WINTER 2007
CAMPUS TECHNOLOGY

A STUDY ON CYBERCRIME'S IMPACT IN THE WORKPLACE

Denise Marcia Chatam, D.B.A., Dean of Technology and Institutional Research, Lone Star College System – Cypress College

Introduction

The U.S. is the global leader in the use of the Internet for commerce and communication, and in using electronic commerce for spending (Rusch, 2005). The continued expansion of legitimate Internet use has led to an increase in fraud and malicious activities that exploits the Internet known as cybercrime. Organizations of all sizes and industries have suffered losses from cybercrimes, though few officially report such incidents (Citrano, 2006; FBI, 2003). Cybercrimes often yield lucrative financial gains while providing low risks for perpetrators (Williams, 2002). The level of cybercrime sophistication, automation, and effectiveness is ever increasing.

Cybercrimes are typically conducted remotely and anonymously to take advantage of flaws in software code, circumvent signature-based tools that commonly identify and prevent known threats, and use social engineering techniques to trick unsuspecting users into revealing sensitive information or propagating attacks. Various experts, from the Federal Bureau of Investigations (FBI) to corporate security analysts warn that as Internet usage increases, e-commerce matures, and national defense and intelligence communities increasingly rely on commercially available information technology, cybercrime will continue to rise (FBI, 2003).

Some of the terms used to describe cybercrimes include electronic crime, computer-related crime, high-tech crime, Internet crime and computer crime. Cybercrimes, in the context of this study are defined as bank, check, debit and credit card fraud; telecommunications and computer crimes; fraudulent identification including identity theft; fraudulent government securities; electronic fund transfer fraud; auction fraud; Intellectual Property Rights (IPR) abuses; economic espionage (theft of trade secrets); online extortion; international money laundering; and work-at-home and online business opportunities schemes (FBI, 2006).

Cybercrime has created major problems and continue to increase at institutions of higher learning (academia) and K-12. Academia is emerging as a particularly vulnerable for Internet crime. Gaining a better understanding of the factors that influence cybercrime incidents should assist academia, the business community, law enforcement and government officials to develop programs that minimize the negative economic and non-economic impact of cybercrime.

Background of the Problem

The U.S. is the global leader in the use of the Internet for commerce and communication, as well as in using electronic commerce for spending (Rusch, 2005). The level of sophistication and effectiveness of cybercrimes is ever increasing. Cybercrime presents a significant risk to the everyday digital activities of consumers and the digital subsistence of organizations. It is therefore unsurprising that academia, business community leaders and government officials are increasingly concerned about cybercrimes from individuals and groups with malicious intent ranging from petty criminal acts to organized crime activities, terrorism, foreign intelligence gathering, and acts of war. Cybercriminals of today are going from trying to hit as many machines as possible to developing techniques that allow them to remain undetected on infected machines longer in order to cause more harm. In the academic setting, keyloggers and spyware infecting devices are more prevalent than easily detected viruses and worms.

Organizations of all sizes and industries have suffered losses at the hands of cyber-criminals – though only approximately nine percent report such incidents (Citrano, 2006; FBI, 2003). Concomitantly, cybercrimes offer high financial yields and can often be performed in a manner that incurs only modest risks because of the anonymity it presents. The lack of incident reporting and the ease of access to electronically stored data have led experts to predict that cybercrime will continue to increase in the years to come. In 2004, the FBI reported that for the first time on a global scale, cybercrime had become more profitable than trafficking drugs (FBI, 2006).

U.S. organizations are estimated to have lost over $67 billion in 2005 (Evers, 2006, p. 1). This is up from the $14 billion in losses reported in 2004 by the American Insurance Association (Easen, 2004, p. 1). Approximately 9 out of 10 U.S. organizations experienced a cybercrime incident in 2005 (Citrano, 2006). There was a 480% increase between 2004 and 2005 (FTC, 2006, p. 3). The Internet Crime Compliant Center (IC3), a government partnership between the FBI and the National White Collar Crime Center (NW3C) gave an annual report that also suggests that the current trends and patterns of cybercrimes will continue to increase (IC3, 2006). The research of IC3 indicates that only one in seven incidents of fraud ever captures the attention of enforcement or regulatory agencies (IC3, 2006).

The top 10 countries where complainants and perpetrators resided are illustrated in Figures 1 and 2.

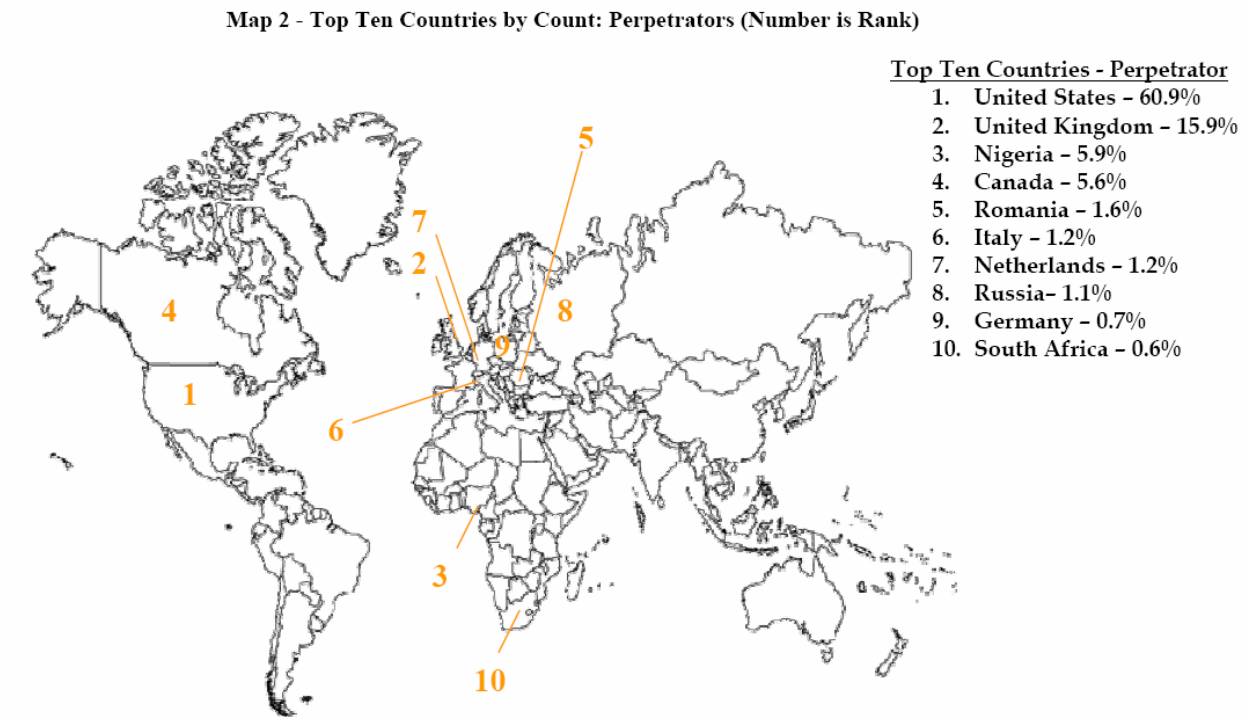


Figure 1. Map. Top 10 Countries by Count: Perpetrators (Number is Rank) Note. Adapted from The IC3 2006 Internet Crime Report. January 1, 2006 – December 31, 2006 by the National White Collar Crime Center and the Federal Bureau of Investigation, 2007.

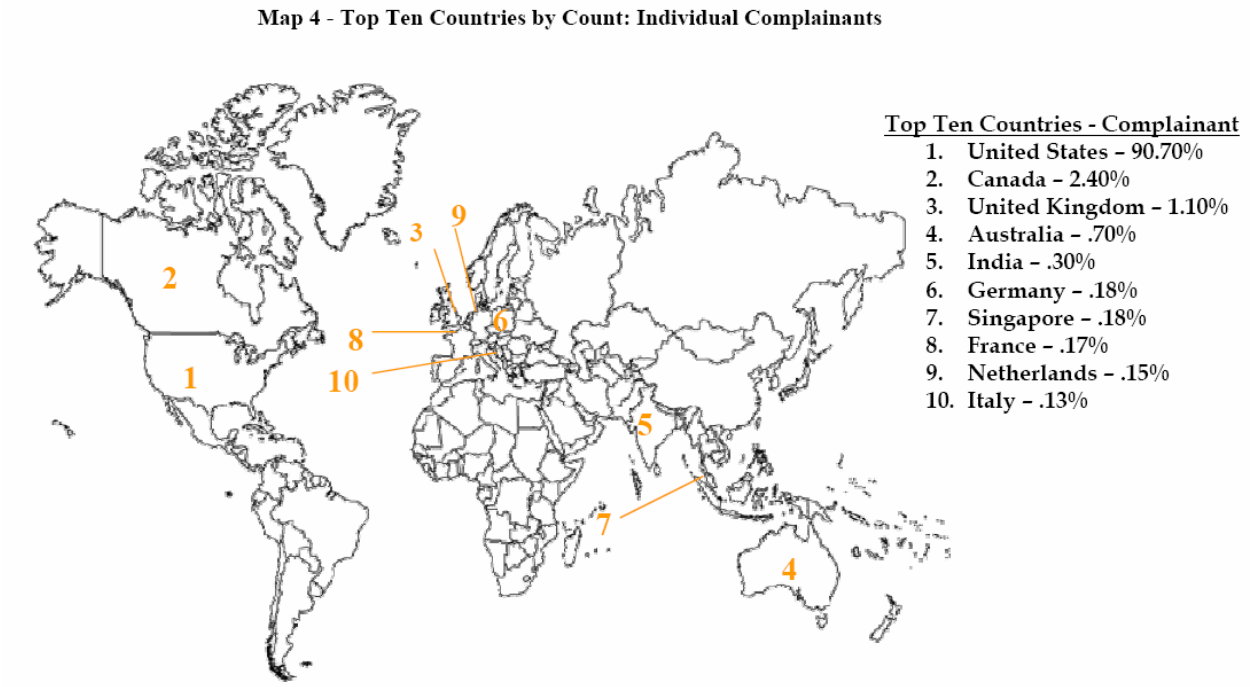


Figure 2. Map. Top 10 Countries by Count: Individual Complainants (Number is Rank) Note. Adapted from The IC3 2006 Internet Crime Report. January 1, 2006 – December

31, 2006 by the National White Collar Crime Center and the Federal Bureau of Investigation, 2007.

As displayed in Table 1, in 2006 California was ranked first among all U.S. states in the reported number of cybercrimes. Reports indicate that incidents of cybercrime are also rising more rapidly in the major metropolitan areas of Texas, California, Florida, and New York than the national average.

Table 1.
Top 10 Cybercrime States by Count – Individual Complainants and Perpetrators (Number Rank)

	Complainants		Perpetrators	
Ranking	State	Percentage of Complainants	State	Percentage of Complainants
1	California	13.5%	California	15.2%
2	Texas	7.2%	New York	9.5%
3	Florida	7.1%	Florida	9.3%
4	New York	5.5%	Texas	6.5%
5	Pennsylvania	4.0%	Illinois	4.5%
6	New Jersey	3.6%	Pennsylvania	3.3%
7	Illinois	3.5%	Tennessee	3.2%
8	Ohio	3.3%	North Carolina	3.1%
9	Virginia	3.0%	Ohio	3.1%
10	Michigan	2.9%	New Jersey	3.0%

Note. Adapted from *The IC3 2006 Internet Crime Report. January 1, 2006 – December 31, 2006* by the National White Collar Crime Center and the Federal Bureau of Investigation, 2007, pp. 10 – 13.

Table 2.
Top 10 Cybercrime States by Count – Individual Complainants and Perpetrators (Number Rank)

	Complainants		Perpetrators	
Ranking	State	Percentage of Complainants	State	Percentage of Complainants
1	California	13.6%	California	15.2%
2	Florida	7.1%	New York	9.8%
3	Texas	6.6%	Florida	8.4%
4	New York	5.6%	Texas	6.9%
5	Pennsylvania	3.9%	Illinois	4.8%
6	Illinois	3.7%	Pennsylvania	3.6%
7	Ohio	3.6%	Ohio	3.6%
8	New Jersey	3.1%	Georgia	3.0%
9	Michigan	3.0%	New Jersey	3.0%
10	Virginia	2.9%	Michigan	3.0%

Note. Adapted from *The IC3 2005 Internet Crime Report. January 1, 2005 – December 31, 2005* by the National White Collar Crime Center and the Federal Bureau of Investigation, 2006, pp. 10 – 13.

One of the problems with the security in place within many organizations is that many executives fail to see security as adding directly to the profitability of their organization (Garg, Curtis & Halper, 2003). It is difficult for security experts to prove that through improved security the losses saved and the direct positive impact on profitability. Many U.S. organizations, including academia, have been slow in responding with new measures to safeguard their computing systems from intruders (FBI, 2006). Some organizations have spent millions on a computing security system to make it architecturally sound, only to find that the system fails when a single individual places his or her password on a sheet of paper in an unlocked desk drawer.

Money and ego has become the primary motivator of most major cybercrimes of today. The value of a successful breach can become financially lucrative while the opportunity for apprehension is low. For academia, there are many areas of exposure. As the use of credit cards grows on campus, the opportunity for compromise is there. Credit-card network breaches are increasingly becoming one of the most constant and potentially devastating threats any organization faces that handles credit cards, particularly academia. For example, the value of data yielded from a cyberattack, on average, is as follows:

1. Financial reports = $5,000
2. Product design = $1,000
3. Credit card + PIN = $500
4. Trojan log = $300
5. Driver's license = $150
6. Social security number + Name = $100
7. Valid credit card = $20

From another perspective, the hypothetical situation is presented below in Table 3.

Table 3.
Hypothetical Situation – Cybercrime

Hypothetical Situation:	
A university student database is hacked which contains the names, social security numbers, and addresses of 10,000 students.	
The cybercriminals profits is $1,000,000 (10,000 records x $100/each = $1,000,000)	
What is the potential impact to the university?	
Student/parent notification	$25 x 10,000 = $250,000
Credit monitoring (one year)	10,000 accounts x $14/mon x 1year = $168,000

Fraud liability (records actually used in a crime)	100 accounts x $1,500 = $150,000
Damaged Reputation	***PRICELESS***

Several surveys were reviewed. *The 2001 Computer Security Survey dated July 31, 2002 (Form CS-1),* was a pilot test conducted by the U.S. Department of Justice Bureau of Justice Statistics (U.S. DOJ-BJS) on cybercrime against organizations which concluded that there is a need to produce valid national estimates (Rantala, 2004). The Canadian Centre for Justice Statistics conducted a study on cybercrime and concluded that because of ongoing financial losses by all types of organizations there is a greater interest in analyzing trends on cybercrime (Kowalski, 2002). *The Information Security Breaches Survey of 2006* (ISBS 2006) managed by PricewaterhouseCoopers indicated that there is an ongoing need to help organizations in the United Kingdom (U.K.) and around the globe better understand the risks they face as they embrace the Internet as stated by Alun Michael, the United Kingdom Minister of State for Industry and the Regions (Michael, 2006). The *Computer Security Institute (CSI) Computer Crime and Security Survey* is a study conducted jointly by the FBI and CSI, concluded that there is an ongoing need to increase security awareness, promote information protection and encourages cooperation between law enforcement and the private sector (Computer Security Institute, 2006).

Cybercrimes are complex, typically involving multiple parties in each investigation. Local law enforcement agencies must work with various organizational structures, follow varying regulations and engage multiple law enforcement agencies. Tracing cyber-criminals is difficult as the crime frequently transcends a maze of national boundaries and maneuvers through thousands of computing devices and systems (FBI, 2006).

Law enforcement agencies have expressed concerns with respect to the capability of the private sector, academia and local government agencies' ability to provide protection from cybercrime given the economic impact of the problem. The U.S. Secret Service Director W. Ralph Basham stated in 2004 that with the potential for cybercrime expanding rapidly throughout the world it is important for the private sector to increase its awareness of cybercrime and become better educated as to its consequences (U.S. Department of Homeland Security & U.S. Secret Service, 2004).

To combat cybercrime, organizations will need to be better informed of information sharing, statistics, and education on the subject. Approaches to cyber security will vary, especially when comparing industries and regions where more incidents occur than in industries and regions where occurrences are less frequent and e-commerce is not as widely used. These approaches to cyber security give the perception of a lower number of incidents in less densely populated regions of the country and in specific industries that has not yet been validated (Uranga, 2003).

Problem Statement

In the U.S., estimates of annual losses caused by cybercrime are in the billions of dollars and are continually increasing in terms of numbers of victimizes and overall costs (FBI, 2006; IC3, 2006; U.S. Department of Homeland Security, 2004). U.S. organizations lost an estimated $14 billion in 2004 as reported by the American Insurance Association (Easen, 2004, p. 1); according to the latest statistics available, cybercrime costs rose approximately 480% to $67 billion in 2005 (Evers, 2006, p. 1). Institutions of higher learning are increasingly becoming the target of cybercrimes. The threat of cybercrime, the increase in attacks, and the resulting economic and non-economic losses underscore the need to bolster the understanding of the causes and consequences of cybercrime for academia.

The problem is that cybercrime has increased in the U.S. from $14 billion in 2004 to $67 billion in 2005, a 480% increase in one year. Reported are 9 out of 10 organizations are affected by cybercrime, yet less than 10% report an incident to law enforcement or government agencies tracking these crimes (Cistrano, 2006). By some estimates, as few as one out of four hundred cybercriminals are caught. Even fewer are prosecuted. For those who are captured, tried, and convicted, the monetary penalty may be small, jail time, if any, may be minimal, and the crime is often classified as a misdemeanor. Law enforcement will typically not invest resources to investigate a crime unless the value of the incident(s) is $10,000 or more a patterns of larger activities is suspected.

A quantitative correlational study was conducted to explore relationships between the computing environments; the number of cybercrime incidents and the factors that influence cybercrime has on an organization. The independent variables were (a) the computing infrastructure, (b) the number of cybercrime incidents detected, and (c) the investment in security technology of organizations. The dependent variables were (a) the percentage of cybercrime incidents reported, and (b) the resulting economic damages. The survey was conducted on business leaders and security professionals from organizations in the greater Houston area, a population of convenience. In 2004, the greater Houston area had a population of 113,154 organizations (U.S. Census Bureau, 2006). Using a margin of error of 5%, a confidence level of 95%, and a confidence interval of six the minimal sample size was determined to be 263, according to the Creative Research Systems sample size calculator (Creative Research Systems, 2006).

Data was gathered using 11 questions. The survey instrument was designed to provide a high level of anonymity eliminating the need for the respondent to provide any identifying information about themselves or their business in order to increase the probability of a response. Quota sampling was the method used to select organizations with the characteristics desired for the research.

The research study provides a broad account of the many influences leading to the growth of cybercrime in the U.S. The objective of the study was to advance the community's knowledge on cybercrime, to influence practices and policy towards minimizing the economic damages of cybercrime on organizations, and to encourage reporting of cybercrime incidents to the appropriate agencies.

The significance of the study provides academia, business leaders, information security personnel, and government officials with scientific information that can be used to aid in developing and revising legal, industry and organizational instruments aimed at identifying the material elements of cybercrime. The data gathered and analyzed may also support the establishment of a common and recommended national minimum standard for information security (Pocar, 2004). Significant correlational data between any of the independent variables and dependent variables can support the attractiveness of investing more in information security technology by an organization. The study provides law enforcement with supporting documentation that it can use to help establish priorities and allocate resources aimed at improving cybercrime incident reporting rates. For the public, the study provides data on the economic harm cybercrime create which ultimately affects the cost of goods and services.

The sample population consisted of 132 of the largest organizations within the greater Houston area and 131 randomly selected organizations of varying sizes and types (see Table 4). The industry sectors used for profiling organizations were:

1. Financial services (finance, insurance, banking, real estate, rental, and leasing).
2. Professional, information, communications and entertainment (professional, consulting, scientific, management, information, administrative, arts, and recreation).
3. Industrial markets (manufacturing, energy, utilities, chemical, warehousing, wholesale trade, waste management services, construction, agriculture, forestry, fishing, hunting, and mining).
4. Consumer markets (retail trade, accommodation, and foodservices).
5. Healthcare and public sector (public administration, educational, health, and social services) (Texas Economic Development, Business and Industry Data Center, 2004).

Table 4.
Number of Organizations by Employment Size Class for the U.S., State of Texas, and the Houston MSA

Number of Establishments by Employment-size Class				
		Number of Employees		
		Small	Medium	Large
Location	Number of Establishments	1-99	100-499	500+
Harris County	113,154	109,976	2,819	359
Texas	491,092	478,865	10,851	1,376
U.S.	7,387,724	7,215,786	153,610	18,328

Note. Adapted from the *U. S. Bureau of the Census, 2004 Economic Census, Houston-Baytown-Sugar Land, TX Metropolitan Statistical Area* by the United States Census Bureau, 2006.p. 1.

Research Questions

The research questions used were:

1. What factors best predict the number of cybercrime incidents and the number of incidents reported to government agencies and law enforcement by an organization?
2. What factors best measure the number of cybercrime incidents and the economic damages incurred by an organization?
3. Is there a significant relationship between the computer environment and the economic damages resulting from cybercrime experienced by an organization?
4. Is there a significant relationship between the computer environment and the percentage of cybercrime incidents reported to law enforcement and government agencies by an organization?
5. Is there a significant relationship between the investment in security technology and the economic damages experienced by an organization?
6. Is there a significant relationship between the investment in security technology and the reporting of cybercrime incidents to government or regulatory agencies by an organization?

Hypotheses

Based on the findings from prior research on cybercrime, it was appropriate to examine whether there exists a significant relationship between computer infrastructure, the number of cybercrime incidents and the level of investment in information security technology and the percentage of incidents reported to law enforcement and the resulting economic damages incurred.

Stated in terms of a null hypothesis (Ho) and an alternate hypothesis (Ha), the research will either reject or fail to reject the hypothesis using statistical means. The set of hypothesis for the study were:

Ho1: There is not a significant positive relationship among the factors recorded and the economic damages incurred by an organization.

Ha1: There is a significant positive relationship among the factors recorded and the economic damages incurred by an organization.

Ho2: There is not a significant positive relationship among the factors recorded and the percentage of incidents reported to government agencies or law enforcement by an organization.

Ha2: There is a significant positive relationship among the factors recorded and the percentage of incidents reported to government agencies or law enforcement by an organization.

Ho3: There is not a significant relationship between the computing environment and the economic damages incurred for an organization.

Ha3: There is a significant relationship between the computing environment and the economic damages incurred for an organization.

Ho4: There is not a significant relationship between the computing environment and the percentage of incident reporting by an organization.

Ha4: There is a significant relationship between the computing environment and the percentage of incident reporting by an organization.

Ho5: There is not a significant relationship between the investment in security technology and the economic damages incurred for an organization.

Ha5: There is a significant relationship between the investment in security technology and the economic damages incurred for an organization.

Ho6: There is not a significant relationship between the investment in security technology and the percentage of incident reporting by an organization.

Ha6: There is a significant relationship between the investment in security technology and the percentage of incident reporting by an organization.

Conceptual Framework

The conceptual framework depicts a two-stage relationship where a set of dependent variables are influenced by the independent variables, which in turn determine the outcome, the causes and consequences of cybercrime on an organization. There are two primary groups of variables: (a) independent variables – the computing environment, level of investment in security technology, and the number of cybercrime incidents detected; and (b) dependent variables – the percentage of incidents reported and economic damages incurred. An identical study could result in quite a different outcome due to modifying factors.

The diagram in Figure 3 depicts the conceptual framework explaining the relationships among the variables:

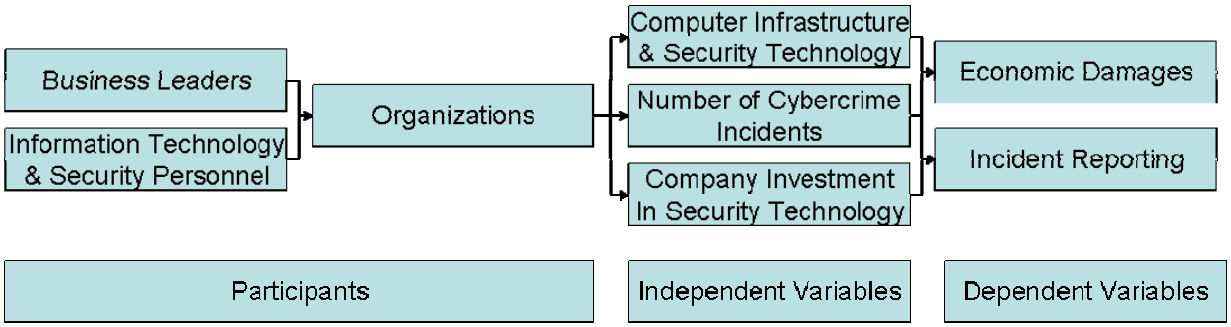


Figure 3. Conceptual Framework

Historical Perspective

Cybercrime has been in existence since data has been stored in electronic form. Individuals and groups representing various socio-economic, gender, age, racial, and national orientations commit cybercrimes (Federal Deposit Insurance Corporation, 2001, 2003, and 2004). Early forms of cybercrime included identity theft used by fugitives to avoid capture, those who forged checks, or those who negotiated stolen or counterfeit checks (Barr, 2004; Gibbons, 1999). The new generation of cyber criminals has proliferated with cybercrime growing rapidly and in complexity (Broder, 2003). The advances in computing technology with digital color printing, multi-media applications, and the Internet have enabled amateurs to produce high quality counterfeit documents (Barr, 2005; Block, 2004). Factors that contribute to cybercrimes are (a) cybercrime is

easy to learn how to commit, (b) requires few resources relative to the potential harm inflicted, (c) cybercrime can be committed without being physically present in the jurisdiction, and (d) many times the offense is not clearly illegal (Bierman and Cloete, 2003; McConnell, 2001). Massive databases of learning institutions, financial institutions, and airline companies that store credit card and other identification information for legitimate purposes are also used at greater frequency to launch cybercrimes that are more complex and broader in scope (Bell, 2002; FBI, 2003). These factors are major contributors in making cybercrime one of the fastest growing crimes in both in the United States and worldwide (McConnell, 2001).

Related Theories

Cybercrime is a white-collar crime (IC3, 2006, Krause, 2002; NWC3 and FBI, 2005). In 1949 criminologist, Edwin H. Sutherland coined the term *white-collar crime* in his last book entitled *White Collar Crime* (Sutherland, 1949). The *White-Collar Criminality Theory* created by Sutherland states that white-collar crime is the real crime which leads to financial costs that are usually several times as great as the financial cost of all the crimes which are customarily regarded as the "crime problem" (Sutherland, 1949).

When Sutherland introduced the concept of white-collar crime, his thinking was that of a successful white male, middle-class professional. He assumed that white-collar crime was crime committed by offenders who have a high social status and respectability, determined by their professional duties (Camp, 2003; Sutherland, 1949). He thought that criminal behavior was a learned behavior rather than primarily a pathological or biological behavior. This sentiment became the basis for his Differential Association Theory. In 1949, Sutherland noted that females were less likely to commit crimes because they are destined to bear children and more closely supervised than males. He also asserted that variables of masculinity such as aggression, competition, rationality, machismo, and power were contributors towards criminal behavior over feminine characteristics such as sweetness, sensitivity, irrationality, and obedience (Vande Walle, 2002).

Donald Cressey, a leading expert in organized and white-collar crime in the U.S. and a student of Sutherland's, developed the criminological theory Social Science and the Repression of Crime. This theory stated that if strict controls were imposed on all personnel within a business, then violations such as embezzlement, management fraud, and other criminal activities would be greatly reduced, however little business would be conducted (Cressey, 1955 and 1960).

Marshall Clinard studied criminology comparing places with little crime such as Switzerland, with places with high crime rates such as the U.S. (Clinard, 1978). His goal was to answer the question of whether the maintenance of moral boundaries through the identification and punishment of crime is necessary for societies characterized by relatively low crime (Unnithan, 2002).

Marshall Clinard and Peter Yeager (1980) defined corporate crime as any act committed by corporations that is punishable by the state under administrative, civil, or criminal law.

Clinard and Yeager suggest that white-collar crimes are sociological as well as legalistic in nature. Clinard and Yeager also suggest that white-collar behaviors that may be unethical or immoral in the corporate context may not explicitly violate any laws. For example, an information security analyst who cheats on his security reports by altering the results may not have violated a law or regulation but instead has violated an ethical rule or norm of the information security community. The act of altering security reports is a white-collar offense as the information security analyst has engaged in an unethical or immoral behavior within his occupational context.

Primary U.S. Reporting Agency

The FBI is the primary law enforcement agency investigating cybercrimes. The FBI and many other agencies tracking cybercrime incidents find that incidents of cybercrime were under-represented due to the low level of cybercrime incident reporting and the difficulty in detecting and punishing the crime (FBI, 2003). Many crime victims elect not to report a cybercrime incident because they felt reporting the crime was “not worth the effort” (IC3, 2006, p. 14). Despite the reluctance to report cybercrime incidents by organizations and consumers, statistics reveal a rapid increase in cybercrime activities. From January 2000 to September 2004, the FBI’s investigations in the financial institution fraud arena have resulted in more than 11,466 indictments, 11,362 convictions, and approximately $8.1 billion in restitution orders (FBI, 2006, p. 3).

Types of Cybercrimes

The primary types of cybercrimes are data, network, access, and other crimes (Whitney, 2004; Williams, Dunlevy and Shimeall, 2006). Cybercrimes under the title of data crimes include data interception, data modification, and data theft. Data interception is the interception of data in transmission (Bigelow, 2005). Data modification is the alteration, destruction, or erasure of data (Bigelow, 2005). Data theft is the taking or copying of data, regardless of whether it is protected by other laws such as copyright and privacy laws, Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA) (Electronic Privacy Information Center, 2004; McConnell, 2001; U.S. Department of Health and Human Services, 2003, 2006).

Cybercrimes regarding network access includes network interference and network sabotage. Network interference is the impeding or prevention of access of others (Bigelow, 2005). The most common example of network interference is a distributed denial of service (DDoS) attack that floods a web site(s) or an Internet Service Provider (ISP). DDoS attacks are frequently launched from numerous computers that have been hacked to obey the commands of the perpetrator (Evans, and Furnell, 2000). Network sabotage is the modification or destruction of a network or system. Network sabotage frequently occurs with ghost accounts; accounts not closed when an employee leaves a company that can give a disgruntled employee a back door into the network (Barr, 2003; McNeil Solida, 2003).

Cybercrimes include access crimes such as unauthorized access and virus dissemination. Unauthorized access is the hacking or destruction of a network or system (McConnell, 2001). For example, the U.S. DOJ reported on March 1, 2006 that a federal

computer security specialist within the Department of Education's Office of Inspector General installed software on the computer of a supervisor enabling him to access its stored data at will. He later used this privileged access to view email and other electronic transactions of his supervisor then shared the information with others in his office. The accused pled guilty and was later sentenced to five years in prison and fined $250,000 (U.S. DOJ-CRM, 2006).

Virus dissemination is the introduction of software that is harmful to a system or data therein. In 2005, the U.S. DOJ reported that a 21-year-old male of Beaverton, Oregon used more than 20,000 infected computers he had infected with a computer worm program to launch a DDoS attack against eBay in 2003. The attack caused a denial of service for legitimate users who wanted to access eBay. The perpetrator, awaiting sentencing could receive up to ten years imprisonment, a $250,000 fine or twice the gross gain or loss, and three years supervised release (U.S. DOJ, 2005).

Data and other types of cybercrimes include aiding and abetting cybercrimes and computer related forgery and fraud. Computer-related forgery is the alternation of data with the intent to represent it as authentic. Computer-related fraud is the alteration of data with the intent to derive economic benefit from its misrepresentation (McConnell, 2001). In February 2006, the U.S. DOJ reported that a 41-year-old male of Cleveland, Ohio obtained stolen debit card account numbers, personal identification numbers (PINs), and personal identifier information of the true account holders that he encoded on blank cards. He used the counterfeit debit cards to obtain $384,000 in cash advances from ATM machines in the greater Cleveland area over a three-week period. The perpetrator received a sentenced of 32 months in prison, three years of supervised release for bank fraud and conspiracy, and ordered to pay $300,749 restitution to the bank and $200 to the Crime Victim's Fund (White & Kern, 2006).

Regulatory Landscape

Personal and financial information is at the core of business transaction records and financial data that identifies customer information (Ponsaers, 2002). The volume and value of personal and financial information makes it very attractive to those with criminal intentions. Federal, state, and local legislation as well as the marketplace regulate governance of the information. Keeping sensitive information away from those with malicious intent is a growing problem for many organizations and government agencies and a genuine concern for consumers and organizations alike. Legislation exists requiring and encouraging law enforcement personnel and business leaders to do more in protecting sensitive information and still fighting cybercrime remain a major issue.

Together, technology and the computer infrastructure play an essential role in identifying solutions to cybercrime including fraud management, logical security issues, and maintaining compliance to a growing number of regulations to address cybercrime (Collins, et. al., 2001; Equifax, 2004). Many regulations, both government and industry based are in place today such as the Intelligence Authorization Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act), Healthcare Information Protection Act (HIPAA),

Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry (PCI) standards by the credit card industry. Increased cybercrime activity and the need for organizations to provide greater protection of sensitive data and assets influenced the development of each of these regulations.

The Intelligence Authorization Act requires the President to submit annually to Congress updated information on the threat to U.S. industry from foreign economic collections and industrial espionage (Office of the Press Secretary, The White House, 2001). The PATRIOT Act expands the authority of U.S. law enforcement to help in fighting terrorism and to detect and prosecute other crimes such as cybercrime used to support terrorism (Podgor, 2002; Trandahl, 2001; Wikipedia, 2006). HIPAA provides regulations for use by health care providers, their vendors, and those who have access to sensitive data to safeguard personal health information for every individual (U. S. Department of Health and Human Services, 2006). GLBA, also known as the Financial Services Modernization Act of 1999, provides limited privacy protections against the sale of an individual's private financial information and codifies protections against pretexting; the practice of obtaining personal information through false pretenses (Electronic Privacy Information Center, 2004). PCI standards provides for the integrity, availability and confidentiality of account information for all who have access to sensitive data throughout its life cycle (Kutnick, 2006).

Cybercrime is a topic relevant to organizations, community, and criminal justice policies and practices around the world. Cybercrime goes beyond the economic damages to a business; cybercrime also causes damage to the reputation of an organization that can require significant effort to remedy (Chapman, 2003). The next section will review each variable in detail.

Presentation and Analysis of Data

Table 5 provides the means and standard deviation for each of the primary variables studied.

Table 5.
Summary List of Measurement Variables (n=307)

No.	Variable	*M*	*SD*
1.	Top computer security concern	4.09	2.854
2.	Number of access types to computer systems	2.65	1.611
3.	Number of servers	2.34	1.327
4.	Number of individual PCs, laptops, and workstations (computers)	2.88	1.477
5.	Number of security measures in place	3.769	2.387
6.	Percentage of cybercrime incidents detected	1.35	0.477
7.	Percentage of cybercrime incidents reported to law enforcement or computer incident agencies	5.05	1.507
8.	Amount spent on computer system security technology	2.74	1.441
9.	Percentage of the total 2006 IT budget spent on computer system security technology	1.91	1.323

No.	Variable	*M*	*SD*
10.	The dollar value of the losses and costs incurred	4.67	1.954

Research Questions

Research Question 1

Research Question 1 asked, “Is there a significant relationship between the percentage of cybercrime incidents detected and the economic damages resulting from cybercrime incidents experienced by an organization?” There was support for rejecting the null hypotheses with $r = 0.188$ at $\alpha = 0.01$. There is a significant positive relationship among the factors recorded and the economic damages incurred by an organization.

Additional findings include:

1. The smaller the organization the more likely they reported an incident of cybercrime.
2. 72.6% (223/307) reported losses and costs associated with a cybercrime incident
3. 27.4% (84) organizations did not report any losses.

By value of losses/costs:

4. 9.1% (28) reported losses and costs of less than $1,000.
5. 12.7% (39) incurred losses and costs between $1,000 and $50,000.
6. 14.0% (43) incurred losses and costs between $50,000 and $100,000.
7. 6.8% (21) incurred losses and costs between $100,000 and $200,000.
8. 3.0% (40) reported losses and costs of $200,000 or more.
9. 9.4% (29) detected an incident of cybercrime yet did not experience any losses or costs.

By industry:

10. 23.1% (71) of the organizations in the financial services sector had incurred losses and costs from cybercrime
11. 23.8% (73) of the organizations in the professional information, communications, and entertainment industry
12. 21.8% (67) of the organizations in the industrial markets
13. 19.5% in the consumer markets
14. 11.7% in the healthcare and public sector, including academia.

Research Question 2

Research Question 2 asked “Is there a significant relationship between the percentage of cybercrime incidents detected and the percentage of cybercrime incidents reported to law enforcement or government agencies by an organization?” There was support for rejecting the null hypotheses with $r = 0.461$ at $\alpha = 0.01$. There is a significant positive relationship between the percentage of cybercrime incidents detected and the percentage of cybercrime incidents reported to law enforcement or government agencies by an organization.

Additional findings include:

1. Small organizations were more likely then medium and large size organizations to report cybercrime incidents to law enforcement or government agencies.

2. 200 of 307 organizations stated that they had detected an incident of cybercrime.
   - 4.9% (15) of the organizations reported 10% or less of cybercrime incidents
   - 5.2% (16) reported between 10 - 25% of cybercrime incidents
   - 8.1% (25) reported between 26 - 50% of cybercrime incidents
   - 6.2% (19) reported between 51 - 75% of cybercrime incidents
   - 12.7% (39) reported between 76 - 100% of cybercrime incidents.
3. 28.0% (86) who detected incidents of cybercrime did not report.
4. 9.8% (30) of organizations in the financial services industry had reported cybercrime incidents, the highest of all industries.
5. 3.3% of the healthcare and public sector, including academia, had reported cybercrime incidents.

Research Question 3

Research Question 3 asked, "Is there a significant relationship between the computer environment and the economic damages incurred by an organization?" There was support for rejecting the null hypothesis with $r = 0.155$ at $\alpha = 0.01$. There is a significant positive relationship between the computing environment and the economic damages incurred for an organization.

Additional findings include:

1. In general, the more PCs, laptops, and workstations (computers) a business had the lower the economic damages experienced by an organization.
2. 15.0% (46) of the organizations with nine or fewer computers had experienced economic damages.
3. 13.0% (40) with 10 - 24 computers had experienced economic damages.
4. 17.6% (54) with 25 - 99 computers had experienced economic damages.
5. 14.7% (45) with 100 - 499 computers had experienced economic damages.
6. 7.8% (24) with 500 - 9,999 computers had experienced economic damages.
7. 4.6% of the organizations with 10,000 or more computers had experience economic damages.

Research Question 4

Research Question 4 asked, "Is there a significant relationship between the computer environment and the percentage of cybercrime incidents reported to law enforcement or government agencies by an organization?" There was support for rejecting the null hypothesis as follows:

Table 6.
Research Question 4 Pearson's *r* and p-values

Variable	Pearson's *r*	p-value
Number of access types to computer systems	-.152**	.007
Number of servers	-.192**	.001
Number of PCs, laptops and workstations	-.129**	.023
Number of security measures in place	-.153**	.007
Number of servers	-.192**	.001

There is a significant negative relationship between the computing environment and the percentage of incident reporting by an organization.

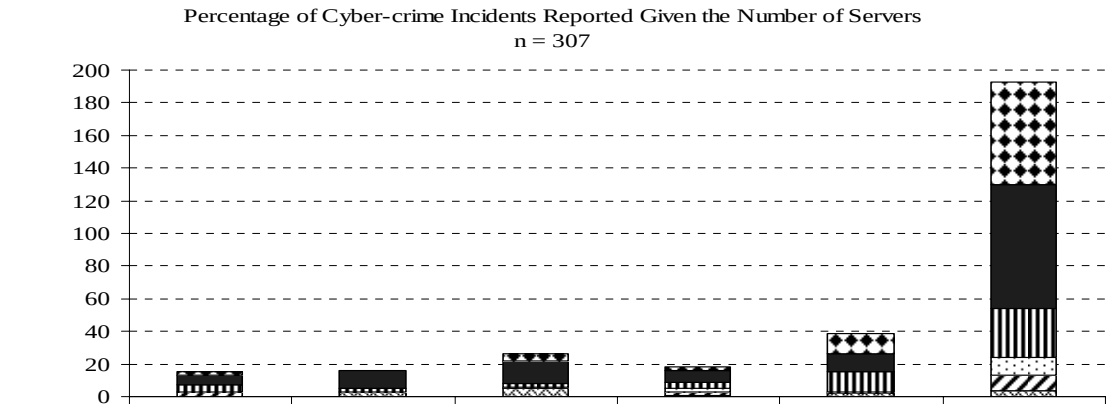
Additional findings include:

1. 37% (114) of the organizations reported incidents of cybercrime to law enforcement or government officials.
2. 19% (58) stated they had reported 50% or more of their cybercrime incidents to law enforcement or government officials.
3. Small organizations were more likely to report an incident of cybercrime to law enforcement or a government agency than medium and large organizations.
4. 63% of organizations, regardless of size, did not report an incident of cybercrime to law enforcement or a government agency.
5. The healthcare and public sector, including academia, was less likely to report incidents of cybercrime than other industries.
6. Organizations that had two different types of security measures in place were more likely to report incidents of cybercrime (see Table 7).

Table 7.
Frequency Table of the Number of Security Measures in Place Given the Percentage of Cybercrime Incidents Reported (n=307)

Number of security measures	1	2	3	4	5	6	7	8	9	10	Total
Number of organizations Reporting	0	12	26	19	17	23	10	18	14	12	114
Percentage (%) of organizations Report	3.9	8.5	6.2	5.5	7.5	3.3	5.9	4.6	3.9	5.9	37.1

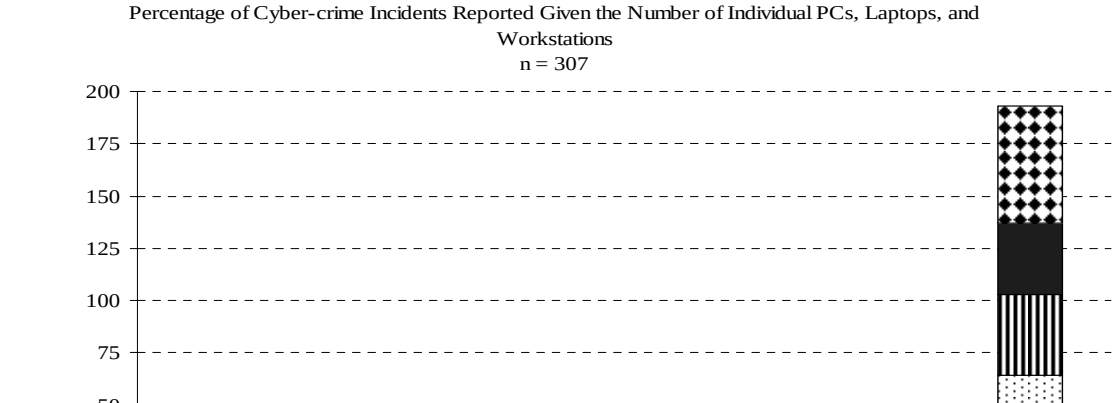
7. Organizations with nine or fewer servers were more likely to report incidents of cybercrime than organizations with a greater number of servers (see Figure 4).



	>10%	10-25%	26-50%	51-75%	76-100%	None
None	2	0	4	2	13	63
1 - 9	6	11	14	7	11	76
10 - 99	4	2	2	4	12	30
100-199	0	0	0	2	0	11
200-499	3	0	1	2	1	9
500+	0	3	5	1	2	4

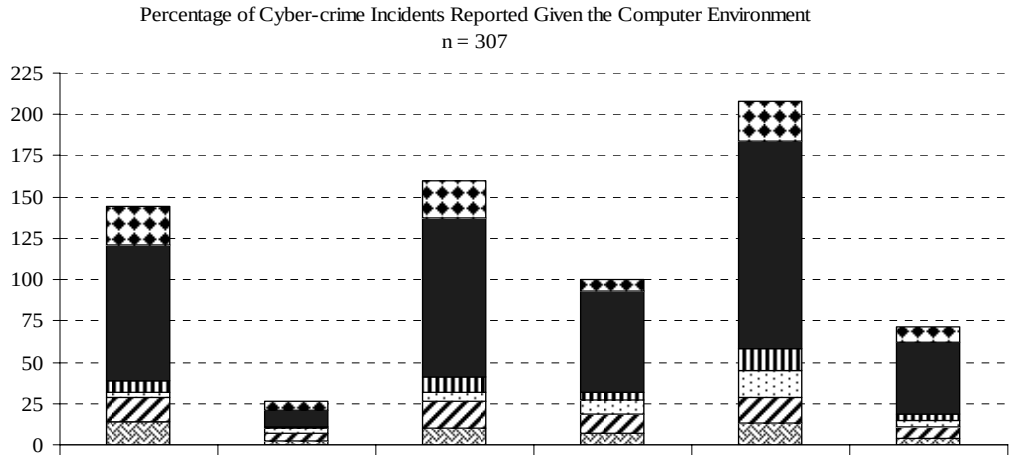
Figure 4. Percentage of cybercrime incidents reported given the number of servers (N=307).

8. Organizations with 500 or fewer computers were more likely to report an incident than those organizations with a greater number of computers (see Figures 5 and 6).



	>10%	10-25%	26-50%	51-75%	76-100%	None
1 - 9	4	1	1	2	9	56
10 - 24	4	4	9	1	6	34
25-99	2	5	8	8	8	39
100 - 499	2	2	2	5	11	39
500- 9,999	3	2	1	1	1	21
10,000+	0	2	5	1	4	4

Figure 5. Percentage of cybercrime incidents reported given the number of individual PCs, laptops and workstations.



	Internet, Intranet, EDI	Mainframe	Stand-alone PCs	VPN	LAN, WAN	Wireless
None	23	5	23	7	24	9
>10%	82	10	96	61	126	43
10-25%	7	1	9	5	13	4
26-50%	3	3	6	8	16	4
51-75%	15	5	16	12	16	7
76-100%	14	2	10	7	13	4

Figure 6. Percentage of cybercrime incidents reported given the computer environment.

9. 29% (89) of the organizations that experienced a cybercrime incident had three or fewer types of access to their computer systems (see Table 8).
10. 6.8% (21) had 4 - 5 types of access to their computer systems.
11. 10.5% (32) had 6 - 7 types of access to their computer systems.

Table 8.
Frequency Table of the Number of Access Types to Computer Systems Given the Percentage of Cybercrime Incidents Reported (n=307)

Number of Access Types	1	2	3	4	5	6	7	Total
Number of Organizations Reporting	24	39	26	12	9	22	10	115
Percentage of Organizations Reporting	7.8	12.7	8.5	3.9	2.9	7.2	3.3	37.5

Research Question 5

Research Question 5 asked, “Is there a significant relationship between the investment in computer security technology and the economic damages resulting from cybercrime experienced by an organization?” There was support for rejecting the null hypothesis as follows:

Table 9.
Question 5 Pearson's *r* and p-value

	Dollar value of losses and costs

	Pearson's *r*	p-value
Percent of total budget spent on security	-.075	.190
Amount spent on computer security	.228*	.000

Note: * denotes correlation is significant at the 0.01 level (2-tailed).

There is a significant relationship between the investment in security technology and the economic damages incurred for an organization.

Additional findings:

1. The smaller the organization the more likely it would incur losses and costs associated with a cybercrime incident.
2. 15.0% (46) of the organizations spent $5,000 or less on computer security.
3. 18.6% (57) spent between $5,000 and $49,000.
4. 13.4% spent between $50,000 and $99,000.
5. 12.7% spent between $100,000 and $199,999.
6. 13.0% (40) spent more than $200,000 on computer security.

Research Question 6

Research Question 6 asked, "Is there a significant relationship between the investment in computer security technology and the reporting of cybercrime incidents to government or regulatory agencies by an organization?" There was not support for rejecting the null hypothesis as follows:

Table 10.
Question 6 Pearson's *r* and p-value

	Percentage of cyber-crime incidents reported	
Variable	Pearson's *r*	p-value
Amount spent on computer security technology	-.105	.066
Percent of total budget spent on security technology	-.034	.557

Note: ** denotes correlation is significant at the 0.01 level (2-tailed). * denotes correlation is significant at the 0.05 level (2-tailed).

There is not a significant relationship between the investment in computer security technology and the percentage of cyber-crime incident reporting by businesses in the greater Houston area.

Additional findings include:
There was support for rejecting the null hypothesis as follows:

1. In general, the more an organization spent on computer security technology the more likely it was to report incidents of cybercrime to law enforcement or government officials.
2. 4.9% (15) of the organizations that invested $5,000 or less in computer security technology indicated that they had reported incidents of cybercrime

3. 9.8% (30) of the organizations that invested more than $200,000 in computer security technology indicated that they had reported incidents of cybercrime.
4. Small organizations were more likely to report incidents of cybercrime than large organizations.
5. There was little difference in the percentage of cybercrime incidents reported among the industries.

Other Data

The top three computer security concerns, as reported by respondents, were (a) embezzlement 30% (92), (b) intrusion or breach of computer systems 22% (67), and (c) computer viruses and denial of service attacks 11% (33). These top three computer security concerns reflect the thinking of 63% of the organizations reporting. Figure 7 depicts in ranking order all the variables identified.

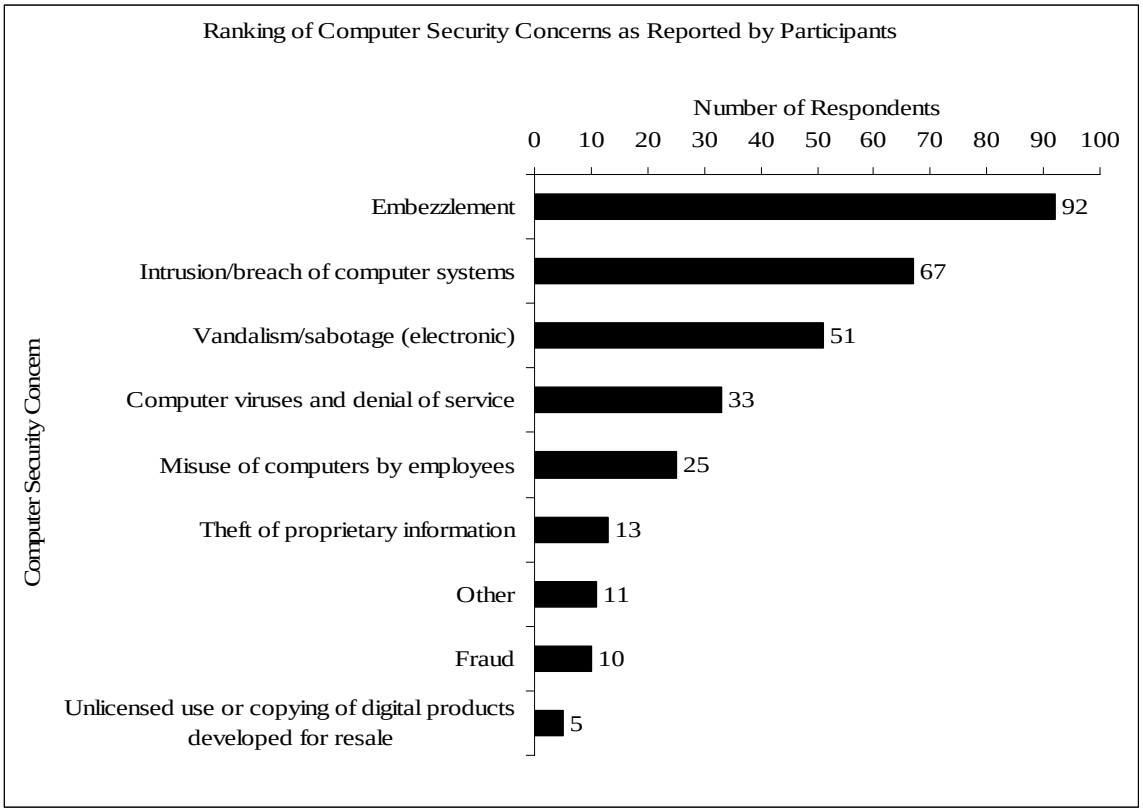


Figure 7. Ranking of computer security concerns by an organization.

Summary of Findings

The data indicates that there is a significant relationship between the:

1. Percentage of cybercrime incidents detected and the dollar value of losses and costs incurred from a cybercrime incident.
2. Percentage of cybercrime incidents detected and the percentage of cybercrime incidents reported to law enforcement or government agencies.
3. Computer environment and the dollar value of losses and costs incurred from a cybercrime incident.

4. Computer environment and the percentage of cybercrime incidents reported to law enforcement or government agencies.
5. Investment in computer security and the dollar value of losses and costs incurred from a cybercrime incident.

The data indicates there is not a signification relationship between the:

6. Investment in computer security and the percentage of cybercrime incident reporting by an organization.

Conclusions, Implications, and Recommendations

Conclusion

The results of the study provide support that cybercrime is influenced by the level of prevention applied within the computer infrastructure of an organization; an outcome strongly suggested by prior studies. The results from the research suggest that while there is a need for organizations to report cybercrime incidents detected they also need legislation that encourages the reporting of these incidents to law enforcement or regulatory agencies. The results also suggest that the level of investment in the security of the computing infrastructure influences the economic damages a business incurs from a cybercrime incident.

Table 11.
Correlational Summary - Pearson's Correlation Coefficient for Each Relationships Examined (n=307)

		Dependent Variables	
	Independent Variables	Percentage of cybercrime incidents reported	Dollar value of the losses and costs incurred (Economic Damages)
1.	Number of access types to computer systems	-.152**	.050
2.	Number of servers	-.192**	.040
3.	Number of computers	-.129**	.151**
4.	Number of security measures in place	-.153**	.108
5.	Percentage of cybercrime incidents detected	.461**	.188**
6.	Investment in computer system security technology	-.105	.228**
7.	Percentage of the total 2006 IT budget spent on computer system security technology	-.034	-.075

Note: * denotes correlation is significant at the 0.01 level (2-tailed).

Implications

Current findings provide support for the adoption of a more planned approach to information security as a part of an information technology strategy before a cybercrime attack occurs. The information technology strategy requires increased focus and attention by senior management. Unfavorable situations were characteristic of

organizations who invested less in their computer infrastructure given their size and industry. Many organizations will invest significant resources in physical security to reduce the risk of burglary and theft of goods on their premise. Many physical security breaches result in lower economic and non-economic than cybercrimes, which can cause far greater economic and non-economic harm to an organization. Organizations that invest more in their computer security infrastructure reduce the rewards of committing a crime by increasing the difficulty and the associated risks of capture.

It is important to study cybercrime as it brings to light knowledge of what daily factors actually constitute a level of victimization for an organization and what might reduce cybercrime. While some approaches (such as a longitudinal study) may be helpful in better understanding cybercrime, the correlational study illustrated that there are behaviors that affect the likelihood of an organization falling victim to cybercrime. The results specifically demonstrated that organizations who invested more in their computer security infrastructure reduced their likelihood of cybercrime victimization.

Leadership Implications

The findings imply that if organizations participate in a process that promotes information security, they will develop transformational behaviors with which to provide greater security for their organization regardless of industry. As individual organizations enhance their information security posture, organizations across the community will benefit.

Organizations need transformational and principle-centered leaders whom can direct evolving IT organizations towards a more secure IT environment. Such an environment would enable growth, education, and an enhanced virtual security posture. It is crucial that organizations increase their investment in computer security technology and demand technological solutions that are affordable, reliable, and scalable from their vendors. Failure to implement these IT changes, as shown by the study, will result in increased incidents of cybercrime attacks that are more severe in terms of potential economic and non-economic damages.

Leaders concerned with the sustainability and success of their organizations' computer security infrastructure must find solutions to the challenges of the changing workforce, workplace, and technology. The study supports the theory that patient cyber-criminals have been able to gradually remove IT security obstacles and have matured beyond DDoS attacks to cybercrimes causing even greater dollar losses. The current study supports the theory that organizations need to invest more and build a computer infrastructure using leaders and information security personnel that exhibit transformational behaviors for managing innovation and change.

Training and information exchange sessions could aid key personnel understand when and under what condition they should report incidents of cybercrime as well as how much and where to invest in computer security technology. These improvements support law enforcement and policy makers in societal pursuits of decreasing cybercrime. Findings from the research may support leaders and policy makers in their efforts to acquire corporate sponsorship in developing and passing new legislation that promotes

greater incident reporting. Additionally, the findings support partnerships among academia, corporations, law enforcement, and government policy makers who may serve as models of desired behaviors. Academic leaders might find the results significant as the outcomes support claims of the value of investing in a computer security program to better protect the service of students and faculty.

Many organizations characterize cybercrime as a serious threat to their organization. Given the inexorable means that cybercriminals have to attack an organization and the anticipated increase in cybercrime, it is recommended that organizations develop useable models to identify programs based on industry and size to help reduce their vulnerability to cybercrime. Given the relative leadership crisis many organizations face when a cybercrime event occurs and the negative impact on an organization, there is a pressing need to investigate further cybercrime's links to economic damages and computer security infrastructure.

Organizational leaders who intend to lead through changing technological contingencies, who face limited funding and support to enhance their computer infrastructure, and who recognize the importance of a sound information security program are advised to continually pursue the type of information imparted in the study. While benefits to the organization of improved information security, decision-making, greater creativity, and innovation are inherent, significant costs may be incurred. Organizational leaders who fail to welcome new technology risk higher incidents of cyber attacks.

Policy Implications

The policy formulation and implementation process requires collaboration among several stakeholders. As the framework for examining cybercrime matures, it is apparent that the primary groups in the policy creation and allocation of resources to combat cybercrime include law enforcement, the business community, consumers, academia, and government policy makers. It seems imperative that these groups collectively reach the consensus that cybercrime is a major social issue that continues to grow as the world becomes increasingly dependent on computers and the networking of various computing devices. We have experienced significant world events because of computer shortcomings, such as the 2003 power failures on the Eastern U.S. seaboard and in London committed by cybercriminals.

To mobilize resources and implement policies that will protect the U.S. from cybercrimes, organizations should recognize that computer misuse within an organization has the capability to create major social issues. Cybercrime is a major threat to U.S. domestic and national security because of the potential impact these crimes can have on the economy and critical infrastructures. Cybercrime is a major threat to academia because the liberal access granted within many college and university environments that provide greater academic freedoms also presents a greater opportunity for cybercrimes such as illegal file sharing,

Although a common computer infrastructure was not discovered that is better able to prevent cybercrime, the findings did indicate that organizations share a common

propensity for cybercrime attacks based on their computer security infrastructure and their risk to cybercrime.

As learned from the study, organizations of all types generally view cybercrime as becoming a more serious threat to their organization as cyber-attacks increase in severity and frequency, and as the computer infrastructure increases in complexity. It is likely that where a business is not aware of certain types of cybercrime, ignorance may become the greatest threat for a business. Cybercrimes have the ability to cause major damages to any organization. Until academia, business leaders, law enforcement and government policy makers are able to garner sufficient resources and training, true reform will continue to lag in how organizations might protect their systems.

Collectively, the results from testing these hypotheses illustrated that given the current resources and budgetary constraints, many organizations continue to under-fund, are unfamiliar with, or are ill prepared to protect, investigate, and enforce sound computer security practices to help in minimizing the risks associated with cybercrime. While the list of cybercrimes identified within the study was not exhaustive, it did offer a starting point from which to address the issue.

Recommendations

The recommendations for an organization are as follows:

1. Assume your organization will be attacked and begin to prepare by implementing an information security program based on best practices.
2. Encourage organizations to report cybercrime incidents as they occur in order to place pressure on law enforcement to prioritize prevention of cybercrime and allocate sufficient resources to investigate and prosecute perpetrators.
3. Create a national standard that is universally accepted defining cybercrime.
4. Develop a single national database to gather and compile cybercrime data.
5. Establish legislation that encourages incident reporting while reducing the risks associated with reporting.
6. Develop policies that provide stronger sentences for those found guilty of committing a cybercrime.
7. Academia in partnership with law enforcement should educate the society on when and how to report cybercrime incidents.
8. Academia and the business community should collaborate on research and the development of new technologies to foster faster delivery and more affordable information security solutions.
9. Establish partnerships among academia, government, law enforcement, and the business community to jointly develop educational programs offering focused on cybercrime prevention.
10. Have academia provide courses and programs both through credit and non-credit programs that cover learners of all ages and skill.
11. Implement victim friendly reporting mechanisms to encourage reporting of incidents within and by organizations.

12. Reconsider approaches used within an organization to determining the appropriate level of investment in computer security technology and the IT infrastructure.
13. Increase investment in information security to reduce the level of victimization to cybercrime.
14. Attention should be given to more adequately secure and reduce the number of “backdoors” that cybercriminals can access.
15. Strengthen information security controls that are in place.
16. Build the computer infrastructure of an organization to prevent or minimize the impact of cybercrime.
17. Educate and invest in current security technology and the human firewall today -- the greatest tools to reduce the economic harm resulting from cybercrime.
18. Use multiple forms of security measures to make entry by users with malicious intent more difficult.
19. Manufacturers of hardware and software should build products with security as a core function of any product so that organizations can focus on configuration and education rather than selection of third party solutions to provide security for their environment.
20. Apply proactive prevention measures such as real-time content inspection, zero-hour vulnerability protection, anti-crimeware, anti-spyware, anti-phishing, anti-virus, and URL filtering.

Summary

The descriptive correlation study analyzed the correlation between the computer environment, investment, and the number of cybercrime incidents detected and the economic harm and the percentage of cybercrime incidents reported by an organization.

The findings from the study are important for academia, business leaders and information security personnel and suggest the influence of the investment in computer security technology and an organization’s IT infrastructure influences the number of cybercrime attacks, the percentage of cybercrime incidents reported, and the dollar loss that results from a cybercrime event.

The most significant variable interaction found is the moderately positive correlation between the percentage of cybercrime incidents detected and the percentage of cybercrime incidents reported. The more incidents an organization experiences the more likely the organization will report incidents at a higher level. Conversely, there was no significant relationship noted between the investment in computer security technology and the percentage of cybercrime incidents reported.

It is important for organizations to report cybercrime incidents, as they occur in order to place pressure on law enforcement to prioritize prevention of cybercrime and allocate sufficient resources to investigate and prosecute perpetrators. Organizations should collaborate with policy makers to develop policies that encourage the reporting of cybercrime incidents and provide stronger sentences for those found guilty. Education is an essential element of prevention.

Lessons learned from this study is that as details emerge regarding the influence cybercrime attacks have on an organization, business leaders should be concerned that many organizations are not prepared to protect their organizations from cybercrime attacks. Concerns regarding cybercrime have grown from simple virus attacks, theft of proprietary information, and DDoS attacks to the shut down of critical infrastructures, millions of compromised records, and loss of productivity for sustained periods. Weaknesses in information security are a widespread problem with potentially devastating consequences. Business leaders and academia, in collaboration with government officials, law enforcement agencies, and consumers should pursue opportunities to develop stronger prevention programs.

About the Author

Denise Chatam, D.B.A., is Dean of Technology and Institutional Research at Lone Star Community College – Cy-fair and author of *Cybercrime: Secure IT or Lose IT* scheduled for release January 2008. Dr. Chatam has more than 20 years of progressive IT leadership in auditing, security, business continuity, global application development, and project management. She is a public speaker on cybercrime prevention programs, implementing and sustaining a comprehensive risk management program including SOX and PCI, project management tips, tricks, and traps, and IT analysis and strategy. Dr. Chatam holds a Doctorate of Business Administration, specializing in information security and cybercrime, a Masters of Science in Engineering Management, Industrial Engineering, and a graduate certificate in project management. For more information, please contact Dr. Chatam at denise.m.chatam@nhmccd.edu.

References

Barr, J. G. (2003, December). *Monitoring employee computer usage.* Retrieved electronically December 27, 2004, from URL: http://80-www.faulkner.com.ezproxy.apollolibrary.com/products/securitymgt/docs/monitoring1203.htm.

Barr, J. G. (2004, March). *Educating employees about identity theft.* Retrieved electronically December 27, 2004, from URL: http://80-www.faulkner.com.ezproxy.apollolibrary.com/products/securitymgt/docs/pdf/idtheft032004.pdf.

Barr, J. G. (2005, January). *Corporate espionage via spyware.* Retrieved electronically February 1, 2005, from URL: http://80-www.faulkner.com.ezproxy.apollolibrary.com/products/securitymgt/docs/spyware0105.htm.

Barr, J. G. (2005, May). *Forensic computing.* Retrieved electronically June 25, 2006, from URL: http://www.faulkner.com.ezproxy.apollolibrary.com/products/securitymgt/.

Bell, R. E. (2002, April). The prosecution of computer crime. *Journal of Financial Crime, (9)*4, pp. 308 – 326. London, England.

Bierman, E., & Cloete, E. (2002). Classification of malicious host threats in mobile agent computing. *ACM International Conference Proceeding Series, Proceedings of the 2002 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology,* pp. 141 – 148. Port Elizabeth, Republic of South Africa: South African Institute for Computer Scientists and Information Technologists.

Bigelow, B. V. (2005, February 3). Computer theft may put workers' data in danger. *Knight Ridder Tribune Business News.* Washington, DC: Knight Ridder Tribune Information Services.

Block, S. (2004, November 30). New weapon to battle identity thieves unsheathed this week. *USA Today.* Arlington, VA: USA Today Information Network.

Broder, B. (2003, December 15). *Identity theft: Assessing the problem and efforts to combat it: Hearing before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, House of Representatives, One Hundred Eighth Congress, First Session, December 15, 2003.* Washington, DC: United States Government Printing Office.

Camp, E. G. (2003, April 30). *White-collar crime: History and social impacts.* Retrieved electronically September 6, 2006, from URL: http://www.providence.edu/polisci/students/corporate_crime/index.html.

Chapman, R. E. (2003, October). *U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, Office of Applied Economics, Building and Fire Research Laboratory, Application of Life-cycle Cost Analysis to Homeland Security Issues in Constructed Facilities: A Case Study.* Retrieved electronically December 18, 2004, from URL: http://www.bfrl.nist.gov/oae/publications/nistirs/7025.pdf.

Citrano, V. (2006, January 20). *Mueller's FBI puts computer crime losses at $32M.* Retrieved electronically September 1, 2006, from URL: http://www.forbes.com/facesinthenews/2006/01/20/fbi-computer-security-cx_vc_0120autofacescan07.html?partner=vnu.
Clinard, M. B. (1978). *Cities with little crime: The case of Switzerland.* Cambridge, England and New York, NY: Cambridge University Press.
Clinard, M. B. & Yeager, P. C. (1980). *Corporate Crime (Law and Society Series).* New York, NY: The Free Press, a Division of Macmillan Publishing Co., Inc.
Computer Security Institute. (2003). *2003 CSI-FBI Survey results*. Retrieved electronically November 22, 2003, at URL: http://www.gocsi.com/.
Computer Security Institute. (2004). *2004 CSI-FBI Survey results*. Retrieved electronically November 18, 2005, at URL: http://www.gocsi.com/.
Computer Security Institute. (2006). *2005 CSI-FBI Survey results*. Retrieved electronically July 1, 2007, at URL: http://www.gocsi.com/.
Consumer Protection Division, Office of the Attorney General, State of Washington (2004). *Con games that target older adults.* Retrieved electronically December 28, 2004, from URL: http://www.atg.wa.gov/consumer/con_games.shtml.
Creative Research Systems. (2006). *The survey system sample size calculator.* Retrieved electronically April 9, 2006, from URL: http://www.surveysystem.com/sscalc.htm.
Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage.
Cressey, D. R. (1955). Changing criminals: The application of the Theory of Differential Association. *American Journal of Sociology (61),* pp. 116 – 120.
Cressey, D. R. (1960). Epidemiology and individual conduct: A case from criminology. *Pacific Sociological Review (3).* pp. 47 – 58.
Creswell, J. W. (2002). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Upper Saddle River, NJ: Pearson.
Easen, N. (2004, April 21). *Cybercrime is right under your nose.* Retrieved electronically September 1, 2006, from URL: http://www.cnn.com/2004/BUSINESS/04/20/go.cyber.security/index.html.
Electronic Privacy Information Center. (2004, March). *The Gramm-Leach-Bliley Act.* Retrieved electronically December 29, 2004, from URL: http://www.epic.org/privacy/glba/.
Equifax. (2004). *About your credit.* Retrieved electronically January 5, 2004, from URL: http://www.equifax.com/.
Equifax. (2004). *Fraud.* Retrieved electronically September 8, 2004 from http://www.equifax.com.
Equifax. (2004). *Identity theft.* Retrieved electronically December 19, 2004, from URL: http://www.equifax.com/corp/identity-theft.htm.
Equifax. (2004). *Identity Theft Insights.* Retrieved electronically December 18, 2004, from URL: https://www.econsumer.equifax.com/consumer/.
Evans, M. P., and Furnell, S. M. (2000). Internet-based security incidents and the potential for false alarms. *Internet Research: Electronic Networking Applications and Policy, (10)*3, pp. 238 – 245. Plymouth, UK: MCB University Press.

Evers, J. (2006, January 19). Computer Crime Costs $67 Billion, FBI Says. *Cnet News.com.* Retrieved electronically September 30, 2006, from URL: http://news.com.com/Computer+crime+costs+67+billion%2C+FBI+says/2100-7349_3-6028946.html?tag=cd.top.

Federal Bureau of Investigation. (2003). *FBI announces operation continued action targeting financial institution fraud.* Retrieved electronically December 13, 2004, from URL: http://www.fbi.gov/pressrel/pressrel04/contaction091704.htm.

Federal Bureau of Investigation. (2003). *FBI announces operation continued action targeting financial institution fraud.* Retrieved electronically December 13, 2004, from URL: http://www.fbi.gov/pressrel/pressrel04/contaction091704.htm.

Federal Bureau of Investigation. (2006, January 18). *Hot off the press. New FBI computer crime survey.* Retrieved electronically July 27, 2006, from URL: http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm.

Federal Deposit Insurance Corporation. (2001, March). *Social Security Standards for Customer Information.* FIL-22-2001. Washington, DC: FDIC.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security, (11)*2, pp. 74 – 83. Bradford, West Yorkshire, England: Emerald Group Publishing Limited.

Gibbons, D. C. (1999, April). Review Essay: Changing lawbreakers – What have we learned since the 1950s? *Crime & Delinquency, (45)*2, pp. 272-293.

Internet Crime Complaint Center. (2006). *About us.* Retrieved electronically March 25, 2006, from URL: http://www.ic3.gov/about/.

Internet Crime Complaint Center. (2007). *IC3 2005 Internet Crime Report. January 1, 2006 – December 31, 2006. Prepared by the National White Collar Crime Center and the Federal Bureau of Investigations.* Retrieved electronically November 1, 2007, from URL: http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

Kowalski, M. (2002). Cybercrime: Issues, data sources, and feasibility of collecting police-reported statistics. *Minister of Industry, Catalogue Number 85-558-XIE.* Ottawa, Ontario, Canada: Statistics Canada, Canadian Centre for Justice Statistics.

Krause, M. S. (2002, August). *Contemporary white collar crime research: a survey of findings relevant to personnel security research and practice.* Washington, DC: United States Navy.

Kutnick, G. (2006, April 24). *Complying with the Payment Card Industry Standard.* Retrieved electronically September 3, 2007, from URL: http://www.gartner.com/it/products/podcasting/asset_147277_2575.jsp.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical research planning and design.* (7th Ed.) New York: NY: Macmillan.

McConnell, B. W. (2001, March 6). *Hearing on cybercrime, Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe.* Paris, France: McConnell International.

McNeil Solida, M. (2003, February 18). *Ex-pension employee is charged.* Retrieved electronically December 28, 2006, from URL: http://www.carlbrizzi.com/news/display.php3?NewsID=71.

Michael, A., Potter, C., & Beard, A. (2006). *Information Security Breaches Survey 2006.* Retrieved electronically August 30, 2007, from URL: http://www.dti.gov.uk/industries/information_security.

National White Collar Crime Center. (2001). *Identity Theft.* Retrieved electronically December 1, 2004, from URL: http://www.nw3c.org.

National White Collar Crime Center and the Federal Bureau of Investigation. (2005). *IC3 2004 Internet Fraud – Crime Report. January 1, 2004 – December 31, 2004.* Retrieved electronically February 1, 2005, from URL: http://www.ifccfbi.gov/strategy/2004_IC3Report.pdf.

National White Collar Crime Center and the Federal Bureau of Investigation. (2006, February), *IC3 2006 Internet Crime Report. January 1, 2006 – December 31, 2006.* Washington, DC: Federal Bureau of Investigations.

Office of the Press Secretary, The White House. (2001, December 28). *President Signs Intelligence Authorization Act. Statement by the President*. Retrieved electronically June 15, 2007, from URL: http://www.whitehouse.gov/news/releases/2001/12/20011228-3.html.

Podgor, E. S. (2002, Summer). Computer crimes and the USA PATRIOT Act*. Criminal Justice, (17)*2, pp. 61 – 63, 69.

Ponsaers, P. (2002, April). What is so organized about financial-economic crime? – The Belgian case. *Crime, Law and Social Change (37)*3, pp. 191-201. Netherlands: Kluwer Academic Publishers.

Rantala, R. R. (2004, March). Cybercrime against organizations*. United States Department of Justice, Office of Justice Programs, The Bureau of Justice Statistics Technical Report (NCJ200639).* Retrieved electronically October 28, 2005, from URL: http://www.ojp.usdoj.gov/bjs/.

Rusch, J. (2005, May 3). *The rising tide of Internet fraud.* Retrieved electronically July 27, 2007, from URL: http://www.usdoj.gov/criminal/cybercrime/usamay2001_1.htm.

Salkind, N. J. (2003). *Exploring Research. (5th ed.).* Upper Saddle River, NJ: Prentice Hall.

Schwartz, M. (2003, June 11). *CSI/FBI Report: Losses down, vulnerabilities up.* Retrieved electronically June 1, 2006, from URL: http://www.esj.com/Security/article.aspx?EditorialsID=583.

Social Security Administration. (2006, March 16). *U.S. House of Representatives – March 16, 2006 Committee on Ways and Means Subcommittee on Social Security Statement for the Record, Social Security Number High-Risk Issues.* Retrieved electronically June 24, 2007, from URL: http://www.ssa.gov/oig/communications/testimony_speeches/03162006testimony.htm.

Sutherland, E. H. (1949). *White Collar Crime.* New York, NY: Dryden Press.

Sutherland, E. H., and Cressey, D. (1978). *Principles of Criminology. (10th ed.).* New York, NY: Lippincott.

Texas Economic Development, Business and Industry Data Center. (2004). *Education, migration, and other social characteristics by COGs.* Retrieved electronically September 28, 2007, from URL: http://bidc.state.tx.us/demprofile/.

Texas Economic Development, Business and Industry Data Center. (2004). *Industry Statistics.* Retrieved electronically December 28, 2006, from URL: http://bidc.state.tx.us/demprofile/Industry.xls.

Texas Economic Development, Business and Industry Data Center. (2004). *State Comparison – Texas and the United States.* Retrieved electronically December 28, 2004, from URL: http://bidc.state.tx.us/50state/result.cfm.

Texas Economic Development, Business and Industry Data Center. (2004). *The Texas Challenge in the Twenty-First Century: Implications of Population. Table 2.7 Population for the State of Texas and Council of Government Regions in Texas in 2000 and Projects to 2040 Assuming Alternative Projection Scenarios.* Retrieved electronically December 28, 2006, from URL: http://txsdc.tamu.edu/pubsrep/pubs/txchalcog/cogtab2-07.txt.

Trandahl, J. (2001, October 24). *USA PATRIOT Act. HR3162 RDS, 107TH Congress, 1st Session, H. R. 3162 in the Senate of the United States October 24, 2001.* Washington, DC: Electronic Privacy Information Center.

United States Census Bureau. (2006). *County Business Patterns.* Retrieved electronically January 20, 2007, from URL: http://www.census.gov/prod/www/abs/cbptotal.html.

United States Department of Health and Human Services. (2003, May). *Office for Civil Rights (OCR) Privacy Brief, Summary of the HIPAA Privacy Rule, HIPAA Compliance Assistance.* Retrieved electronically December 29, 2006, from URL: http://www.hhs.gov/ocr/privacysummary.rtf.

United States Department of Health and Human Services. (2006). *Public Law 104-191, August 21, 1996 Health Insurance Portability and Accountability Act of 1996.* Retrieved electronically September 30, 2006, from URL: http://aspe.hhs.gov/admnsimp/pl104191.htm.

United States Department on Homeland Security. (2004). *President's Commission on Critical Infrastructure Protection.* Retrieved electronically November 24, 2006 at URL: http://www.ciao.gov/resource/commission.html.

United States Department of Homeland Security and United States Secret Service. (2004). *Secret Service and CERT Coordination Center release comprehensive report analyzing insider threats to banking and finance sector. First of a series of reports to focus on threats to information systems and data in critical infrastructure sectors.* Retrieved electronically January 25, 2007, from URL: http://www.secretservice.gov/press/pub1804.pdf.

United States Department of Homeland Security and United States Secret Service. (2004, July 21). *U.S. Secret Service Joins Federal Task Force to Solve Major Network Intrusion Case. PUB 16-04.* Washington, DC: United States Secret Service, Office of Government and Public Affairs.

United States Department of Homeland Security and United States Secret Service. (2004, October 28). *U.S. Secret Service's Operation Firewall Nets 28 arrests. International undercover investigation prevents millions in financial loss. (GPA 23-04).* Washington, DC: United States Secret Service Office of Government and Public Affairs.

United States Department of Justice. (2005, December 28). *Man pleads guilty to infecting thousands of computers using worm program then launching them in denial of service attacks.* Retrieved electronically April 17, 2006, from URL: http://www.cybercrime.gov/clarkPlea.htm.

United States Department of Justice, CRM. (2006, March 1). *Former federal computer security specialist pleads guilty to hacking Department of Education computer.* 06-106. Retrieved electronically April 17, 2007, from URL: http://www.cybercrime.gov/kwakPlea.htm.

United States General Accounting Office. (2002, March). *Identity Theft: Prevalence and cost appear to be growing.* Retrieved electronically December 19, 2007, from URL: http://www.ntis.gov.

United States House of Representatives. (2003, April 3). Fighting fraud: Improving logical security*. U.S. House of Representatives, Subcommittee on Financial Institutions and Consumer Credit, Joint with the Subcommittee on Oversight and Investigations, Committee on Financial Services.* Washington, DC: Government Accounting Office.

United States House of Representatives. (2003, June 26). *108th Congress First Session. H.R.2622. Fair and Accurate Credit Transactions Act of 2003 (Introduced in House).* Retrieved electronically December 19, 2006, from URL: http://thomas.loc.gov/.

Unnithan, N. P. (2002, January). Wayward Icelanders: Punishment, boundary maintenance, and the creation of crime. *Contemporary Sociology, (31)*1. Washington, DC: American Sociological Association.

Uranga, J. J. (2003, September 30). *Report on the Conference on cyber-security.* Buenos Aires, Argentina: Organization of American States Conference on Cyber-Security.

Vande Walle, G. (2002, April). “The collar makes the difference” – Masculine criminology and its refusal to recognize markets as criminogenic. *Crime, Law & Social Change (37),* pp. 277-291. Netherlands: Kluwer Academic Publishers.

Weir, M. (2004, February 24). PostX leads fight against online identity theft; leader in the secure content delivery space becomes founding member of coalition formed by Information Technology Association of America (ITAA). *PR Newswire Association, Inc.* Retrieved electronically December 27, 2006, from URL: http://web5.infotrac.galegroup.com/itw/infomark/117/199/59088646w5/purl=rc1_ITOF_0_A113560927&dyn=3!xrn_1_0_A113560927?sw_aep=uphoenix.

White, G. A., & Kern, R. W. (2006, February 28). *Cleveland, Ohio man sentenced to prison for bank fraud and conspiracy.* Retrieved electronically April 17, 2006, from URL: http://www.cybercrime.gov/flurySent.htm.

Whitney, S. (2004, December 1). Trend turns, more purchase coverage for cybercrime. *Best’s Review, 105(8):90.* Oldwick, NJ: A.M. Best Co. Inc.

Williams, P. (2002). *Organized crime and cybercrime: Implications for business.* Retrieved electronically October 15, 2007, from URL: http://www.cert.org/archive/pdf/cybercrime-business.pdf#search='FBI%20cyber%20crime%20profit'.

Williams, P., Dunlevy, C., & Shimeall, T. (2006, April 15). *Intelligence Analysis for Internet security.* Retrieved electronically June 1, 2007, from URL: http://www.cert.org/archive/html/Analysis10a.html.
Wikipedia. (2006). *English dictionary.* Retrieved electronically June 26, 2007, from URL: http://www.wikipedia.org/wiki/.