis document presents my three major findings from the comparative survey analysis and examination of previous study results. First, there is a need to enhance our current identity theft victim profiles. Second, there are concerns about the methodologies used in previous identity theft surveys. Third, deficiencies are present in the design of previously administered identity theft survey instruments. Each of these is discussed in the following three subsections.

The profile of an identity theft victim needs to be enhanced.

Unfortunately it is difficult to use Berg's (2005b) content analysis of newspaper articles to enhance the known profile of an identity theft victim. Out of 577 articles, only fourteen included information on a victim's age. These ranged from 26 to 59, with a mean of 38.9. Overall this is not a very representative sample, especially given that other studies provide better age-related demographic information. The FTC's 2005 Consumer Sentinel identity theft data accounts for victims from under age 18 through over age 65, with 29% between ages 18 and 29 (FTC, 2006). Of the 55 RIT victims, 48 out of the 51 respondents who marked their age were between 18 and 23 (Berg, 2005a). Clearly, younger victims were not represented in the sample of newspaper articles used.

Victims' names were mentioned 79 times, and I used their first name to derive gender. For victims with a name that was not distinctively male or female, I examined the pronouns in the article used to describe the victims, and I also used Google to ascertain the gender of two victims, both of whom were public figures. The 577 articles included 51 males, 28 females, 1 unknown, and 6 non-individuals (i.e., commercial entities)[8]. This produces a male-to-female ratio of 1.8 to 1, with nearly twice as many male victims as females in this sample. In contrast, the male-to-female ratio of Rochester Institute of Technology victims was 1 to 1.3, with females victimized more than males (Berg, 2005a). Unfortunately, looking to national surveys and statistics does not provide any additional information on the differences in victimization rates between genders. While the FTC's demographic data includes age, they have not made public any reports on gender. The Synovate and Javelin reports do not include any demographic

[8] These numbers do not add up to 79 since some victims were named in multiple articles, and one article discussed twelve (male) victims all named Paul C. Casey.

breakdowns, on neither age nor gender, for comparative purposes. However, Javelin (2005) does note that younger victims were at a higher risk of the offender opening new accounts in their name, while middle-aged victims tended to be victimized by frauds costing the largest total dollar amount.

Thus, my major finding is that current research is unsatisfactory to use in developing enhanced identity theft victim profiles.

The methodologies used for previous survey administration are problematic.

1) Telephone-Based

To date, the most comprehensive identity theft victimization surveys have been conducted via telephone. While 94.0% of United States households do subscribe to phone service[9], a growing portion of the population has chosen to solely use a cellular phone instead of a landline (Belinfante, 2005, p. 2). Since 2000, the number of landlines provided by carriers has declined, in part because of the move towards wireless service; this is in contrast to the growth experienced prior to that year (FCC, 2005). Findings from Mediamark Research's (2004) in-home interviews of 26,000 Americans show that 8.1% of U.S. households do not have a landline, up from 1.4% in 2001, with cell-only consumers having a median age of 28.8. These numbers are echoed by the Federal Communications Commission, who reported that 6.0% of households were estimated to have gone wireless, up from 1.2% in 2001 (Belinfante, 2005, p. 2). Since many individuals with cell phones have good credit and money in the bank, they are potential targets for identity thieves. However, because telephone surveys do not reach people whose only means of phone communication is a cell phone, this particular population is not surveyed.

[9] This includes users of cellular/wireless phones, in addition to landlines.

Similarly, the telephone penetration rate for households headed by an individual under age 25 is only 87.6% (Belinfante, 2005, p. 2). This is another indication that the younger population might not be reached in the national surveys, resulting in their experiences not being recognized in those findings.

In addition, individuals who cannot afford the monthly cost of telephone service would not be represented in a telephone-based survey. According to the most recent Federal Communications Commission report, while 98.5% of households with incomes between $75,000 and $99,999 had telephone service, only 79.8% of households with an income under $5,000 did (Belinfante, 2005, p. 2). While it is possible that the financial situation of the low-income population would make them less likely to be victimized, this view cannot be verified or refuted without empirical testing.

2) English-Only

Even though English is the official language of the United States, the segment of the population who speaks another language is continuously growing. This is especially true of Hispanics, with that population forecasted to grow to 102.6 million by July 1, 2050 – an increase from 41.3 million as of July 1, 2004 (U. S. Census Bureau, 2005a). As of 2004, roughly 39 million out of a total population of 212 million spoke a language other than English at home, which included 23 million Spanish-speaking U.S. residents age 18 and over (U. S. Census Bureau, 2005b). Of those, roughly half indicated that they spoke English less than "very well", including 4 million "well", 5 million "not well", and 3 million "not at all" (*Ibid*., 2005b). Based on an examination of the Synovate and Javelin instruments and methodology, it does not seem like the survey was administered to any non-English speakers. There is a 2001 Spanish-language

version of the NCVS, but the Bureau of Justice Statistics web site (http://www.ojp.usdoj.gov/bjs/cvict.htm) does not indicate if the 2004 update with identity theft questions was also administered bilingually. Given that around 18% of individuals within the United States do not speak English, this is a very large population that could be potential victims. However, again, without empirical testing, it is impossible to examine these specific victim experiences.

3) Number of Respondents

Of the three major surveys, only the NCVS asks about victimization of other members in the household. The Synovate (2003) and Javelin (2005a) surveys are focused solely on the respondent. For these studies, because only one individual is questioned, there could be others at the residence whose experience is never documented. Additionally, both Synovate and Javelin only surveyed adults over age 18. An NCVS interviewee, on the other hand, is only required to be at least 12 years of age. Given that there were about 9,300 FTC (2005) complainants in 2004 that were under age 18, Synovate and Javelin completely ignored this sector of the victim population.

Finally, nearly 300 million individuals reside in the United States, 75% of which are adults over age 18, but there were only about 4,700 respondents in the Synovate survey and 4,000 in the Javelin survey. In contrast, the National Crime Victimization Survey has a sample size of about 76,000, which increases the chance that victimization experiences will be captured. Because of the low number of respondents for Synovate and Javelin, can these responses genuinely be extrapolated out to accurately reflect the U.S. victim population? Obviously it would be impossible to survey every adult in the country; doing so would require an enormous amount of resources, between time, money, and manpower. To this end, usually clustered

random sampling is used to generate a representative sample of U.S. households. While Synovate and Javelin did use this method to obtain their sample, when compared to the higher response rate of the NCVS, it appears that there is room for improvement.

Thus, my major finding is that there are concerns with the methodologies used in previous identity theft surveys. Their flaws include administering surveys via the telephone, administering surveys only in English, and not using a large sample size.

There are deficiencies in the current survey instruments used.

While the Synovate (2003) survey was designed to capture the experiences of an identity theft victim, it did nothing to delve into the cause of their victimization. The follow-up by Javelin asked some questions concerning activities that, if not done, could facilitate victimization, but these were limited in scope. Moving beyond standard measurements, such as classifying the type of identity theft perpetrated, determining time spent recovering, or quantifying the monetary costs lost, is necessary for enhancing prevention efforts. The common belief is that any individual, regardless of their personal characteristics, may become a victim. Taking preventative steps does not guarantee that someone's personal information will not be misused. However, these generalizations are made without examining any victim or non-victim behaviors. Is someone more likely to be victimized because of something they do or do not do? Do their attitudes on victimization contribute? For example, does someone who feels that they are very likely to become a victim then take steps to minimize their perceived risk?

Similar sentiments hold true when examining the NCVS instrument. It is extremely comprehensive for capturing experiences, especially for victims of violent or interpersonal crimes, though it also does not look at victim facilitation. This could be, in part, because our

society does not like to suggest that a victim may have played a part in their victimization. Look at the outrage that follows when someone expresses the view that a rape victim should not have been wearing a certain outfit in a certain neighborhood or that a homicide victim should not have gotten mad at his or her assailant. Even with financial crimes, such as identity theft, there may be hesitation to suggest that a victim's attitudes or behaviors may have been the defining factor in their victimization.

Nonetheless, it is clear that some people become identity theft victims and some people do not. Why is this the case? If it were true that everybody was a potential victim, then wouldn't more people be victims? The Synovate survey results, extrapolated to the general United States population, suggest that as many as ten million Americans have been identity theft victims. The Javelin follow-up states that 9.3 million Americans became victims. Yet there have not been 9.3 to ten million people to come forward and say that they have been affected by this crime. Is it that, unlike a physical or interpersonal crime, a victim of an economic fraud may not know of their victimization? Could millions of individuals, even after reading the news and popular magazines extolling the dangers of identity theft, still have no clue of their status?

Or could it be that not everyone is a potential victim? Does it make a difference if people monitor their credit reports and/or credit scores? Does it make a difference if they scrutinize their credit card and bank statements every month, if not more often, looking for any possible discrepancy? Do they delete so-called "phishing" e-mails without falling victim to the financial scams contained within? Do they avoid opening attachments in e-mails from unfamiliar addresses, or ideally from any addresses at all? Are they running anti-virus software on their computer to check for viruses, trojans, and worms? Do they update the anti-virus software regular to make sure that its checking for the most recently released viruses, trojans, and worms?

Do they run programs to detect spyware and adware, and are these program definitions updated as well? Is a firewall installed to prevent potentially exploitative servers from connecting to a PC and to prevent outward exploits from connecting? It could be that these sorts of preventative activities do not matter. Alternatively, it could be that the numbers of victims are blown out of proportion. Between the Synovate and Javelin surveys, they claim that nearly twenty million individuals have been victimized, based on responses from less than nine thousand respondents.

The expanded instrument used in the Javelin (2005b) survey update was an important step in getting a fuller picture of the identity theft victim experience. Rather than solely ask about their victimization itself, questions asked about behaviors which may have facilitated the incident in their case. The majority of these are not computer-based, though they are measures typically found in recommendations for preventing identity theft. These behaviors are: shredding personal documents before discarding, using a locked mailbox, retrieving incoming mail within a few hours of delivery, depositing outgoing mail at the post office or in a locked box, and canceling paper credit card or bank statements and checking them online instead. Respondents were asked if they did do these activities ("yes"), did not do these activities ("no"), or were not sure if they did them ("don't know"); there was also an option if they refused to answer.

However, only one question focused on computer-based prevention, asking if the respondent uses anti-virus, anti-spyware, or firewall software. Previous research shows that identity theft victims employ a personal firewall more often than non-victims (Berg, 2005a). Additionally, victims more frequently open e-mail attachments than non-victims (*Ibid*., 2005a). This would seem to indicate that a wider variety of computer-based prevention behaviors should be asked about, ideally in the form of separate questions.

Thus, my major finding is that there are deficiencies in the identity theft victimization survey instruments currently used. Surveys lack questions focusing on preventative behaviors, including both their use/lack of use and their frequency of use.

III. Recommendations

A. Changes for Future Surveys

More demographic information in should be obtained from survey findings.

Examining age and gender are key in identity theft prevention efforts. Certain age groups may be more likely to engage in what would be considered risky behaviors. For example, financially unsavvy younger individuals may not regularly check their bank or credit card statements. Older individuals may not be savvy when it comes to computer security and thus not use anti-virus software or a personal firewall. A Pew Internet Project report found that there were clear differences in knowledge of Internet-related terms between younger and older adults, with those age 18-29 more likely than those age 65+ to say they knew what terms such as "firewall", "phishing", "spyware", and "adware" meant (Rainie, 2005). When examining gender, similar sentiments hold true. Men were found to be more likely than women to respond that they know the meaning of those terms (*Ibid*., 2005). In terms of overall Internet usage, the Pew Internet Project also found that men and women use the Internet in different ways (Fallows, 2005), which could open them up to different forms of computer-based victimization. Given these differences, age and gender demographics are necessary when developing educational programs to target specific populations, since the various populations do not all have the same needs.

An examination of the empirical data concerning the use of computer security techniques of identity theft victims at RIT shows that there are differences by gender. While all twenty-two female victims said they used anti-virus software, five out of the twenty-nine male victims (17.2%) said they did not use it[10]. Five female victims (22.7%) versus eight male victims (27.6%) indicated that they did not use a personal firewall. Four female victims (18.2%) said they do not avoid opening e-mail attachments, while five male victims (17.2%) said they do not. Only seven female victims (31.8%) and ten male victims (34.5%) noted that they updated their virus definitions weekly or more, with the rest updating them monthly or less; this included two females and six males who said they never updated them, and one male who was not sure about update frequency. Nearly 40% of the victims never updated security patches or were not sure if they did so, including five females and five males who never did and seven females and three males who were not sure. In contrast, among non-victims[11], about the same percentage of males (87.7%) and females (85.1%) used anti-virus software. More males than females indicated that they used a personal firewall (59.5% versus 35.6%) and avoided opening e-mail attachments (93.3% versus 81.9%). About the same percentage of non-victim males (14.1%) and non-victim females (14.4%) said they never updated their anti-virus directions. Only about 30% of non-victims never updated security patches or were not sure if they did so.

It is easy to offer general recommendations for preventative measures that individuals should follow, but do these truly help? Different sectors of the population may require different foci for educational programs. For example, if young adults age 18-29 are the ones who use anti-virus software and update their definitions daily, then education should not stress updating definitions daily. But if it is the adults over age 40 who do not regularly update virus

[10] While there were 55 victims in total, only 51 indicated their gender.

definitions, then their educational program should target this behavior. Similarly, while the RIT data is admittedly limited, and more research must be done on identity theft victimization by gender, it does show that there may be a need for different educational programs for males and females.

A number of improvements to methodologies for national surveys can be made.

Ideally, surveys should be administered in-person in lieu of being telephone-based surveys. However, the solution to developing new sampling methods to target the sectors of the population not reached by telephone is not necessarily simple. Using lists of property owners will not include renters, who are often younger and/or lower-income individuals. DMV lists of license holders will probably not contain names of those too poor to own a car or of those who live in cities with good public transportation and therefore do not need a car. Lists of registered voters are not always representative of the racial makeup of an area, and younger adults are less likely to vote as well. Census Bureau lists might work, since those are designed to be representative across the entire population for demographics such as age, gender, and income. The sample used for the National Crime Victimization Survey may be desirable as well, as it also fits these representative criteria. The use of the NCVS sample could be verified once findings are released from the 2004 version, which asked the identity theft questions.

National surveys should also recognize the large sector of the population that does not speak English or does not speak it well. At the very least, surveys should also be administered in Spanish, since that is the language spoken most often after English. Care must be taken to ensure that the translations are adequate representations, since mistranslations could change the

[11] These percentages are based on the actual number of respondents for each question, as opposed to the total number (224 females and 529 males).

meaning of the English questions. This could affect the validity of making comparisons between findings of the English survey and findings of the non-English survey, if the different surveys are not truly equivalent in meaning (Hambleton, 1992).

Questions asking about offline preventative behaviors should be enhanced.

One of the largest problems with victimization surveys is that they are focused on the incident itself, without always identifying potential risk factors. While these types of surveys are thus able to give strong demographic details about victims, the harms suffered as a result, and what specific forms the crime takes, they do not present a general picture of the victim and their experience prior to the point of victimization. However when it comes to identity theft, there are so many possible situations that may lead to victimization that it becomes difficult – if not impossible – to ask any and every question about what precipitation may have occurred. The following are a number of standard questions to help gauge an individual's likeliness towards being victimized by identity theft, derived from suggested prevention measures.

Financial savvy:

- Do they check their credit card statements? How often?
- Do they check their bank statements? How often?
- Do they check their credit records? How often?
- Do they check their credit scores? How often?
- Is the back of their credit card signed, or have they written "see ID"?
- Do they have a debit card or a credit card? If they use a debit card, how frequently do they check those statements?
- Are they subscribed to credit monitoring services that will automatically engage in this type of financial watch?

Restricting physical access to personal information:

- Do they carry their Social Security card in their wallet/purse?
- Do they carry other cards with their SSN in their wallet/purse?
- Do they leave their wallet/purse in a publicly accessible location when outside their home? If so, do they ever leave it out of sight?
- Do they shred any paperwork or mail containing sensitive personal information before disposing of it? If so, how is it disposed of?[12]

The pervasive nature of identity theft is evidenced by the fact that even those who take preventative measures to avoid becoming a victim may still end up being one. Due to the variety of methods that an offender may use to obtain personal information, there is no single way that an individual can protect themselves. Someone who frequently checks their financial records, does not carry their SSN with them, and shreds all paperwork could still be victimized. This is highlighted by the Congressional hearing testimony from Maureen Mitchell and Nicole Robinson describing their experiences:

> "My husband and I have always been financially prudent and fiscally responsible. We have always paid our bills in a timely manner, and we manage our finances prudently and responsibly. We have always exercised the normal consumer precautions to ensure our privileged financial information remains private. We have never lost our wallets, never been burglarized, we obtain the credit card receipts when we use our credit cards, we do not give our credit cards to waiters in restaurants, we do not bank on the Internet, we don't order merchandise via the Internet, and we shred our paper trash to prevent someone from "dumpster diving" and obtaining our personal information. We have never given our social security numbers out over the phone, and we had our social security numbers removed from our driver's licenses. We had also checked our credit reports in

[12] I anecdotally heard of a data breach where paperwork containing sensitive information was shredded, and the bags of shredded material were left out as trash. Enterprising individuals decided to see what they could find in the bags. Even though the paperwork had been shredded, it had been done horizontally and at the same width as each row of personal information. The individuals did not even need to tape papers together in order to recover any data.

> March of 1999 to ensure their accuracy (U. S. House of Representatives, Mitchell, 2003)."
>
> "I had always been a person who kept my Social Security card under lock and key. I never gave personal information over the phone and I always shredded and systematically discarded pre-approved credit applications. And I check my credit reports every year (U. S. House of Representatives, Robinson, 2001)."

However, it would generally hold that the more protective measures taken, the less likely it is that they will become a victim. This can be seen as an extension of routine activities theory, as engaging in prevention techniques would harden a victim target and make him or her less suitable, as well as provide capable guardianship.

Questions asking about computer security techniques should be enhanced.

While anti-virus, anti-spyware, and firewall software are all important computer security techniques, they are not the same application in practice. Anti-virus software is designed to detect any virus or worm infection on a computer, then remove it either through deletion or quarantining the infected files. Anti-spyware software is also used for detection and removal, but it is focused on adware, spyware, or tracking tools. Firewalls are used for determining what applications can and cannot be allowed through a network. The Javelin (2005b) instrument was a key step forward from Synovate (2003) by asking about the use of these techniques, but the manner in which it asked, through the use of a single question, was faulty. Since each technique is a completely separate means of prevention, a series of questions should have been asked to ascertain respondent's use, or lack of use, of individual measures. An ideal survey would also ask about other prevention measures. Does the respondent use, or generally use, strong passwords (e.g., alphanumeric passwords of at least eight characters in length that also contain at

least one symbol). Does the respondent open e-mail attachments? Does the respondent employ the latest operating system patches released? However, due to a lack of empirical data currently tying identity theft victimization to other forms of computer-based prevention measures, it cannot be stated if such acts as using strong passwords and not opening e-mail attachments will decrease victimization.

For a more accurate assessment, any survey should not merely ask if a technique is used, but instead inquire about the frequency of usage or updates. Anti-virus software is worthless if virus definitions are not updated on a regular basis. Similarly, anti-spyware software also requires updated definitions to properly identify any potential threats. Rather than limit this question to a yes/no/don't know answer, a follow-up should be: how often do you use a certain technique? Responses can range on a Likert-scale, from "never" to "annually" to "every few months" to "monthly" to "weekly" to "daily". Just as checking financial records on a regular basis is important, so too is updating computer protections. This is especially true given that software companies tend to release updates on a regular basis to reflect current computer-based threats; if someone does not keep up with this, their computer will not have adequate protection.

Additionally, previous empirical research shows that the friends or peers of victims may have illicit interests of their own, namely committing online harassment and computer-based plagiarism, and that they also do not view the sending of "spam" e-mails as being very wrong (Berg, 2005a). It is difficult to say if this would be generalizable to the non-college or university adult population who would be part of the samples of national (victimization) surveys. At least for plagiarism, once an individual is out of school, they are usually not engaging in academic dishonesty. For crime and delinquency as a whole, the age-crime curve holds that rates of criminal behavior typically drop as a person increases in age, following a peak during late

adolescence (Sampson & Laub, 1993). If seventy-five percent of FTC victims are between ages 18 and 49, with the average age of victims reported about in newspaper articles being approximately 39, this would most likely indicate that these individuals are at a stage in their life when they are not engaged in illicit activities. Combined with the anecdotal statement "birds of a feather flock together", friends of the victim are probably not engaged in illicit activities either. Still, the only way to verify this empirically would be to include measures of friends' behaviors in an identity theft study.

While support remains limited for routine activities theory tied to high tech crime, and specifically identity theft, victimization, it is nonetheless important to recognize that engaging in certain online behaviors may make an individual more prone to becoming a victim. For example, one recommendation in the Javelin (2005a) report is for consumers to ignore Internet links contained inside an e-mail and instead type the URL (web address) directly, in order to avoid falling victim to a phishing scheme. In this fashion, the common online activity of "receiving e-mail" could make someone more likely to be victimized. However, while questions are asked concerning prevention activities, nothing is asked about victims' Internet use. Do they shop online, pay for online pornography access or engage in online gambling? Out of the 11.6% of Javelin (2005a) victims who reported that their information had been taken through online means, 2.5% indicated it was accessed during an online transaction. Do they surf the web? 5.2% indicated that their information was stolen due to computer spyware; this could have been installed when they accessed certain web pages. Do they engage in online chatting (i.e., instant messaging)? This could also open an individual to virus infection or chat-based phishing attempts.

Computer security and computer proficiency are certainly important to an extent, given that identity theft may be facilitated through online methods and computer-based contact, but these are not absolute. Preventative methods via computer could be indicative of an individual's larger prevention strategy, though; the person who does not update their anti-virus software on a regular basis may also be the person who does not check their credit card statements monthly. Overall, in order to develop effective educational programs, more research must be done to ascertain where the failures that facilitate identity theft are occurring. Asking the above questions about both online and offline prevention techniques will help educators and policymakers determine what consumer behaviors could be resulting in victimization.

B. Prevention and Treatment Policies

There is a need for improved organizational accountability.

Organizations should be held accountable for any actions, or the lack thereof, that may lead to a potential data breach. Laws similar to those passed in California and New York could be the solution to this sort of problem. California's Security Breach Disclosure Act (2002) requires companies to inform their customers if their personal information may have been compromised. New York's Information Security Breach and Notification Act (2005) requires entities conducting business in New York State to inform New York residents and three New York state offices to disclose any breaches in computerized data containing private information. While, as a consumer, we might hope that a company with which we do business would inform us if they have lost tapes of customer data or been hacked into, for example, there is no guarantees that they will. It may only be through the use of governmental regulation that this

action would occur. Laws such as this one would then encourage companies to engage in protective measures to ensure that access to customer data remains secure. According to the Javelin (2005a) report, victims whose information was stolen due to a lost wallet, checkbook, or credit card were able to more quickly discover that they were victimized than if the information was taken in other ways. If an individual does not know that an organization with which they do business lost their data, they may not become aware of their victimization. The greater the time period before victimization is discovered, the harder it can be for a victim to recover, especially if the offender has been able to use the victim's identity on a long-term basis.

Accidents can and do happen, since the loss of customer data by a company does not necessarily make them negligent. However, whatever the reason for the loss, timely notification for the individuals with compromised information can enable them to file fraud alerts, cancel credit cards, and otherwise monitor their financial records track of any data misuse. Disclosure laws may also reduce the chance of accidents by increasing corporate awareness of the data protection component of their business. If an organization knows that they will be subject to penalties for not securing their data properly, they will take steps to prevent a breach from occurring.

Employees must also assume liability if their actions or inactions lead to victimization. For example, if an offender uses a victim's credit card at a store, the card has "see ID" written on the back signature panel, and the employee does not verify identity by asking to see photo identification, some of the blame should rest on them. If a loan or credit application is turned in with obviously incorrect information, which can happen if an offender does not know all the correct victim data, it should be red-flagged by an employee instead of automatically passed through. Corporate policies, either internally developed or mandated by the government, should

include both steps that employees should take to do their part to protect consumers and provisions for the disciplinary actions that will be taken if they fail to do their job. Again, accidents could occur due to human fallibility, but there should be measures in place that will reduce or minimize negligence and lack of knowledge.

Financial companies require improved regulation.

Inside the financial services industry, losses from the various fraud crimes that make up identity theft continue to grow. Secret Service financial crimes investigation found identity fraud cost $442 million in fiscal year 1995, $450 million in fiscal year 1996, and $745 million in fiscal year 1997 (U.S. General Accounting Office [GAO], 1998). In 1997, credit card company losses for Visa were $490 million out of $505 billion, with fraud representing 0.1% of all transactions, while MasterCard losses in 1997 were $407 million out of $365 billion, representing 0.11% (*Ibid.,* 1998). The American Banker Association's 2000 banking survey found that the 1999 check fraud losses to be $2.2 billion, with an average of 29% of this being attributable to identity theft across all banks (GAO, 2002). Gartner estimated that 1% of all of bank and credit account applications are fraudulent, with a major cause being identity theft (Litan, 2003). Synovate (2003) found that all forms of identity theft cost the financial industry, including businesses, $47.6 billion total and an average of $4,800 per victim. Two years later, the total cost to the financial industry and businesses was $52.6 billion, and a mean per victim of $5,686 due to a few large dollar cases (Javelin, 2005a).

However, as long as overall profits remain high, it seems there would be little incentive for financial companies to modify the way they do business. As Secret Service agent Greg Metz has noted, "[i]f a bank knows they are going to make $100,000 off a particular product, but incur

$10,000 in fraudulent losses off their bottom line, it's still $90,000, so who's going to win that battle?" (Cate & Marra, 2002, para. 15). Any monies spent on prevention efforts are monies that get taken out of a company's profit. In order to stay competitive, companies must keep their costs down and profits high. It is doubtful that an individual company would take the step to change their practices on its own, without government regulations requiring them to do so. While increasing prevention efforts might enhance their public image and make them more attractive to consumers, unless they also dramatically increase profit margins, a small amount of good PR will not be a good enough reason for a change.

Whether they are mandated to engage in prevention efforts or choose to do so, there are a number of measures that can be taken. Bank tellers should always be required to see photo identification for anyone doing a transaction. More credit cards should include the customer's photograph on the front, much as Citibank does now. Credit card issuers should track purchases made on a card and notify the card holder if there is an unusual pattern of activity; commercial software products are available for this purpose. Organizations should employ a system that allows customers to generate a "disposable", single-use credit card number for online purchases, much as American Express and Citibank do now; this number should also only be good for a short amount of time (e.g., thirty days) to ensure that its usefulness is limited in case it falls into the wrong hands. Since financial companies often run credit report checks on their customers, they should notify them in the case of any changes. Similarly, credit reporting agencies should verify information before they add it onto an individual's credit report, as it can be very difficult to remove the incorrect data generated on these reports due to identity theft victimization. Change of address requests should be verified over the telephone with a call to the phone number on record for the account and/or in writing to both the new and old addresses. Finally,

organizational policies should detail how personal (customer) information should be handled, including disposal mechanisms for any printed material.

There is a need for improved individual accountability.

Any potential government regulation of either commercial merchants or the financial services industry, however, does not minimize the need for individuals to take control over their own protection. Someone who carries their Social Security card in their wallet or enters their credit card number over an unsecured web site should also be held accountable for their bad choices. Still, many of these bad choices can be due to a lack of education in the area of prevention. If an individual is unaware that what they are doing or not doing may make them more prone to victimization, they need to learn what is correct or incorrect behavior.

This accountability may be enforced by making a victim responsible, at least in part, for monetary costs stemming from their victimization. Current United States credit laws typically limit consumer liability to fraud from credit cards to $50, though many institutions will waive even this charge (FTC, 1999). Debit/Automated Teller Machine (ATM) card or other electronic funds transfer fraud results in a $50 liability if caught within two days, though this amount increases to $500 after sixty days and could be unlimited (up to the full value) after the sixty days (Federal Deposit Insurance Corporation, 2003). To offset these high losses, companies pass along to consumers the costs of "check fraud-losses, legal fees, increased insurance premiums, and higher banking costs … in the form of higher interest rates and other financial institution fees" (Collins & Hoffman, 2002, para. 4). Certainly, in cases when an individual engaging in prevention behaviors or whose information is otherwise obtained through no fault of their own is victimized, they should not be held fully liable. But increasing consumer penalties may reduce

victimization stemming from negligence. They might also decrease the higher fees that non-victim consumers pay, by placing more of the financial burden for losses on these careless individuals.

Victim treatment policies should be improved.

While victims of violent crimes can often be assisted by established services, it can be harder for an identity theft victim to get the help he or she needs. There is still no single place an individual can turn to when they discover their victimization. The FTC's (2002) ID Theft Affidavit was designed to let victims make a single report to list all fraudulent accounts opened by an offender, and this would then be distributed to the creditors, financial companies, or commercial merchants in question. However, it is not accepted everywhere, so victims may still need to file multiple reports. Victims must also separately contact law enforcement agencies to file police reports and credit reporting agencies to place fraud alerts on their account. Law enforcement agencies do not always have the information or personnel resources to assist victims, let alone investigate those sorts of crimes. Even at the federal level, where employees may be better equipped to handle incidents of identity theft, investigations will not typically take place unless the monetary loss has reached a certain amount. While there are certainly victims who have lost thousands or hundreds of thousands of dollars, most lose more time than money and thus may be unable to be helped by law enforcement.

Beth Givens (2000) of the Privacy Rights Clearinghouse noted that identity theft victims feel "violated, helpless, and angry". One woman described her victimization as "emotional and psychological trauma" and noted that her friends labeled it as "financial rape" (Mitchell, 2003). Economic crime victims have likened their experience to "psychological mugging" (Office for Victims of Crime, 2000, p. 1). Victim services programs need to recognize that these

individuals, while affected in a different way than those who have been hurt by a violent crime, are still in need of assistance. Much as crisis hotlines exist for issues such as cancer, sexual abuse, suicide, domestic violence, substance abuse, and now even hurricane Katrina, an identity theft hotline would provide a knowledgeable individual with which a victim could talk. This would let them obtain any information they need that would help with recovery efforts, but perhaps more importantly it would give them a supportive someone who would listen to their frustrations. Commercial merchants and the financial services industry could also provide their own support service to their customers who have been victimized. They would then be able to tailor the information provided to their own organization, including any steps that must be taken that are specific to their business.

There needs to be a true central clearinghouse for victims. This type of organization would be similar to the FTC's consumer complaint line, allowing people to call in with questions about identity theft or report a victimization, but they would also handle follow-up telephone calls to businesses, credit reporting agencies, financial companies, and law enforcement agencies. It could also be used in conjunction with the existing ID Theft affidavit, giving the employees staffing the hotline a list of places to contact about an individual's victimization. This would help eliminate the run-around that victims often get when they must call multiple organizations to dispute charges or incorrect information and otherwise take the steps towards recovery.

Policies also need to be in place to address how victimization incidents are handled by the commercial and financial sectors. Currently the burden of proof is often on a victim to prove who they are when they contact organizations to report their victimization. However, this burden of proof should be on the issuing party of a transaction even prior to the identity theft incident

being able to occur. Proper identity verification measures, such as those described in the following section, should take place to ensure that the individual whose SSN or other information is being used is the person actually using the information. These policies should be true of collection agencies as well. They should have to prove that a victim was the individual who opened an account, made purchases, or engaged in other fraudulent transactions, as opposed to the victim having to prove that they were not the person involved. The same requirements should also hold true for collections agencies that were sold an original account, especially given that merchants may be too quick to sell off these fraudulently opened accounts without making sure of the correct owner of the information used to open them. Because of the difficulty in clearing incorrect information and entries off of a credit report once it has been recorded, better identity verification, discussed below, is needed to prevent a fraudulent account from being opened at all.

C. Information Technology Prevention Strategies

More employee and consumer training is needed.

While the problem of identity theft is a complex one, not all of the solutions presented in the area of prevention need to be. On the simple end, more training for commercial and financial employees will make them more aware of how to prevent victimization. Employees, after their training, should be able to recognize situations that have the potential of leading to identity theft victimization and know what steps they can take in order to stop them. This training can be implemented using IT by offering computer-based instructional modules combining text, audio, and video. Instead of static training videos, interactive methods might better engage an individual and provide a means of testing if content is being learned. Using the concept of

Intelligent Computer-Based Instruction (ICBI), scenarios could be designed and given to employees to test them. If the employee fails at recognizing a potential identity theft incident or fails at identifying prevention measures that should be taken, their training can then be targeted to address specific weaknesses. The use of a game as an immersive instruction tool is also touted as generating meaningful learning, and its players are able to apply what is learned in the real world (Foreman, 2003). Combining these two techniques could overcome the direct learning weaknesses generally seen in gaming situations, as games are not necessarily conducive to supporting educational aims (Siemer & Angelides, 1995, p. 1376). An intelligent simulation would adapt to the individual's educational needs, assess learning achievement, and provide immediate feedback to the user about their progress (*Ibid*., 1995).

Similar training mechanisms could be developed for consumers as well, testing them on general identity theft prevention concepts. While there would not be the same sort of mandates for individuals to engage in this training as would exist for corporate employees, there are nonetheless situations in which it could be in effect. Schools, especially colleges and universities, can incorporate prevention education training as part of other classes, in standalone seminars, or during new student (e.g., freshman or transfer) orientations. Training modules could be part of software installations; instead of merely checking a box to show that they have read the licensing agreement, the user must also pass a "security awareness test" before they can complete the installation process. This method is similar to what some places already require of users before they can initiate Internet connections on their PC, where they must first obtain a passing score on a computer security quiz prior to obtaining an Internet Protocol (IP) address. An expanded version of this quiz would allow for the interactive scenario training described

above. It could also be used by Internet Service Providers as a means to ensure their users have knowledge about proper security protections before they first go online.

Improved computer security techniques should be used.

Consumers are not the only ones who could fall victim to a computer-based identity theft incidents. Commercial and financial organizations, as the keepers of customer personal information, may also be targets. It is not enough to merely recommend that individuals follow good computer security techniques on their own systems; organizations must do as well. This includes running anti-virus software and regularly updating virus definitions. Firewalls should be set up with properly set Access Control Lists to allow only permitted network traffic in and out of a company intranet. All machines should be updated with the most recent operating system and software patches to prevent vulnerabilities from being exploited. Employee workstations and company mainframes should be protected by strong passwords that are difficult for outsiders to guess or for dictionary cracker programs to hack. Internally-used software applications should be designed in a manner that limits data access to solely those employees who need it for their work. In addition, while not specifically an IT-method, all computer systems should also have physical protection in place that restricts their access to both inside employees and outside individuals.

Personal identity should be better validated.

The United States is a land of instant credit, which is one factor in the increased growth of identity theft. Merchants are often unwilling to alter their processes to help prevent identity theft if they feel that this it will create difficulties in consumers being able to obtain credit (Sullivan, 2004). It has been said that "[f]inancial services providers (FSPs) might be

encouraging identity theft through aggressive marketing practices" including "[t]he mass mailings of pre-approved applications" (Wheatman, Hunter, Behrens, De Lotto & Litan, 2002, para. 2). According to the Gryphon Foundation (2001), "[b]ecause of competitive pressures, many creditors will not take time to confirm the identity of the person who accepts the pre-approved offer. For businesses, the economic incentive is to write off losses due to credit card fraud as a cost of doing business" (para. 30). This stance has created fiction between victims, who complain that the commercial industry has not done enough to prevent victimization, and merchants, who do not want to lose potential customers if credit authorization takes too long. Clearly, there must be a compromise that will offer better identity verification that will not take the "instant" out of "instant credit". As computing resources improve and connections become faster, commercial merchants could have high-speed links to a verification database server. Since it is not merely enough to check that a Social Security number is valid in order to prevent identity theft, the assorted pieces of data which comprise an individual's financial identity must also be validated to be sure that they match together correctly. Is the address given on a credit card or loan application the correct address on file? Is the date of birth correct? Does the mother's maiden name match? This computerized checking is important, as various technical systems can catch fraudulent activity more accurately than humans alone, but IT is not infallible. To that end, human workers must also do their part to verify identity, providing a dual-layer system of man and machine working together.

While credit card numbers are certainly powerful, the numbers of incidents that stem from fraudulent Social Security number use illustrate an even greater power. The Social Security number is a key piece of information for an offender, as it is an identifier within various databases in the United States. Even when other data is faulty, a valid SSN can open many

doors. On any application, the name, address, date of birth, and other fields may all be incorrect, but as long as the SSN is right, it is extremely easy for the offender to get credit, loans, or other lines of finance. Again, validation systems need to be employed here to detect potential misuses of personal information and ensure that an individual cannot gain access to existing or new accounts, or commit other fraudulent acts, with only a single piece of victim data.

Validation processes must be undertaken regardless of if the application or transaction is made online or offline (e.g., in a store or at a bank). The address and other information given in an application should be checked to see if they match what is on file in an individual's credit report. It is not enough to check to see if the SSN is correct, as noted above. Signature analysis programs could also be used to verify that the signature being given is the correct one for the named individual. A database of signatures could be stored for a company, then every time a person does business with them, their signature would be checked against the database.

Database modification should reduce or eliminate the use of Social Security numbers.

As previously noted, while the original intent for Social Security numbers was that they would remain used as unique identifiers solely within the Social Security Administration, today they are used in a variety of organizations. Ideally, the use of a SSN as an individual's main identifier in assorted databases should be eliminated, or at least scaled back. Because its easy availability in everyday existence has helped set the conditions for its misuse, reducing its widespread usage would result in a reduced risk of identity theft victimization. To do so, the SSN would need to be replaced with some other unique identifier and any forms of identification that previously listed the SSN would need to be reprinted with the new ID number. While businesses may not have taken this action by claiming that it is prohibitively expensive, the costs of these modifications have been said to be negligible compared to organizational preparation for

the year 2000 calendar change (Computer Professionals for Social Responsibility, 2002). In practice, though, "the costs of identity theft and loss of privacy may outweigh the institutional costs of modified database practices" (*Ibid*., 2002, para. 10). Multiple victims have urged Congress to stop the United States' reliance on using SSNs, or to at least protect them better (U. S. Senate, Twentyman, 2002; Robinson, 2001; U. S. House of Representatives, Stevens, 2000c). By continuing to facilitate victimization through an over-reliance on Social Security numbers, companies may eventually lose customer business because the customers start losing trust in the company.

Law enforcement resources should be improved.

Like any interstate crime, committed in a location different from that of the victim's residence, identity theft poses unique challenges for law enforcement. Local law enforcement may not be equipped with the means to investigate in a different area than their own, or, even if they have the ability, they may not want to engage in investigative efforts outside their jurisdiction. While federal agencies do have the capability to investigate interstate crimes, these must be serious enough for the agencies to examine, which often requires either a high amount of monetary harm or victimization of the government itself (e.g., document fraud or benefits fraud). The use of the Internet as a facilitator of criminal activity also increases the number of interstate offenses. This requires more cooperation among law enforcement agencies at the local and state level, as well as federal involvement in the more serious cases, for proper investigations to occur. However, as crimes committed become more technical in nature, federal agencies may be better equipped to handle investigations due to their access to specialized knowledge and equipment. Training for law enforcement should address these needs, by giving officers the ability to

understand the ways in which IT can used to commit crimes. This could be done in a similar manner to the interactive techniques proposed for corporate employee training, by developing scenarios used to test police officers' knowledge and adapting them to each individual.

If agencies are already overworked with the investigation of other types of offenses, especially physically serious crimes such as murder, rape, or robbery, then the financial crime of identity theft may have a lower priority. After the FBI told Robert Anderson that, "in California … they really couldn't get into cases like this or …any kind of a personal theft thing unless it rose to the level of $250,000", the Inspector General's office told him that "they could not do anything because of the burden of the backlog of beneficiary theft" (i.e., mail theft of Social Security checks) (U. S. House of Representatives, Anderson, 1999). Robert Horowitz had a similar experience, being "told … by more than one of the companies [he] dealt with [that] they're not going to attempt to catch the criminal because the amount of fraudulent activity was not significant enough" (U. S. House of Representatives, Horowitz, 2000b). He also "[came] to the conclusion that the police are overwhelmed by this type of crime, simply too many cases and not enough manpower" (Horowitz, 2000b).

One solution to the resource problem is the development of centralized law enforcement databases that allow agencies to share their information about identity theft cases. Similar to databanks such as AFIS (Automated Fingerprint Identification System) or CODIS (Combined DNA Index System), a national system would let any local, state, or federal jurisdiction have access to each others' victim complaints. This can be done by allowing complaints or police report information to be entered at a lower-level database and propagated upwards through the system, and vice versa. Using this method, except for time periods of replication between databases, each jurisdiction would have a complete copy of the database at any time. Agencies

could then use these databases to compare complaints from their jurisdiction with that of another jurisdiction with a goal of matching offender motives or identifying patterns of offending behavior. Geographic Information Systems (GIS) technologies could be used to create comprehensive maps of victim, offender, and commercial or financial business information, including demographics such as victim residence, offender residence (if known), counts of victims by geographic area, or locations of commercial or financial businesses where fraudulent transactions occurred. Information could also be compared to the demographics of the local area to record trends in such data as age, gender, income, or race, and this can also be used for targeted prevention efforts.

While the FTC does provide access to its Consumer Sentinel database to law enforcement agencies, it only contains victim information for those individuals who specifically call the FTC or make an online complaint. An identity theft database like AFIS or CODIS would ideally contain information on a separate set of individuals – those who contact law enforcement. However, the concern is always that there are low rates of reporting victimization. In 2005, 30% of 245,881 FTC complainants reported that they notified law enforcement of their victimization and a report was taken (FTC, 2006, p. 15). Another 9% said that they notified law enforcement but a report was not taken (*Ibid*., 2006, p. 15). Similarly, only about 25% of all Synovate (2003) victims reported the crime to local police, though this increased to 43% of victims of new accounts and other frauds (p. 9). Reporting rates also increased as the monetary harm increased; only 23% reported to police if their loss was $1,000 or less, but 74% reported if the loss was $5,000 or more (*Ibid*., 2003, p. 47). Among college students, out of 49 victims at RIT, eight indicated that they had contacted police or law enforcement. These low figures could mean that

a major limitation of creating a national database would be that only a small number of total victimizations would be added to it.

IV. Conclusion: Does IT Matter?

In the United States, while we pride ourselves on our independence and self-responsibility, there is only so much we can do to protect ourselves against financial crimes. Personal information, including names, addresses, dates of birth, or telephone numbers, is easily available, whether via the Internet or due to its existence in a multitude of corporate and financial databases. Social Security numbers are frequently used on a widespread basis; a SSN may serve as the driver's license number in some states, a student ID number at any number of colleges and universities, or a patient ID number for insurance companies. Given this ubiquitous nature of personal information, I pose the question: "Does IT matter?" Can information technology strategies truly make a difference when it comes to prevention efforts? Even when we are unwilling to give out our Social Security number over the phone to a utility company, for example, that number is going to be accessible to someone who wants to find it. Similarly, steps we take to protect ourselves may go for naught in the absence of protective measures on the part of the commercial or financial industries. This works to limit how much a person can prevent their victimization, if a risk factor is beyond their control.

In an ideal situation, IT strategies do matter. While these measures may not fully prevent identity theft, even some prevention is better than no prevention. But in the end, no matter how strong the information technology strategies are, prevention comes down to the human element. Even if technologies are put in place on the server-side, the instant an employee answers a question over the phone that they shouldn't, or brings a laptop into work, or shares a password,

or does any number of other activities, IT becomes worthless. On the consumer end, an individual who doesn't configure their personal firewall properly or whose computer is powered off during the time periods that its anti-virus software is trying to update to the latest virus definitions will also not be protected by the technology. Security is only as strong as its weakest link. This highlights the importance of employee or consumer training to address weaknesses than IT cannot prevent.

Perhaps the key may be the "illusion of security"; even if IT efforts are not effective in reality, it is more important that they have the appearance of minimizing victimization. Consumer victims have offered their own recommendations for what they would like to see commercial merchants and the financial services industry do to assist in prevention, including IT-based measures. It is impossible to say if their victimization would still have occurred had these measures been in place at the time, but it is also possible that the offender may have been stopped before any identity theft incident could have been initiated. Victims may be less outraged at corporate entities if they felt that the commercial and financial sectors at least attempted to prevent identity theft, either due to good human practices or effective IT measures, instead of doing nothing at all.

What also matters is the need for further research to examine the nature and extent of the problem known as identity theft. Over seven years after it was first made a federal crime, we have minimal data about its victims. The national surveys do not address what may be the most pertinent questions concerning facilitation of victimization through bad consumer practices. In the case of the Javelin (2005a) study, only cursory findings have been made publicly available; for an individual or organization to get access to the full report, it will cost them $2,500. While known survey findings can be used to assist with prevention efforts, the questions being asked of

victims or individuals are not designed to make prevention a main goal. Surveys, instead of being reactive, should be proactive. They need to take into account the recommendations I have made above, especially concerning the individual's use, or lack thereof, of preventative behaviors. Additionally, findings must reflect additional demographic characteristics so that weaknesses in prevention behaviors can be identified in specific populations, thus providing the basis for targeted educational programs.

Identity theft crimes affect millions of Americans each year, presenting a reality that is not easily addressed. We are living in an era where the problem of identity theft is huge and cannot be ignored. Government agencies and research institutions need to step in and ask the important questions of residents that will not only find out how this crime has victimized them, but discover what behaviors and attitudes may have contributed to their situation. Prevention education programs should be focused on specific population groups and tailored to what they need most to learn. Finally, the use of information technology strategies should enhance prevention efforts while at the same time not minimizing the need for human intervention and involvement. Even if identity theft cannot be stopped, various sectors of United States society must work together in order to try. This thesis is only a beginning to help us understand this complex problem, but hopefully it will provide answers towards a solution.

V. References

Bard, M. & Sangrey, D. (1979). *The crime victim's book*. New York: Basic Books, Inc.

Becker, H.S. (1964). *The other side: perspectives on deviance*. New York: The Free Press of Glencoe.

Belinfante, A. (2005, November). *Telephone subscribership in the United States (data through July 2005)*. Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division. Retrieved December 22, 2005, from the Federal Communications Commission Web site: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-262084A1.pdf.

Berg, S. (2004). *Identity theft: Business victimization*. Unpublished manuscript, Rochester Institute of Technology, Rochester, NY.

Berg, S. (2005a, November). *Rates and traits of identity theft victimization among college students at a technology institute*. Paper presented at the American Society of Criminology annual meeting, Toronto, Ontario, Canada.

Berg, S. (2005b, May). *What in general are the causes, correlates and factors surrounding the occurrence of identity theft?* Unpublished manuscript, Rochester Institute of Technology, Rochester, NY.

Berghel, H. (2000, February). Digital village: Identity theft, Social Security numbers, and the Web. *Communications of the ACM*, 43(2), 17-21. Retrieved October 1, 2003, from the ACM Digital Library.

Braithwaite, J. (1997). Poverty, power, white-collar crime and the paradoxes of criminological theory. In M. McShane & F. P. Williams III (Series Eds.), *Criminal justice: Vol. 3. Criminological theory* (pp. 66-84). New York: Garland. (Reprinted from *Australian and New Zealand Journal of Criminology, 24*, 40-48.)

Brooker, K., & Levinstein, J. (2004, February 23). Just one word: Plastic. *Fortune*, *149*(4), 125-130.

Cate, K. & Marra, T. (2002, May 3). Standard rises for federal ID theft cases. *The Tampa Tribune*.

Clinard, M. B. & Meier, R. F. (2001). *Sociology of deviant behavior* (11th ed.). Fort Worth, TX: Harcourt College Publishers.

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

Collins, J. and Hoffman, S. (2002, January 15). "*Corporate" identity theft: A new twist*. Retrieved February 4, 2004, from the MSU Identity Theft Partnerships for Prevention Web site: http://www.cj.msu.edu/~outreach/identity/news4.html.

Degen, R. A. (1987). *The American monetary system: A concise survey of its evolution since 1896*. Lexington, MA: Lexington Books.

Elias, R. (1986). *The politics of victimization: Victims, victimology, and human rights*. New York: Oxford University Press.

Evans, D., & Schmalensee, R. (2003). *Paying with plastic: The digital revolution in buying and borrowing*. Cambridge, MA: MIT Press.

Fallows, D. (2005, December 28). *How women and men use the Internet*. Retrieved December 29, 2005, from the Pew Internet & American Life Project web site: http://www.pewinternet.org/pdfs/PIP_Women_and_Men_online.pdf.

Fattah, E. A. (1991). *Understanding criminal victimization: An introduction to theoretical victimology*. Scarborough: Prentice-Hall Canada.

Federal Communications Commission. (2005, June 21). *Trends in telephone service*. Wireline Competition Bureau, Industry Analysis and Technology Division. Retrieved December 22, 2005, from the Federal Communications Commission Web site: http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/trend605.pdf.

Federal Deposit Insurance Corporation. (2003, August 22). *Correcting bank account errors*. Retrieved December 9, 2003, from the Federal Deposit Insurance Corporation Web site: http://www.fdic.gov/consumers/consumer/information/shopprot.html.

Federal Trade Commission. (1999, March). *Fair credit billing*. Retrieved December 9, 2003, from the Federal Trade Commission Web site: http://www.ftc.gov/bcp/conline/pubs/credit/fcb.htm.

Federal Trade Commission. (2001a). *Identity theft complaint data: Figures and trends on identity theft: January 2000 through December 2000*. Retrieved September 18, 2003, from the Federal Trade Commission web site: http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2000.pdf.

Federal Trade Commission. (2001b, January). *Pretexting: Your personal information revealed*. Retrieved September 18, 2003, from the Federal Trade Commission Web site: http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm.

Federal Trade Commission. (2002, February 5). *Federal Trade Commission announces ID Theft Affidavit: New form simplifies process for thousands of ID theft victims*. Retrieved May 20, 2005, from the Federal Trade Commission Web site: http://www.ftc.gov/opa/2002/02/idtheft.htm.

Federal Trade Commission. (2003, January 22). *Identity theft victim complaint data: Figures and trends: January 1 – December 31, 2002*. Retrieved October 1, 2003, from the Federal Trade Commission for the Consumer Web site: http://www.consumer.gov/idtheft/charts/CY2002OverallCharts.pdf.

Federal Trade Commission. (2006, January). *Consumer fraud and identity theft complaint data: January - December 2005*. Retrieved January 29, 2006, from the Federal Trade Commission for the Consumer Web site: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

First National Bank of Sullivan. (n.d). *Identity Theft*. Retrieved September 29, 2003, from the First National Bank of Sullivan Web site: http://www.firstsullivan.com/theft/theft.htm.

Fletcher, J. D. (2003). Victims of victimless crime. In J. Sgarzi & J. McDevitt (Eds.). *Victimology: A study of crime victims and their roles*. (pp. 309-330). Upper Saddle River, NJ: Prentice Hall.

Florian, E., Burke, D., & Mero, J. (2004, July 26). The money machines. *Fortune*, *150*(2), 100-104.

Foreman, J. (2003, July/August). Next generation: Educational technology versus the lecture. *EDUCAUSE Review*, *38*(4), 12-22.

Gryphon Foundation. (2001, December 27). *Gryphon foundation newsletter, volume number 6*. Retrieved February 5, 2004, from the Gryphon Foundation Web site: http://www.gryphonfoundation.com/winter_2001.htm.

Gulotta, G. (1984, January). New approaches to victimology. *International Review of Applied Psychology*, *33*(1), 87-95.

Hambleton, R. (1992). *Translating achievement tests for use in cross-national studies*. (Doc. Ref.: ICC454/NRC127). Paper prepared for the Third International Mathematics and Science Study (TIMSS).

Hibbert, C. (2001, December 10). *History and significance of the Social Security number*. Retrieved October 1, 2003, from the Computer Professionals for Social Responsibility Web site: http://www.cpsr.org/cpsr/privacy/ssn/SSN-History.html.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge: Ballinger Publishing Company.

Information Security Breach and Notification Act, A04254A, New York, Assembly (2005). Retrieved January 12, 2006, from the New York State Assembly Web page: http://assembly.state.ny.us/leg/?bn=A04254.

Javelin Strategy & Research. (2005a, January). *2005 identity fraud survey report.* Retrieved December 16, 2005, from the Javelin Strategy & Research Web site: http://www.javelinstrategy.com/reports/documents/2005_Javeln_Strategy_Research_Identity_Fraud_Survey_Complimentary_Report.pdf.

Javelin Strategy & Research. (2005b, January). *2005 identity fraud survey report: Identity fraud questionnaire*. Retrieved December 16, 2005, from the Research and Markets Web site: http://www.researchandmarkets.com/reportinfo.asp?report_id=297455.

Johnston, D. (1996). Introductory remarks. In J. Helmkamp, R. Ball, and K. Townsend (Eds.), *Definitional dilemma: Can and should there be a universal definition of white collar crime?* (pp. 1-4). Proceedings of the Academic Workshop, June 22-24, 1996. Morgantown: WV: National White Collar Crime Center.

Kennedy, D. B. (1983, December). Implications of the victimization syndrome for clinical intervention with crime victims. *Personnel & Guidance Journal*, *62*(4), 219-222.

Klebaner, B. J. (1974). *Commercial banking in the United States: A history*. Hinsdale, IL: The Dryden Press.

Lilly, J. R., Cullen, F. T., & Ball, R. A. (2002). *Criminological theory: Context and consequences* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Lin-Fisher, B. (2001, June 12). Huge purchase by imposter pushes identity theft victim into spotlight. *Akron Beacon Journal*. Retrieved October 1, 2003, from Academic Search Elite via Ebsco.

Litan, A. (2003, November 12). *Application fraud and rising identity theft plagues banks*. Retrieved February 4, 2004, from the Gartner Web site: https://www2.rit.edu/~gartner/research/118400/118450/118450.html.

McQuade, S. C., III. (1997). *So-called "cybercrime": Its nature and manageability: An appendix report submitted for inclusion in the President's commission final report on critical infrastructure protection*. Unpublished manuscript, Institute of Public Policy, George Mason University.

McQuade, S. C., III. (1998). *Towards a theory of technology-enabled crime*. Unpublished manuscript, Institute of Public Policy, George Mason University.

McQuade, S. C., III. (2001). *Cops versus crooks: Technological competition and complexity in the co-evolution of information technologies and money laundering*. Unpublished doctoral dissertation, George Mason University.

McQuade, S., Castellano, T., Berg, S., Fisk, N., & Linden, E. (2004). *RIT computer use and ethics survey*.

McQuade, S. C., III. (2005). *Understanding and managing cybercrime*. Boston: Allyn & Bacon.

Mediamark Research. (2004, September 29). *Cell phones displace landlines in record numbers, according to latest Mediamark Research analysis: Households without landlines are increasingly young, upscale*. Retrieved December 22, 2005, from the Mediamark Research Web site: http://www.mediamark.com/mri/docs/pr_9-29-04_cellphones.htm.

Meier, R. F., & Miethe, T. D. (1997). Understanding theories of criminal victimization. In M. McShane & F. P. Williams III (Eds.), *Victims of crime and the victimization process* (pp. 225-265). New York: Garland. (Reprinted from *Crime and Justice: A Review of Research*, *17*, 459-99).

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

National Center for Victims of Crime. (2001). *Get help series: Identity theft*. Retrieved September 17, 2003, from the National Center for Victims of Crime Web site: http://www.ncvc.org/gethelp/identitytheft/.

National White Collar Crime Center & the Federal Bureau of Investigation. (2005). *IC3 2004 internet fraud - crime report: January 1, 2004—December 31, 2004*. Retrieved June 9, 2005, from the Internet Fraud Complaint Center Web site: http://www.ifccfbi.gov/strategy/2004_IC3Report.pdf.

Office for Victims of Crime. (2000, May). *Victims of fraud and economic crimes: Results and recommendations from an OVC focus group meeting*. (OVC Bulletin NCJ 176357). Washington, DC: U. S. Government Printing Office.

Parker, D. B. (1976). *Crime by computer*. New York: Scribner's.

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

Pfohl, S. J. (1981). Labeling criminals. In H. L. Ross (Ed.), *Law and deviance* (pp. 45-64). Volume 5: Sage Annual Reviews in Studies of Deviance. Beverly Hills, CA: Sage Publications.

Quinney, R. (1974). Who is the victim?. In I. Drapkin & E. Viano (Eds.), *Victimology* (pp. 103-119). Lexington: Lexington Books. (Reprinted from *Criminology*, *10*(3), 314-323.)

Rainie, L. (2005, July). *Data memo: The average American internet user is not sure what podcasting is, what an RSS feed does, or what the term "phishing" means*. Retrieved December 29, 2005, from the Pew Internet & American Life Project web site: http://www.pewinternet.org/pdfs/PIP_Data_Techterm_aware.pdf.

Sampson, R. J., & Laub, J. H. (1993). *Crime in the making: Pathways and turning points through life*. Cambridge, MA.: Harvard University Press.

Saunders, K. M., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers, & Technology*, *13*(2), 183-192.

Schafer, S. (1968). The victim and his criminal: A study in functional responsibility. New York: Random House.

Schur, E. M., & Bedau, H. A. (1974). *Victimless crimes: Two sides of a controversy*. Englewood, NJ: Prentice Hall.

Security Breach Disclosure Act, SB 1386, California, Senate (2002). Retrieved January 3, 2006, from the California State Senate Web site: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2004, January). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences*, *49*(1), 131-136.

Shichor, D. (1989). Corporate deviance and corporate victimization: A review and some elaborations. *International Review of Victimology*, *1*, 67-88.

Siemer, J., & Angelides, M. C. (1995). Evaluating intelligent tutoring with gaming-simulations. In C. Alexopotdos, K. Kang, W. R. Lilegdon, & D. Goldsman (Eds.), *Proceedings of the 1995 Winter Simulation Conference* (pp. 1376-1383). New York: ACM Press.

Social Security Administration. (2000, March 1). *Social Security Number chronology*. Retrieved January 4, 2005, from the Social Security Administration Web site: http://www.ssa.gov/history/ssn/ssnchron.html.

Social Security Administration. (2003, March). *A brief history of Social Security.* Retrieved January 4, 2005, from the Social Security Administration Web site: http://www.ssa.gov/history/briefhistory3.html.

Sullivan, B. (2004). *Your Evil Twin*. Hoboken, NJ: John Wiley & Sons.

Synovate. (2003, September). *Federal Trade Commission – Identity theft survey report*. Retrieved September 18, 2003, from the Federal Trade Commission Web site: http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Tomz, J. E., & McGillis, D. (1997, February). *Serving crime victims*. (2nd ed.). U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. Washington, DC: U.S. Government Printing Office.

U. S. Census Bureau. (n.d.). *Statistical abstract of the United States 2004-2005*. Retrieved December 22, 2005, from the U.S. Census Bureau Web site: http://www.census.gov/prod/2004pubs/04statab/pop.pdf.

U. S. Census Bureau. (2005a, September 8). *Hispanic heritage month 2005: September 15-October 15*. Retrieved December 22, 2005, from the U.S. Census Bureau Web site: http://www.census.gov/Press-Release/www/releases/archives/facts_for_features_special_editions/005338.html.

U. S. Census Bureau. (2005b, August 30). *2004 American Community Survey*. Retrieved December 31, 2005, from the U.S. Census Bureau Web site: http://www.census.gov/acs/www/.

U. S. Department of Justice. (1979). *Computer crime: Criminal justice resource manual*. Washington DC: U. S. Government Printing Office.

U. S. General Accounting Office. (1998, May). *Identity fraud: Information on prevalence, cost, and internet impact is limited*. (Report No. GAO/GGD-98-100BR). Washington, DC: U. S. Government Printing Office.

U. S. General Accounting Office. (2002, February 14). *Identity theft: Available data indicate growth in prevalence and cost*. (Report No. GAO-02-424T). Washington, DC: U. S. Government Printing Office.

U. S. House of Representatives (1999). *Identity theft: Is there another you?* Joint Hearing before the Subcommittee on Telecommunications, Trade, and Consumer Protection and the Subcommittee on Finance and Hazardous Materials of the Committee on Commerce, April 22, 1999. Washington, DC: U. S. Government Printing Office.

U. S. House of Representatives. (2000a). *H.R. 4311, The Identity Theft Prevention Act*. Hearing before the Committee on Banking and Financial Services, September 13, 2000. Washington, DC: U. S. Government Printing Office.

U. S. House of Representatives (2000b). *Protecting privacy and preventing misuse of the Social Security number*. Hearing before the Subcommittee on Social Security of the Committee on Ways and Means, July 17, 2000. Washington, DC: U. S. Government Printing Office.

U. S. House of Representatives (2000c). *Use and misuse of Social Security numbers*. Hearing before the Subcommittee on Social Security of the Committee on Ways and Means, May 9, 2000. Washington, DC: U.S. Government Printing Office.

U. S. House of Representatives (2001). *Protecting privacy and preventing misuse of the Social Security number*. Hearing before the Subcommittee on Social Security of the Committee on Ways and Means, May 22, 2001. Washington, DC: U. S. Government Printing Office.

U. S. House of Representatives (2003). *Fighting Identity Theft – The Role of FCRA*. Hearing before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Financial Services, June 24, 2003. Washington, DC: U. S. Government Printing Office.

U. S. Secret Service. (2002). *Public awareness advisory regarding "4-1-9" or "Advance Fee" schemes*. Retrieved November 24, 2003, from the United States Secret Service Web site: http://www.secretservice.gov/alert419.shtml.

U. S. Senate. (2000). *Identity theft: How to protect and restore your good name*. Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, July 12, 2000. Washington, DC: U.S. Government Printing Office.

U. S. Senate. (2002). *Identity theft*. Hearings before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, March 20, 2002. Washington, DC: U. S. Government Printing Office.

Wikipedia Group Author. (2005a, January 2). *Credit card*. Retrieved January 4, 2005, from the Wikipedia Web site: http://en.wikipedia.org/wiki/Credit_card.

Wikipedia Group Author. (2005b, January 2). *Automated teller machine*. Retrieved January 4, 2005, from the Wikipedia Web site: http://en.wikipedia.org/wiki/Automatic_teller_machine.

Appendix A: Model Identity Theft Victimization Survey Instrument Description

Drawing from the RIT Computer Use and Ethics Survey (McQuade et al., 2004), FTC (2006) identity theft statistics demographics, and questions from the Synovate (2003) and Javelin surveys (2005b), as well as findings from the RIT survey and recommendations from this thesis, I have developed a model identity theft victimization survey that can be administered to any national population. With slight modifications, it can also be administered to any population of students, especially college or university students.

Results from this survey can be compared to:

- Findings from the RIT survey;
- Findings from the FTC statistics;
- Findings from the Synovate and Javelin surveys;
- United States demographics at the state, county, zip code, and census tract level; and/or
- Any past or future surveys that have similar measures.

Below, I describe the major sections of the model survey, as well as the justification for including each.

A) Computer Use

- Respondent's computer background: How familiar are they with a computer? Someone with more extensive knowledge should ideally be more familiar with security techniques and thus be less likely to be victimized.
- Operating system: More exploits exist for Windows, resulting in more potential victimization incidents that may occur. Windows users may be more naïve when it comes to security, especially those users who do not have an extensive computing background.
- Online computing activity (types and frequencies): Are people doing certain activities more likely to be victimized? This is a test of routine activities theory.

B) Computer Security Techniques

- Types of security measures used: Do people who use good security make themselves less of a suitable target through the use of capable guardianship (i.e., virtual barriers)? This is a test of routine activities theory.
- Changed behaviors after victimization: Do people alter their behaviors to make themselves less likely to be victimized in the future?

C) Financial Security Techniques

- Types of security measures used: Do people who use good security make themselves less of a suitable target through the use of capable guardianship? This is a test of routine activities theory.
- Are the people who do not have good computer security also the people who do not have good financial security?
- Changed behaviors after victimization: Do people alter their behaviors to make themselves less likely to be victimized in the future?

D) Identity Theft Victimization

- Who are the victims? What type of victimization are they experiencing?
- Who are the offenders?
- What were the losses experienced due to victimization?
- What are the victims' reporting behaviors?
- Fear of crime: Are identity theft victims more fearful of victimization in general?

E) Other High Tech Crime Victimization

- Who are the victims? What type of victimization are they experiencing?
- Who are the offenders?
- What were the losses experienced due to victimization?
- What are the victims' reporting behaviors?
- Are identity theft victims also experiencing other forms of high tech crime victimization?

- Security measures: Is a lack thereof contributing to other forms of high tech crime victimization?

F) Demographics

- Standard comparisons: gender, age, race, level of education, marital status, area of residence
- Measures of affluence for comparisons: income, rent/mortgage payment, number of bank/credit card accounts, type of Internet connection
- This tests lifestyle-exposure theory.

The survey instrument itself begins in Appendix B.

Appendix B: Model Identity Theft Victimization Survey Instrument

Section A: Computer Use

1. Please indicate the total number of computer devices that you own or have primary control of including desktops, laptops, and PDAs (e.g., Palms). _____

2. When you were growing up, did you have a computer in your house?

   A. YES ⟶

   B. NO (Go onto Question #3)

   2a. If YES, were you the primary user of the computer in your house? (Circle YES or NO)

   A. YES B. NO

3. At approximately what age did you start working on computers? _____ years old.

4. During the last year what computer operating system have you used the most frequently?

   A. Windows
   B. Mac OS
   C. Linux
   D. Unix
   E. Other (please specify) (4a)_____
   F. NOT SURE

5. During the last year, please estimate the number of times AND the average number of hours you spent per week using computers for each of the following activities:

Computer Activity:	Times per week	Hours per week
School/academics	**5a**	**5b**
Work/employment	**5c**	**5d**
Computer gaming	**5e**	**5f**
Online gambling	**5g**	**5h**
Online shopping	**5I**	**5j**
Financial management	**5k**	**5l**
Looking at pornography	**5m**	**5n**
Manage e-mail	**5o**	**5p**
Chat online	**5q**	**5r**

Section B: Knowledge and Use of Computer Security Techniques

6. For computers that you own or have primary control of, please indicate which of the following computer security techniques you use.

Computer Security Technique:	YES- I do/use	NO- I do not do/use	NOT SURE
6a. Antivirus software			
6b. Personal firewall			
6c. Anti-spyware software			
6c. Restrict Internet browser/cookie settings			
6d. Avoid opening unsolicited email attachments			
6e. Change software manufacturer defaults			

7. For computers that you own or have primary control of, how often do you:

Security Procedure or Update Method:	Never	Annually	Every Few Months	Monthly	Weekly or more often	NOT SURE
7a. Update virus definitions						
7b. Update anti-spyware definitions						
7c. Change passwords						
7d. Update security patches						
7e. Backup data						
7f. Check operating system and security software logs						

8. If you became an identity theft victim, did you start doing or using any of the above techniques? YES or NO

8a. If yes, which ones?

_____

_____

_____

_____

9. Would most of your computer passwords be considered "strong"?

A. YES

B. NO

C. NOT SURE

Explanation: A "strong password" is composed of random alphabetical, numerical and special characters that do not form any coherent words, along with being upper/lower case sensitive and at least eight characters long. For example, **ro9Ux~!bN3** would be a strong password.

10. How do you keep track of your password(s)? *(Circle the method you use the MOST)*

A. Write it/them down on paper in an easily accessible location
B. Write it/them down on paper and keep in a secret/secure location
C. Memorize
D. Store on a computer device
E. Other (please explain): (10a)_____

11. Have you ever shared your password with someone else?

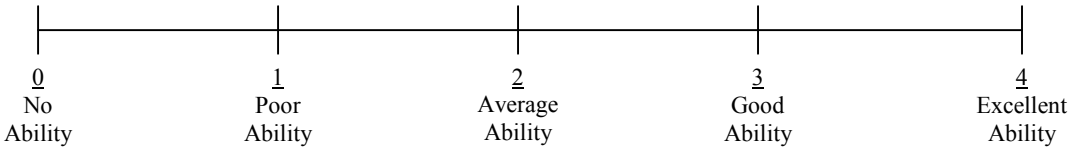
A. YES →

B. NO

11a. If YES, did you change it the next time you logged on or soon afterward?

A. YES B. NO

12. On scale below, please circle your ability to protect your computer data/information.
(Note: If NOT SURE, please check this box instead) → ☐



13. People periodically upgrade their computer equipment for a variety of reasons. Within the last year, have you purchased equipment or services in order to improve your computer security?

A. YES →

B. NO

13a. If YES, what did you purchase?

_____

_____

_____

Section C: Knowledge and Use of Financial Security Techniques

14. Please indicate which of the following financial security techniques you do or use.

Financial Security Technique:	YES- I do/use	NO- I do not do/use	NOT SURE
14a. Write "SEE ID" on the back of a credit or debit card instead of signing it			
14b. Avoid carrying a Social Security card in a purse or wallet			
14c. Shred documents with personal information before disposal			
14d. Subscribe to credit monitoring service			
14e. Avoid leaving a purse or wallet in a public location when not present			

15. How often do you:

Security Procedure:	Never	Annually	Every Few Months	Monthly	Weekly or more often	NOT SURE
15a. Check credit or debit card statements						
15b. Check bank account statements						
15c. Check credit reports						
15d. Check credit score						

16. If you became an identity theft victim, did you start doing or using any of the above techniques? YES or NO

16a. If yes, which ones?

_____

_____

_____

_____

Section D: Identity Theft Victimization

17. In the table boxes below, please CHECK to indicate how many times, if at all, during the last year you have personally experienced EACH of the types of identity theft incidents listed.

Type of Identity Theft Incident:	Never (0)	Once (1)	Twice (2)	Three or more (3+)	NOT SURE
17a. Someone used your Social Security number					
17b. Someone used your existing credit or debit card account					
17c. Someone opened a new credit or debit card account in your name					
17d. Someone gained access to your existing bank account					
17e. Someone opened a new bank account in your name					
17f. Someone opened a new phone or utilities account in your name					
17g. Someone took out a loan in your name					
17h. Someone gained employment in your name					
17i. Someone gained government documents or benefits in your name					
17j. You were the victim of identity theft in some other way not listed (see 18 below)					

18. If you were a victim of identity theft in some other way not listed in the table above, please explain what happened:

_____

_____

19. If you were victimized, do you know who victimized you?

A. YES ⟶
B. NO
C. NOT SURE

19a. If YES, was the offender a:

A. Stranger
B. Acquaintance
C. Friend
D. Relative
E. Other person (please specify): (19b) _____

20. Which of the following types of harms have you personally experienced as the result of any of the incidents listed on the previous table (i.e., Questions 17a–17j)?

(Check all that apply)

20a. Loss of computer data/information	
20b. Loss of computer services	
20c. Loss of money	
20d. Loss of other property	
20e. Loss of privacy	
20f. Loss of time	
20g. Loss of credit or debit card number(s)	
20h. Loss of Social Security number	
20i. Loss of emotional well-being (emotional harm)	

21. If you were the victim of theft or another type of property loss, what is your estimate of the total dollar loss you incurred?

$ _____

22. If you indicated that you experienced any of the incidents listed in Question 17a-17j on the previous page, did you report the incident(s)?

A. YES →
B. NO ↓

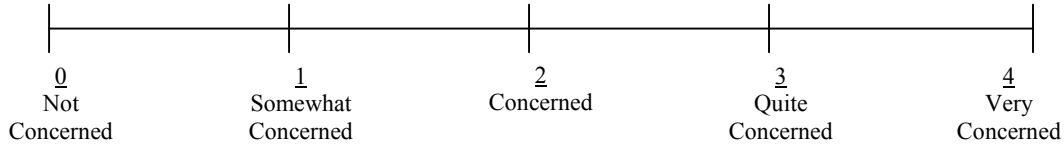
22a. If YES, to whom did you report the incident(s)? *(Circle all that apply and skip to 24)*

A. Parent
B. Supervisor
C. System administrator or lab assistant
D. Campus Information Technology Services (ITS)
E. Campus Information Security Office/officer
F. Campus safety/security officer
G. Police/law enforcement
H. Credit Card Company
I. Credit Reporting Agency
J. Other (please specify) (22b)_____

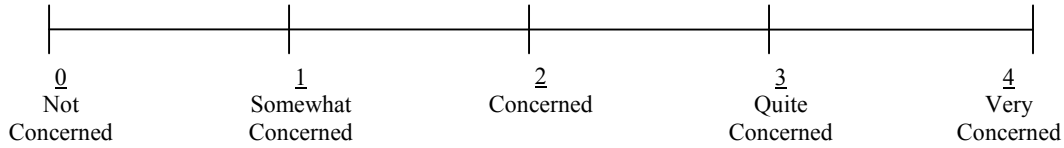
23. If NO, why didn't you report the incident(s)? *(Circle all that apply)*

A. Someone else called
B. Did not have the time
C. Did not know exactly where or how to report it
D. The incident was too minor or not worth it
E. Fear of retaliation
F. Believe no one would do anything about it
G. Believe offender(s) would not be caught
H. Believe court system would not punish the offender
I. Other (please explain) (23a) _____

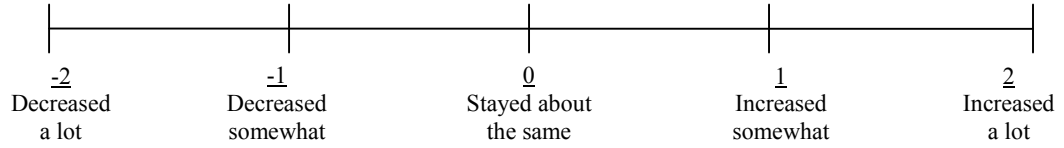
24. How concerned are you about becoming a victim by way of a computer?



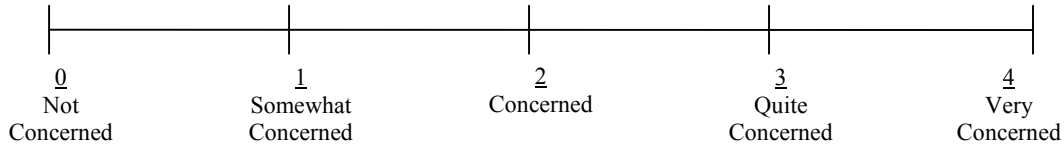
25. How concerned are most people you know about becoming a victim via a computer?



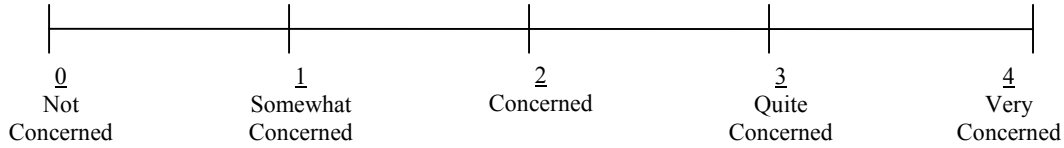
26. During the last year, do you think incidents of computer victimization have . . .



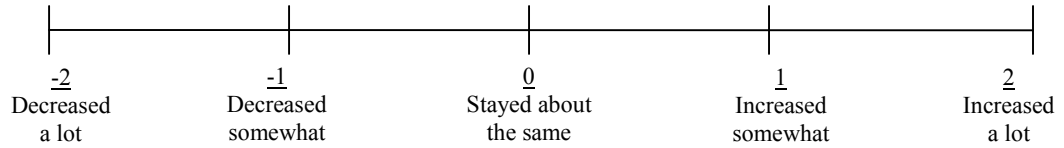
27. How concerned are you about becoming a victim not by way of a computer?



28. How concerned are most people you know about becoming a victim not via a computer?



29. During the last year, do you think incidents of non-computer victimization have . . .



Section E: Computer-Based Victimization

30. In the table boxes below, please CHECK to indicate how many times, if at all, during the last year you have personally experienced EACH of the types of computer incidents listed.

Type of Computer Incident:	Never (0)	Once (1)	Twice (2)	Three or more (3+)	NOT SURE
30a. You accidentally downloaded a virus or worm.					
30b. You were denied computer access or service because of someone's malicious computer conduct.					
30c. Someone used a computer to harass or embarrass you.					
30d. Someone used a computer to threaten you.					
30e. Someone "hacked" into your computer					
30f. Someone used a computer to stalk you					
30g. Someone stole your computer or other electronic device					
30h. Someone used a computer to defraud or cause you financial loss					
30i. You were victimized via a computer in some other way not listed (see 31 below)					

31. If you were victimized by way of a computer in some other way not listed in the table above, please explain what happened:

_____

_____

Section F: Additional Information for Comparison Purposes

32. Gender: _____ Male _____ Female

33. What is your approximate age?

A. Under 18
B. 18 - 24
C. 25 - 29
D. 30 - 39
E. 40 – 59
F. 60 or older

34. With which of the following groups do you most identify with?

A. White/Caucasian
B. African American/Black
C. Hispanic/Latino
D. Asian
E. Native American
F. Other (please specify) (34a)_____

35. What is your household income?

A. Under $20,000
B. $20,000 to $49,999
C. $50,000 to $99,999
D. $100,000 to $149,999
E. $150,000 and greater

36. What is your education level?

A. Some high school
B. High school graduate
C. Some college
D. Bachelor's degree
E. Graduate or professional degree

37. What is your relationship status?

A. Single
B. Long-term relationship
C. Married or in a civil union
D. Divorced
E. Widowed

38. Do you own or rent your residence?

A. OWN
B. RENT

39. How much is your monthly rent or mortgage payment?

A. Under $500
B. $500 to $1000
C. Over $1000

40. How many credit or debit cards do you have?

A. 0
B. 1-2
C. 3-4
D. 5+

41. How many bank accounts do you have?

A. 0
B. 1-2
C. 3-4
D. 5+

42. Does your residence have a broadband or high speed (non-dial up) Internet connection?

A. YES
B. NO
C. UNSURE

43. Do you use wireless Internet access?

A. YES
B. NO
C. UNSURE

Appendix C: Use of Previously Written Material

Portions of this thesis have been drawn from three previous reports completed as part of my MS Information Technology coursework. These include the following:

- Introduction and Literature Review (Berg, 2004; Berg, 2005a; Berg, 2005b)
- Methodology (Berg, 2005b)
- Recommendations (Berg, 2004; Berg, 2005b)

Berg, 2004 was written for Enterprise Security. Berg, 2005a and Berg, 2005b were written for Independent Studies.

Additionally, the model identity theft survey instrument in Appendix B contains many questions taken from the RIT Computer Use and Ethics Survey (McQuade et al., 2004), of which I was a co-developer.