CRIMINAL JUSTICE RESPONSES TO

EMERGING COMPUTER CRIME PROBLEMS

Osman N. Sen, B.S.

Thesis Prepared for the Degree of

MASTER OF SCIENCE

UNIVERSITY OF NORTH TEXAS

August 2001

APPROVED:

Robert W. Taylor, Major Professor and
Chair of the Department of Criminal Justice
Tory J. Caeti, Committee Member
Bradley Chilton, Committee Member
David W. Hartman, Dean of the School of
Community Service
Neal Tate, Dean of the Toulouse School of
Graduate Studies

Sen, Osman N., Criminal justice responses to emerging computer crime problems. Master of Science (Criminal Justice), August 2001, 133 pp., 4 tables, 3 illustrations, 100 references.

This study discussed the issue of computer crime as it relates to the criminal justice system, specifically law enforcement. The information was gathered through several books, academic journals, governmental documents, and the Internet. First, the nature and forms of computer crime, Internet crime, and cyber terrorism were analyzed. Next, law enforcement responses were discussed. International aspects of the problem were separately pointed out. Further, detection and investigation of computer crime were examined.

Problems related to the each component of the criminal justice system (law enforcement, investigators, prosecutors, and judges) were described. Specific solutions to these problems were offered. In addition, computer crime handling procedures were presented.

Results indicate that computer crime will increase in the 21st century, and this problem cannot be controlled by traditional methods alone. Using new technology as preventive measures, and increasing awareness and security conscious culture will prevent the problem in the long run.

ACKNOWLEDGEMENTS

I am very thankful to my committee chair Dr. Robert W. Taylor for his guidance, information, and support in this thesis. I also appreciate the help of committee members Dr. Tory J. Caeti and Dr. Brad Chilton. I want to express my appreciation to the University of North Texas Libraries where I have conducted most of my research. I also thank the Turkish National Police for providing me financial support for this degree. Finally, I want to extend my deepest appreciation to my wife, Hikmet, for her love, patience, understanding, and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

CHAPTER 1

INTRODUCTION

Purpose of The Study

This study addresses the issue of computer crime as it relates to the criminal justice system, and especially law enforcement. The entire criminal justice system, including investigators, law enforcement personnel, prosecutors, and judges, are faced with the challenges posed by computer crime. Further, this study describes the impact of computer crime on society and its institutions. A model for law enforcement to respond to computer crime is also presented.

Background

With the enormous advances in the computer and telecommunication industries, computers are now being used in almost all walks of life all over the world. Indeed, computers today touch every aspect of society including the financial industry, manufacturing industry, universities, insurance companies, law enforcement, and governmental agencies. With the advent of the Internet, computer usage has also spread to most individual homes. According to the Computer Emergency Response Team (CERT), the projected number of Internet host computers was 13 million in 1996, 85 million in 1998, 370 million in 1999, and 900 million in 2000 (Cain et al., 1999). The estimated total number of the Internet users (people who are 'online') worldwide as of

November 2000 is 407.1 million (www.spcustom.com). We are so surrounded by computer systems that we cannot avoid interaction with them. This interaction provides computer criminals the opportunity to wreak havoc (e.g., shut down systems, interrupt telephone services, disrupt air and highway traffic, cease bank operations and exchange markets, remotely alter the formulas of medication at pharmaceutical manufacturers, or stop utility services) by using high-tech communications systems. In some cases, our interaction with computer systems is evident, such as when we use an automatic teller machine. However, in other cases our computer interaction may not be so apparent, such as when we use telephone services.

Computer technology provides the ability to collect and analyze large quantities of data very easily and rapidly, as well as the ability to transmit data throughout the world through the use of the Internet. Through computer technology, governments can collect data about specific events, and businesses can collect vital statistics and other information about customers and their purchasing habits.

New technologies have always brought problems as well as solutions. The use of computer technology has not only helped governments, businesses, and individuals, but it has also enabled criminals with sophisticated computer knowledge to use computers in illegitimate ways. Computers offer criminals the opportunity to break laws, and computers offer the ability to commit traditional crimes in non-traditional ways.

Computers and computer systems may be targeted by criminals because of their various idiosyncratic vulnerabilities. Vulnerability has increased following the abrupt rise of computer networks. As the most important aspects of national infrastructure become dependent on computer technology, security issues have received more attention. Most security systems are powerless because of the difficulty of detection. Scarcity of successful detection is due mainly to the vagueness of time and space dimensions often observed in computer crime. It is difficult to determine when and where computer crime occurs. Indeed, computer criminals do not attack with explosives or dynamite; instead, they use telecommunication and other technologies. In other words they attack with 'ones' and 'zeroes'.

The potential damage done by computer-related crime can be more extensive than in traditional crime. Indeed, computer crime may involve large amounts of money in cyberspace. The aggregate losses to governments, businesses, and individuals are estimated to be in the billions of dollars (Aldrich, 2000). Therefore, it is argued that crimes committed through the utilization of computers are now more harmful than so-called traditional crime. Furthermore, organized crime has entered the cyber crime arena. This offers support to the age-old diction: "where money accumulates, so do criminals."

In contrast with traditional security issues, law enforcement does not have enough experience and knowledge in ways to protect computers and networks from these kinds of crime. Thus, most computer crime incidents go undetected. Statistics on computer crime are generally not available. This is due to several reasons, such as reluctance of victims to report incidents, and uncertainty of exact definitions and classifications. Despite the absence of accurate statistics, it is generally agreed that the problem is monumental and is continuing to grow (Peters, 1997).

The expansion of worldwide access to the Internet foretells that computer crime will continue to increase. Recently, devastating computer crime incidents have occurred over the Internet such as the denial-of-service attacks to several major commercial web sites in 2000 (e.g., E-bay, Yahoo, E-trade etc) (Government Prepares, 2000). Additionally, the dissemination of the Melissa virus through the Internet in March 1999 provided dramatic evidence of the significant damage that results from these types of attacks (Computer, 2000). These incidents have fueled the debate on control of the Internet. In most cases, local law enforcement agencies do not have the personnel, equipment, and practical knowledge to proactively detect computer crime. The law enforcement community today is required to keep up with the rapidly growing use of high technology. Hence, growth of computer crime requires police officers that are familiar with advanced technology. It is also imperative that prosecutors, investigators, and judges have significant knowledge of computers and computer systems. In other words, the problem demands crucial and quick attention.

Increasing concern about the threat of computer crime has forced the U.S. Department of Justice to request a $37 million budget increase for the year 2000 (Government Sees, 2000). The Justice Department announced that $8.6 million of this money would fund 100 “Computer Analysis and Response Team” members who would investigate computer-related crime (Government Sees, 2000).

Also, international cooperation is required to fight computer crime. A global framework must be developed to address all types of computer crime. To maintain international response, the Justice and Interior Ministers of the G-8 (Canada, England, France, Germany, Italy, Japan, Russia; formerly known as the G-7 plus Russia) at a meeting held in 1997, in Washington D.C. made the decision to combat computer crime (Computer, 2000). The global nature of computer crime, especially over the Internet, requires a global consensus on computer crime and their regulation.

Most industrialized countries have enacted laws against computer crime since the 1970s. The first computer-specific laws concerned the protection of privacy. However, in the 1980s, the focus shifted to computer-related economic crime. Protection of intellectual property also has become an important issue in computer legislation.

Conventional ways of thinking undervalues the importance of computer crime. Officials are missing the important part of the problem—the intrusions that are not detected. Before prevention and detection can occur, the problem must be described. Therefore, in this study, this new threat is discussed. This study provides a descriptive analysis of computer crime including the nature of computer crime, several illustrative cases, and relevant statistics pertaining to computer crime. Analysis, detection, investigation, and appropriate preventive measures are then addressed. In addition, this study identifies problems that police may face during the investigation of a computer crime. The law enforcement perspective, the current situation of the law enforcement response, and what agencies must do in order to catch up with the demand are discussed. Finally, an overall discussion of computer crime concludes this study.

Scope/Limitations of the Study

The scope of this study includes, but is not limited to, computer crime committed using personal computers, network computers or remote terminals communicating with a remote computer or server via modem. Because of the advent of the Internet, the focus is on events occurring after 1980. A technological shift toward a more distributed (versus centralized) computer environment in the 1980s significantly changed the face of computer crime, especially because of increased access to computers by a great number of people.

There are several limitations that naturally arise from any study on computer crime. For example, there is currently no single data source that provides in-depth, reliable and accurate information on computer crime or computer criminals. Unlike other types of crime (e.g. murder, robbery, burglary), there are no national statistics or uniform reporting systems for computer crime. In addition, there is limited information about computer crime incidents in academic literature. Indeed, the literature contains some speculation. However, no information has been rigorously collected using scientific methods. The most popular data source is a survey conducted by the Computer Security Institute (CSI) and sponsored by the Federal Bureau of Investigation (FBI). Another significant limitation to this study is that computer crime is rarely detected. It is often difficult to determine how the offence was committed. Indeed, accurate time and space features of a computer crime may be vague. Further, there are no universally accepted definitions or classifications of computer crime. As such, centralized statistics would be difficult or impossible to collect. The final limitation of this study is the reluctance of institutions, businesses, and individuals to report computer crime. According to some research, the incidents that are not detected far exceed those that are detected. In essence, what is reported is thought to be only tip of the iceberg (Adamski, 1998; Lohr, 1997, Grabosk, 2000).

Methodology of the Study

This study utilizes focused synthesis methodology to analyze computer crime. Focused synthesis is defined as gathering information related to and based on research questions from a variety of sources (Doty, 1982). A focused synthesis is similar to traditional literature reviews; however, it differs from traditional literature review studies in three primary ways: 1) Focused synthesis is not drawn from only published articles, it might also include the researcher's thoughts, personal past experience, unpublished documents, and congressional hearings; 2) The purpose of focused synthesis is to combine available sources on a subject. Focused synthesis has a different purpose than traditional literature. Focused synthesis is done less formally, and it does not aim only to describe prior research. 3) Finally, focused synthesis is prepared to be used as a study to give much detail on a subject. Yet, most research studies tend to be a background for later studies. Focused synthesis attempts to derive results and policy recommendations based on the information gathered in a study (Majchrzak, 1984). These features provide focused synthesis some advantages; such as it can be completed efficiently, quickly, and in a more realistic manner (Majchrzak, 1984). Yin (1994) posits two relevant and important data collection sources for a study of this type: documentation and archival records.

Documentation and archival records are stable and unobtrusive; however, they reflect bias of authors (Yin, 1994).

This study utilizes the available research from academic journals and books, government documentation and data, and current research available online. The ultimate goal of this is to analyze available material on computer crime and enforcement practices in an effect to provide a comprehensive picture of what computer crime is and what is being done about it.

Research Questions

In focused synthesis methodology, the researcher tries to find answers to certain questions. This particular study attempts to answer the following:

- What is computer crime, and how are the different types of computer crime categorized?
- What are the demographic, social characteristics, and modus operandi" of computer criminals?
- What should law enforcement agencies do to investigate and prosecute computer crime?
- What are the current computer crime laws?
- What are the international and jurisdictional problems of computer crime?
- What is the most important computer crime prevention measure: technology, laws and regulations, or awareness?

Importance of the Study

This study is important because it provide detailed descriptions of the three parts of computer-related crime, which are computer crime, Internet crime, and cyber terrorism. In addition, law enforcement response to computer-related crime is discussed in-depth.

CHAPTER 2

COMPUTER-RELATED CRIME

Introduction

The number of people using the Internet reached 50 million within a four-year span (Levesque, 2000). Like other technologies, it was only a matter of time before crimes would be committed utilizing the Internet and computers. To address the computer-related crime problem effectively, the nature of the problem needs to be understood in detail. In this chapter, three main aspects of computer-related crime are discussed: computer crime, Internet crime, and cyber terrorism. Computer crime is any illegal act committed by a person who has knowledge of computer technology. There are several types of computer crime that will be discussed. Internet crime is any type of crime committed via the Internet including attacks, viruses, and more traditional types of crimes. Cyber terrorism uses computer knowledge to commit or to facilitate a crime for political purposes. Each one presents unique issues for academic research and for law enforcement.

Computer Crime

Definitions

Several authors have attempted to define computer crime, including:

"Computer crime is any violation of a computer crime statute" (Parker, 1981).

> "The destruction, theft, or unauthorized or illegal use, modification, or copying of information, programs, services, equipment, or communication networks" (Perry, 1986).
>
> "Any intentional act involving knowledge of computer use or technology is computer abuse if the perpetrator could have made some gain and the victim could have experienced loss" (Parker, 1989).
>
> "Mostly hidden criminality where there is small probability of detection, a high reluctance to report, and inadequate security" (Tenhunen, 1994).
>
> "Computer crime (computer abuse) is the use of a computer to deceive for personal gain" (Strothcamp, 1998).
>
> "Crimes directed at a computer or a computer system" (Stephenson, 2000).

Computer crime takes several forms such as theft, destruction of data or systems, unauthorized use or copying of data, and alteration of data, viruses, trojan horses, logic bombs, and vandalism. The nature of computer crime has become increasingly complex, as technology and the Internet have grown.

Categories of Computer Crime

A simple definition of computer crime is elusive; therefore, categories of computer crime are offered for clarity. As in the definitions, there is diversity in the categories and types of computer crime. In this study, four major areas of computer crime are discussed.

Role of Computers

The first, and widely accepted area classifies computer crimes in terms of the role that computers play. In this area, computer crime falls into one of four types: computers as the end target, computers as the means (instrumentality), computers as incidental to other crimes, and crimes associated with the prevalence of computers (Carter, 1995). These computer crime types provide a useful typology for this study.

Computers as the end target: In this type of computer crime, the offender uses the computer to destroy or obtain information. In other words, the computer itself is the target. Such offenses include theft of intellectual property (e.g., an idea, invention, business method, unique name, or chemical formula), theft of marketing information (i.e., customer information, and price information), and blackmail based on information obtained from computer files (i.e., insurance information). The most common method of obtaining, altering, or destroying data is to become a “super user” or “root.” These tactics are especially prevalent within Unix networks. These are special terms representing the administrator(s) of the computer system. A favorite method of gaining access to computers is to misuse tools such as network sniffers (programs designed to monitor network traffic in order to help network administrators). Another method is the ‘trap door’ (an easy and fast way to enter a program because most of the programmers add them to bypass security processes). Trap doors are widely used by programmers in order to speed up and fix programming errors or “bugs.”

Computers as the means (instrumentality): The computer and contents of computer files are used to facilitate committing a crime. One of the methods of facilitation is that the criminal can introduce a new programming instruction to manipulate the processes. Another method is converting the legitimate processes to illegitimate processes; including, fraudulent use of bank accounts, automated teller machine (ATM) fraud, credit card fraud, and telecommunications fraud. For instance, a programmer for a large bank can introduce a new code to transfer the fractions of a cent of an account or accounts to his/her personal account. A dazzling example of this is:

> "In just 20 days, a fake automated teller (ATM) machine set up by three men in a Connecticut shopping mall recorded the account numbers and personal identification numbers (PIN) of hundreds of unsuspecting customers but gave out no money. Instead, the operators of the fake ATM machine used the recorded credit card numbers and their home computer, with an expensive read/write device, to duplicate legitimate debit cards. They then used these "clone" cards to make more than $100,000 from valid ATM machines, verifying the transactions with the PINs as entered by the victims on the fake ATM" (Flusche, 1998).

Computers (as) incidental to other crimes: In this type, the computer is only related to the criminal act. The crime could occur without the technology. However, use of computers makes the crime occur faster or more efficiently; often times the crime is more difficult to detect and investigate. Not only did computers make businesses more efficient, but they also expedited some criminal acts. These crimes include: drug trafficking, money laundering, child pornography, and illegal banking transactions. With widespread use of the Internet, this type of offense has significantly proliferated.

Crimes associated with the prevalence of computers: In this final type, targets of crimes are created by the proliferation of the technology. These crimes include copyright violation, software piracy, cyber stalking, software counterfeiting, and theft of technological equipment. These are new types of crimes that are introduced by computing technology. The violation of copyright restrictions of commercial programs is one of the main offenses in this category. Indeed, word processing programs, spreadsheet programs, and databases are being copied and sold illegally, and frequently, all over the world.

Computer Vulnerability

A second area of computer crime classifies computer crimes in terms of vulnerability falling into six types: 1) Hardware, 2) Software, 3) Networks, 4) Information/Data, 5) Computer-controlled devices, and 6) Physical structures and buildings (Bequai, 1983).

Hardware: This type of crime occurs when the crime is against hardware, that is, the physical part of the computer. Terminals, monitors, printers, external modems, and the visible parts of the computer are all called hardware.

Software: This type of crime occurs when the crime is against software, that is, the programs, instructions, and information making the computer work.

Networks: This type of crime occurs when the crime is against a network, which is composed of systems (computers) connected by communications media to transfer information among systems. Modems, routers, switches, hubs are included in networks.

Information/Data*:* This type of crime occurs when the crime is against the data stored in the computer system(s). Sometimes this type may be more important than others. For instance, the case against the former Los Alamos scientist Wen Ho Lee was an example of this type of crime. Dr. Lee was indicted of downloading the lost computer files, which contain classified information (Broad, 2000).

Computer-controlled devices: This type of crime occurs when the crime is against computer-controlled devices, used in numerous industries that are managed and controlled by computers. Certain industries are particularly vulnerable because of a high reliance on computers, such as the medical and aerospace industries. For many corporations, if the computers (which are controlling various devices) are stopped, then almost all production will cease. This type of crime has become more prominent with the convergence of the computer and telecommunication industries and the widespread use of computers in many industries.

Physical Structures and Buildings: This type of crime occurs when the crime is against physical structures and buildings. In this kind of crime, traditional crime and technological crime have merged. The goal of the criminal is to stop the operations and processes done by computers, but they attack the actual buildings to achieve their goal. Attacking a computer system itself may block operations of an institution. Criminals, therefore, choose this method to commit a computer-related crime.

Sources of Computer Crime Threats

A third area of computer crime addresses the source of the threat. In this area, computer crimes fall into two groups: Insiders and Outsiders (Kovacich & Boni, 2000). Insiders are the people working for the company. They may be system administrators, system operators, application programmers, or end-users. They have the best opportunities to commit crime. Kovacich and Boni (2000) listed some of the important insiders: auditors, security personnel, marketing personnel, accountants and financial personnel, management, inventory and warehouse personnel, and human resources personnel.

Outsiders are the people outside the company. They commit the crime by using electronic bulletin boards, networks, the World Wide Web, or telecommunication media. Such people are popularly known as hackers, or crackers. They attack systems from the outside, most likely from a basic home computer.

Types of Computer Crimes

A fourth area of computer crime addresses the actual crime committed. In this area, there are several types of crimes, including: 1) Trojan horses, 2) Back Doors/Trap Doors, 3) The Salami Technique, 4) Logic Bomb, 5) Fraud, 6) Forgery, 7) Hardware/Software Theft, 8) Data Manipulation, 9) Reproduction of a Program, and 10) Telemarketing Fraud.

A Trojan horse, as its name implies, is a malicious code that initiates background processes using legitimate programs while appearing to perform valid functions (Deborah & Gangemi, 1994). This is a common mechanism for hiding viruses or worms (A virus is a code fragment that copies itself into a larger program, modifying that program. A worm is an independent program, which reproduces by copying itself in full-blown fashion from one computer to another, usually over a network (Deborah, & Gangemi, 1994)). It is almost impossible to detect the presence of a Trojan horse because it does not cause any noticeable damage.

Back Doors (also called Trap doors) are programmatic gates added to the code by the programmers to enter the system, and bypass the security measures (Kovacich & Boni, 2000). In this way, programmers can access the program or software easily and quickly. Operating systems (i.e., MS Windows, MS NT, or UNIX) are common places to hide trap doors as well as logic bombs.

The Salami Technique involves gaining assets, especially money, from numerous accounts by an automated way of accumulating tiny fractions (Kovacich & Boni, 2000). The salami technique consists of extracting tiny sums of money from a large number of bank accounts and directing the proceeds into an account owned by the fraudsman. One example is the theft of leftover fractions of pennies that result from standard bank interest calculations.

A Logic Bomb is a program that stays inactive in a system until a specific date or event occurs (Kovacich & Boni, 2000). When the specific date comes or the event occurs, logic bombs delete the files within a computer or throughout the network. Operating systems (i.e., MS Windows, MS NT, or UNIX) are common places to hide logic bombs.

Fraud is deceiving someone with the intent to obtain valuable information or goods. To be considered computer fraud, the intent usually is to steal money, data, computer time and services, or to manipulate (delete/alter) the records at a specific computer file. Computer fraud is manipulating computer data, whereas computer crime is committing a fraud by using computer (Talwar, 1999).

Forgery is when a person/group other than the actual owner claims the possession of the data. This has mainly occurred within the communication function of the computer system, such as in an e-mail account. This is often used in digital signature frauds.

Hardware/Software Theft is another increasing problem. This includes the theft of the physical parts (hardware; desktop, laptop, monitors, printers, modems, etc.) of computers or software programs. Software theft (also called software piracy) is a worldwide problem. Consequently, monetary damage due to software theft has also increased.

Data Manipulation is the alteration, or deletion of records in the data files of computer systems.

Unauthorized reproduction of a program is the reproduction of software programs (operating systems, application programs, or spreadsheets) and selling or using these unlicensed copies (Barrett, 1997).

Telemarketing Fraud is the deception of people through the use of telephone systems, and the act of persuading them to send or provide money. There are several types of telemarketing fraud, such as charity schemes, credit card/credit-repair schemes, and loan schemes, cross-border schemes, internet-related schemes, investment and business-opportunity schemes, lottery schemes, magazine-promotion schemes, and prize-promotion schemes.

Internet Crime

Internet crime is unique due to the changing nature and rapid expansion of the Internet and the number of users. The Internet is widespread, ever expanding, and mostly uncontrolled. Recent Internet crimes (i.e., the Melissa Virus, the "ILove You" Worm, and the Denial of Service attacks to several major e-commerce sites such as Yahoo, E-bay) have raised global awareness of the amount of the danger posed by Internet crime and vandalism. BBC Business Breakfast News reports that Internet crime has increased by 800% in the United Kingdom in the last 15 months alone (Cyber Crime, 2000). The most common Internet crime types are discussed below.

Denial of Service

Denial of service is stopping a system by sending enormous IP (Internet Protocol) packets (Kovacich & Boni, 2000). The system cannot answer requests because of the IP packets. Denial of service attacks are one of the most common attacks used by computer criminals. They are easy to develop, not very harmful, and easily sent. Most computer systems cannot protect themselves from such attacks. These attacks are, and may be used to spread propaganda. The attacker uses several 'innocent' computers on the Internet to send overwhelming e-mail to the targeted web site or send multiple requests to the system. As a result, the targeted system "crashes" and cannot answer its clients. The recent, and well-known attack to major e-commerce web sites (Ebay, E-trade, Amazon) in February 2000 was a denial of service attack. In April and May 1995, air traffic to Kennedy and LaGuardia airports were delayed because of the disruption of the communication between controllers caused by this type of attack (Schwartau, 1996). Denial of service attacks have the potential to shut down power and communication systems as well.

Some basic targets of a denial of service attack are: swap space of the system, bandwidth, kernel tables, RAM, disks, and caches (Husman 2000). There are several methods to protect a system from denial of service attacks. First, certain operating systems can do random checking and monitoring for these types of attacks. Second, special security software may be used. Third, a system manager may scan the ports and user operations regularly. Fourth, for outsider attacks, a firewall may be used (Firewalls are hardware or software -sometimes combination of both- that control the access to a computer system). These firewalls must be updated regularly. Finally, there are some new emerging technologies to detect denial of service attacks. For instance, the FBI's National Infrastructure Protection Center (NIPC) has announced the release of software to identify some types of denial of service attacks (Harrison, 2000).

Spam

Even though electronic mail (e-mail) is a very effective and powerful tool for communication, it has some problems such as spam or "unsolicited e-mail". Spam is defined as the delivery of excessive e-mail messages over the Internet to a person who did not want to receive them (E-mail Spamming, 1997). "Unsolicited e-mail" is defined as any e-mail message that the recipient did not ask to receive (The E-mail Abuse, 1998). Almost all spam is sent for commercial advertisement purposes.

Almost everyone who logs on to the Internet receives spam in some form. There are several sources to get e-mail addresses of people for sending spam messages. The AOL Member Technical Support web page lists several sources for getting e-mail addresses, including: running special programs on the Internet and collecting e-mail addresses from usenets, culling e-mails from service providers, csing programs to search for mailto portions of HTML documents, getting e-mail addresses from 'Internet white pages' directories, buying lists from others who already have a list, getting the address, without the knowledge of the user, while the user is visiting a web site, chat rooms and usenet groups (The E-mail Abuse, 1998).

E-mail filtering or blocking spamming addresses are common options provided by most e-mail services. Users can specify the types of e-mails or specific addresses from which they do not wish to receive e-mail. These services search the "header" information of an e-mail when a user receives a new e-mail and allows or blocks the e-mail according to pre-set parameters.

There is not a specific federal spam law in the United States. Yet, there is pending legislation called the "Unsolicited Electronic Mail Act of 2001" (Sorkin, 2001). This act would prohibit sending unsolicited commercial e-mail messages. According to the Act, Internet Service Providers (ISPs) cannot facilitate or send unsolicited commercial e-mail messages (Sorkin, 2001). At the state level, eighteen states (California, Colorado, Connecticut, Delaware, Idaho, Illinois, Iowa, Louisiana, Missouri, Nevada, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, Washington, and West Virginia) have enacted spam laws (Sorkin, 2001).

Unauthorized Access

Unauthorized access is use of computer systems by unauthorized persons, or use by insider employees for unauthorized activities (Prevent, 2000). Four types of intruders attempt to gain unauthorized access: 1) ordinary computer users who have little knowledge of computer security, 2) expert users who know security and attempt to defeat for thrill, 3) professional hackers or crackers, and 4) organization employees (Prevent, 2000).

Cyber Stalking

Cyber stalking is the use of the Internet, especially e-mail, to stalk (harass, or threaten) a person. Gaining control over victims, who are usually women, motivates cyber stalkers. In some cases, both the cyber stalker and the victim know each other, and the stalking begins after the break up of a relationship. Technology facilitates accessing a wide variety of personal information about victims through the Internet, and many people do not know this information is available. Almost all of our personal information (addresses, bills, financial processes, air fares, etc.) is relatively accessible through communication and computer databases. Cyber stalker can send threatening, or harassing messages repeatedly without fear of easy detection, and use this easily accessible information. This crime will likely increase as Internet use increases.

Internet Hoaxes, Chain Letters, and Pyramid Schemes

Internet hoaxes are e-mail messages containing untrue stories (Hoaxbusters, 2001). Hoaxes aim to set-up worldwide use and vast exposure. Hoax messages contain stories about viruses and other popular topics that make users send them to their friends. The risk and cost of hoaxes are associated with the time spent to read them. If every Internet user receives a hoax message in a week and spends one minute reading, the cost would be (300,000,000 people * 1 minute * $50.00/hr), or approximately $250 million (Hoaxbusters, 2001).

The Computer Incident Advisory Capability (CIAC), a service of the U.S. Department of Energy, breaks down hoax messages into eight categories. These categories are:

1. Malicious Code (Virus and Trojan Warnings): These types of hoax messages are so called warnings about viruses, and other malicious codes.
2. Urban Myths: Stories and warnings about untrue situations of people and animals, especially bad situations. These stories may be a story of word of mouth, and they are alleged to be true to make people pass them to others.
3. Give Aways: Untrue stories about give aways. For instance, if you send this e-mail, Microsoft will send you $100.
4. Inconsequential Warnings: Warnings about unimportant situations. These hoax messages waste time.
5. Sympathy Letters and Requests to Help Someone: Requesting assistance for somebody who is so called 'in need'.
6. Traditional Chain Letters: Letters that encourage people to send them to other people.
7. Traditional Chains: Messages that threaten people if they do not send messages.

8. Scam Chains: messages that appear to be valid but have no valid basis (Hoaxbusters, 2001).

Chain letters are e-mail messages that seem to be true, and urge people to send everyone in their address books (Hoaxbusters, 2001). By circulating messages, chain letters increase exponentially (e.g., copy this in full and send to nine friends). The difference between a chain letter and a hoax message is that a chain letter forces people to pass e-mail messages to everyone they know. A typical hoax message offers money or luck if it is passed to someone (Hoaxbusters, 2001).

Three widely seen types of chain letters are:

1. Hooks: Designed to obtain attention with their title and make receivers read the rest (e.g., Make Money Fast, Get Rich Quick, Danger, Virus Alert, and A Little Girl is Dying)
2. Threats: Based on unrealistic threat or fear urging the reader not to discontinue the chain. They may sound realistic to convince people.
3. Requests*:* E-mail messages that only want users to pass messages to as many people as possible (Hoaxbuesters, 2001).

Even though only the original sender knows the reason, people send chain letters and hoax messages for several reasons: 1) To see how long a chain continues, 2) To harass somebody, and 3) To get money from people (e.g., pyramid scheme) (Hoaxbusters, 2001).

"Pyramid" schemes concentrate mainly on the quick profits (make money fast) to be earned by recruiting other investors who, in turn will recruit others, and so on. In order for everyone to profit in a pyramid scheme, there would have to be a never-ending supply of potential participants, which is apparently impossible. These schemes exploit people who have limited knowledge of business. Many trusting investors have lost millions of dollars by investing in pyramid selling schemes. Even worse, the schemes have robbed some retired persons of their life savings. Therefore, pyramid schemes are illegal throughout the United States.

Viruses

> " A virus is a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces." (Deborah, & Gangemi, 1994).

Viruses are well-known software weapons. They can annoy the target, destroy data, infect boot-sectors, erase CMOS, or delete files on hard drives. Today, computers control telephone networks. By affecting computers, viruses may shut down telephone systems, which is a major threat to communication systems.

Worms

> "A worm is an independent program. It reproduces by copying itself in full-blown fashion from one computer to another, usually over a network. Unlike a virus, it usually doesn't modify other programs." (Deborah, & Gangemi, 1994).

Worms are used to fill up hard drives by sending itself throughout a network. Besides eating up resources they can be designed to delete data on hard drives or over a network. They are not designed to destruct systems. However, worms can crash down a system eventually by eating up all the hard drive space of a system.

Bots

Bots are programs used to “wander” the Internet and carry out specific actions. The term comes from the term “robot.” Bots can be used for either useful or harmful reasons. Bots are very useful to gather information from the Internet, but they may be damaging and malicious when they are used to delete information or messages in newsgroups.

Child Pornography

Child pornography is defined as picturing children in a sexual manner (Caeti, 2001). Another definition is: child pornography or the “Internet crime against children” is defined as sexual exploitation of children by using computers (Office of Juvenile, 1999). As with other types of crimes, computers facilitated child pornography, especially the Internet. Child pornography is becoming a serious issue on the Internet. There are numerous websites that contain child pornography (Caeti, 2001). Almost one third (32.3%) of ‘online people’ visited pornography related websites (Aldrich, 2000). Seventy percent of workers receive pornography related e-mails at work (Cox, 1999).

Prior to the advent of the Internet, several hours of work were needed to develop and disseminate pornographic pictures. However, it takes relatively very short time to prepare and distribute pornographic pictures by using computers and the Internet. Today, even a personal computer can store hundreds of thousands of images. Besides, with the Internet it is very easy to download and upload (receive and distribute) pornographic pictures. This situation exacerbates the situation for law enforcement and judicial officials (Caeti, 2001).

Cyber Terrorism

Along with the changes in information technology, the face of terrorism has changed. Unfriendly nations, and terrorist groups are becoming more and more involved in cyberspace by focusing on the vulnerabilities of technology to attack their adversaries. While primary motivations for terrorism have remained the same, terrorist acts have evolved through the use of technology. There are numerous definitions of terrorism. One widely used definition is: “Terrorism is the illegitimate use of force to achieve a political objective by targeting innocent people” (Laquer, 1987).

Cyber Terrorism is defined as: “the illegitimate use of force to achieve a political objective by targeting innocent people through the exploitation of computerized systems deployed by the target”(Collin, 1998). Another definition is: “the premeditated, politically motivated attack against information, computer systems, computer programs, and data that will result in violence against noncombatant targets by sub national groups or clandestine agents”(Pollitt, no date).

There are differences between cyber terrorist attacks and computer hacking. Cyber terrorist attacks are not done simply for curiosity or vandalism, rather they are executed with the goal of terrorism, extortion, espionage, and harmful disruption. Cyber terrorism is also being used to seek financial support and spread propaganda and information.

Methods and Techniques of Cyber Terrorists

There are several methods and techniques that cyber terrorists use. First, chipping is performing specific functions through the use of computer chips. With the advanced chip technology that exists today, it is very easy to modify some activities at a hardware level by using integrated circuit boards. An integrated circuit is the building block of many home appliances, toys, televisions, cameras, and computers. The Central Processing Unit (CPU) is the chip that functions as the "brain" of the computer. Computer chips may be used to perform specific tasks to send signals to show their location, or to send information about the system in which they operate. They may be designed to cease operation after receiving a specific frequency signal at a predetermined date. Another common chipping technique is to alter existing hardware. For instance, modification of cards used to acquire satellite television can be altered so that free service is provided.

Another terrorist tactic is SYN attacks, which is sending numerous connection requests to the target to create traffic or data jams. As a result, users may not be able to access the site. Terrorists also use nano machines and microbes, which are very small 'robots' designed to enter the physical computer system, through the holes (i.e., slots), to damage the hardware of the system. Microbes, specifically, can destroy all the hardware in a computer lab, a building, or even in a town. They are very sophisticated and harmful.

Terrorists can also make use of High Energy Radio Frequency (HERF) Guns and Electromagnetic Pulse (EP) Bombs. HERF guns are designed to shut down an electronic target (i.e., electronic circuits, computer systems, networks, cars using electronic systems, and planes, etc.) by sending a high-energy radio signal. Indeed, HERF guns are a type of radio transmitter. Electronic circuits are very sensitive to interference from external transmissions. In fact, they are more vulnerable than most people think. HERF guns are used to exploit the vulnerability of electronic circuits.

Electromagnetic Pulse (EP) bombs are designed to shut down the electronics of computer systems. Their damage is more extensive than that of HERF guns; moreover, they damage a larger area than HERF guns. Their primary purpose is to shut down devices near an electronic device, such as electronic bomb. With appropriate strength, the electromagnetic pulse may erase hard disks, floppy disks, and tapes. These devices are used as a weapon in that they may technologically incapacitate an enemy.

Other examples of new technological weapons include Transient Electromagnetic Devices (TEDs) and Transient Electromagnetic Pulse Standard (TEMPEST) Monitoring Devices. TEDs transmit a broad band of frequency to targeted systems. They do not send a single frequency transmission like the narrow band radio frequency (RF) weapons send. TEDs are simple and inexpensive to design, and they may instantaneously attack multiple targets. Moreover, they are virtually undetectable. It is the standard by which the government measures electromagnetic computer emissions and details what is safe (allowed to leak) from monitoring. The standards are detailed in NACSIM 5100A, a document that has been classified by the National Security Agency. Devices that conform to this standard are called TEMPEST certified devices. TEMPEST monitoring devices are designed to use electromagnetic radiation coming from a target to obtain information from that target. TEMPEST monitoring is passive; therefore, it is difficult to detect. They are specifically used to display the screen of the computer monitor, and contents of the memory and hard drives. Since computer monitors transmit a beam of electrons, they are vulnerable to TEMPEST monitoring equipment. Potential users of TEMPEST monitoring devices are: intelligence services, business competitors, disgruntled employees, and terrorists.

Cyber Sabotage and Information Warfare

Cyber sabotage is a physical attack against a computer system. It is common method, and it is easily executed. It may involve the use of fire or explosives, and insiders or outsiders may perform the task. Therefore, business competitors as well as foreign intelligence agencies may use this method. Like other new and emerging technologies, there is a problem with defining Information Warfare (IW). The term has a military aspect, as it is used to describe 'war' on the Internet.

Dorothy Denning (1998) uses the term IW to cover a wide range of activity, including corporate and military espionage and intelligence collection, psychological operations and perception management, attacks on communication systems, consumer fraud, and information piracy. In addition, the concept covers specifically computer-related issues: viruses, Trojan horses, and deliberate and targeted hacking efforts such as computer break-ins and denial-of-service attacks.

No single definition can completely define IW so scholars have developed taxonomies to define it. Schwartau (1996) explains that there are three classes of IW; 1) Personal IW; 2) Corporate IW, and 3) Global IW. According to Schwartau, Personal IW studies information about individuals; Corporate IW studies information as it affects business, commercial, or economic interests; and Global Information Warfare studies information that affects the interest of countries or nations.

Illustrative Cases

The following cases provide an illustration of the common types of computer crime observed today.

Case 1: Hacker Eric Burns a 19-year-old known on the Internet as “Zkylon,” electronically assaulted the U.S. Information Agency, two businesses, and the White House Internet site in the early spring of 1999. He altered the web site of the White House to a black web page with the names of hacker organizations, and included messages like, “Your box was owned,” and “Stop all the war.” After the attack on the White House Internet site, he attacked the web sites of NATO, a U.S. embassy and consulate, and the Vice President at the time Al Gore. Prosecutors argued that the attacks cost businesses and the government more than $40,000.00. After an investigation, FBI agents located Burns, made a surprise raid on his home, and confiscated his computer. He was sentenced to 15 months in prison and was fined $36,240.00 (Hacker, 1996).

Case 2: David Smith created and disseminated the Melissa virus through the Internet in March of 1999. The virus spread abruptly throughout worldwide computer systems, in the United States and Europe. It is estimated that the virus spread to 1.2 million computers located in one-fifth of the largest businesses in the world. The total cost of the damages caused by the virus is estimated at $80 million. Smith was arrested and prosecuted in New Jersey on December 9, 1999, in accordance with State and Federal laws (Computer, 2000).

Case 3: Timothy Lloyd, a 30-year-old programmer, was employed by the Omega Engineering Corporation headquartered in New Jersey. The company manufactures instruments used by NASA and the U.S. Navy. Lloyd was a chief network programmer before he was fired on July 20, 1996. Ten days after he was fired, he activated a "bomb" that deleted all of the company's software and designs. The loss to the company was reported to be at least $10 million. Lloyd faced a maximum of 15 years in prison and fines ranging from $500,000 to $1,000,000. It is estimated that this was the most expensive cyber sabotage in history (U.S. Programmer, 2000).

Case 4: On February 10, 2000, hackers attacked Yahoo, the popular website and search engine. Yahoo's repair engineers realized that they were under a "Denial of Service" attack caused by millions of meaningless digital 'packets' requesting page views. Yahoo was out of service for three hours. This was the first of several attacks on popular web sites. The second attack was on the e-commerce site named "buy.com." Following that attack, the auction web site "Ebay" was incapacitated for four hours. The next victim was "CNN.com." Less than 5 percent of its users could reach the site for about one hour. Other victims were "Amazon.com," "Zdnet.com," "Datek online," and "excite.com" (Sandberg, 2000). After these crippling attacks, the FBI began to investigate the incident. In the aftermath, concern about the security of the Internet caused a stock sell-off many Internet equities. As a direct result of these attacks, several Presidential Commissions were established. About 20 days after the attack, the FBI found one of the three hackers, Dennis F. Moran. He used the screen name “Coolio,” and was a 17-year-old boy. He was a high school dropout with no job. While Moran was telling the Associated Press in an Internet chat room that he was one of the three hackers who attacked the major e-commerce sites, the FBI found him. He did not know that the FBI was monitoring the chat room. FBI agents interviewed him at his home, and he told the FBI that he had been using computers since he was three years old, and each day spent 16 hours on the Internet. Moran received a 15-year sentence and a $4,000 fine (Teen, 2000).

Statistics

One of the biggest challenges of the computer crime problem is that there are no national statistics on the incidence of computer crime. There are several reasons for the scarcity of computer crime statistics. Primarily, it is a very new and emerging problem. Most people are not aware of what computer crime is, and how to handle it. Indeed, even law enforcement agencies have only recently begun to learn about computer crime, how to detect and investigate it, and how to prosecute it. According to the Computer Crime and Security Survey conducted in 1999, by the Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad, organizations did not report computer crime incidents to law enforcement mainly for four interesting reasons (Power, 1999).

First, 32.68% of the respondents did not report intrusions because of the negative publicity. Second, 30.73% of the respondents did not report intrusions because of the idea that competitors would use this to their advantage. Third, 14.00% of the respondents did not report intrusions because they were unaware that it should have been reported. Finally, 22.56% of the respondents did not report intrusions because civil remedy seemed to be the best course of action (Power, 1999).

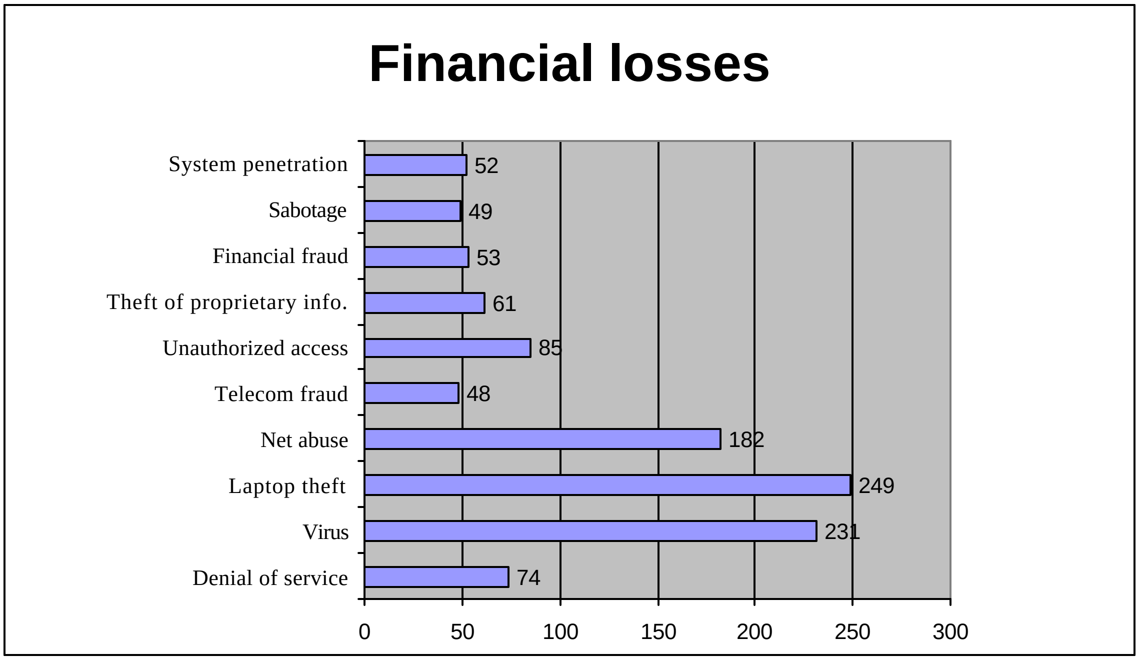
The 1999 CSI/FBI Survey is the fourth of the continuing annual surveys. In 1999, the statistics were based on responses from a much large audience: 521 organizations, such as government agencies, financial institutions, and universities. There are numerous remarkable results of this survey. For example, contrary to popular belief, outsider system penetration accounts for 43% of computer crime incidents, and unauthorized insider access accounts for 37% of these incidents (Power, 1999). In addition, attacks occur from the Internet 41.91% of the time, from internally 37.5% of the time, and from remote dial-ins 20.58% of the time (Power, 1999).

According to the 1999 CSI/FBI Survey (from Figure 2.1.):

- 521 organizations as a total experienced 249 laptop theft incidents.
- The second most happened incident type is virus, and the number was 231.
- 182 net abuse incidents were recorded by these 521 organizations.
- The other recorded incidents were respectively unauthorized access, denial of service, theft of proprietary, financial fraud, system penetration, sabotage, and telecom fraud.

Figure 2.1.

Financial losses



Source: Modified from 1999 CSI/FBI Computer Crime and Security Survey

According to the National Consumer's League's Internet Fraud Watch, the top ten fraudulent activities on the Internet are:

1. Auctions (87%): Bid items are not delivered; prices are increased after the bids are accepted, or value of items is inflated.
2. General Merchandise (7%): Items (everything from T-shirts to VCRs) bought on the Internet are not delivered, or when delivered, they are not the item ordered.
3. Internet Access Services (2%): Internet services are not provided to paying customers.
4. Computer equipment/Software (1.3%): Computer products are not delivered, or when delivered, they are not what were ordered.

5. Work-at-home (.9%): Books and materials are sold and, promise specific services, but the service is never presented/received.
6. Advance Fee Loans (.2%): Promises of loans contingent on a large initial fee. After the initial fee is paid, the loans are never given.
7. Magazines (.2%): Magazines are advertised on the Internet. They are not shipped even when the subscription was paid.
8. Adult services (.2%): Adult service web pages charge more than supposed to or don't provide the service offered.
9. Travel/Vacations (.1%): Airline tickets are sold, but the purchaser receives a different package or nothing at all.
10. Pyramids/Multilevel Marketing (.1%): Traditional pyramid schemes advertised on the Internet (National, 1999).

According to the U.S. Department of Justice, there was a 498% increase in the number of computer intrusions, and a 702% increase in the number of sites attacked between 1991 and 1994 (Cain et al., 1999). However, statistics on computer crime are all based on reported or estimated situations, because detection of these crimes may be extremely difficult. Unfortunately, it is estimated that total loss caused by computer-related crimes is between $500 million to $10 billion.

Profiles and Motives of Computer Criminals and Hackers

The issue of computer crime often renders classical criminological theories useless. Society has now encountered new kinds of crime, (such as computer crime), and criminologists realize that these kinds of crime are committed, in large part, by non-poor, educated, young, technically competent, and mentally fit individuals. It is difficult to portray the computer criminal exactly, but there is a widely accepted profile of the computer criminal. According to Taylor (2000) the typical computer criminal is seen in Table 2.1.

Table 2. 1.

Profile of the Typical Computer Criminal

Age	14-25 years old
Sex	Usually white male, but the number of women are increasing
Socioeconomic Status	Medium to high
Personal Traits	Bright, motivated, and ready to accept the technical challenges (highly intelligent), but they're not successful in school
Fears	Concerned with exposure, ridicule, and loss of status within the community.
Behavior	Boredom and apathy are their main feelings.
Justification	They are in a "thrill-seeking" subculture (their nicknames shows their feelings).

Source: Modified from Taylor (2000), "Computer Crime."

Even if the profile does not apply to all computer criminals, many cases show this type of person as the perpetrator. The motives of computer criminal vary. According to a survey done by Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) in 1997, the motives of the computer criminal are shown in Table 2.2 (Power, 1997).

Table 2.2.

Motives of Computer Criminals by industry, and the number of companies citing each motivation

Motivation	Identified by industry	# Citing motivation
Curiosity	Transport	33
	Banking and finance	29
	Communications/technology/computing	28
	Government	27
	Manufacturing	23
	Insurance	17
	Primary/mining	8
	Retail	7
Espionage	Communications	50
	Government	36
	Banking and finance	26
	Retail	7
	Manufacturing	6
Financial gain	Transport	22
	Government	9
	Retail	7
	Manufacturing	6
Extortion/terrorism	Banking and finance	14
	Manufacturing	9
	Communications/technology/computing	5
Malicious damage	Communications	25

Source: Modified from 1997 CSI/FBI Computer Crime and Security Survey

Hackers or Crackers

The original hacker culture was seemingly harmless, because they believed that all information should be free, shared, and uncensored. These original hackers are called crackers. Crackers support the idea that information should be free, and everybody should have access to any type of information. They do not accept limitations and restrictions so that they attempt to crack those limitations. Their ideology is based on “thrill-seeking” subculture (Taylor, 2000). However, this ideology has changed over time into the public image of “typical hacker.” After becoming popular in the news media, hackers are believed to attack for financial gain, instead of ‘just for fun.’

Hackers exploit the vulnerabilities of operating systems, application programs, and computer systems. Most hackers do not seek new vulnerabilities. Rather, they use the techniques they learned from the original hackers. These hacker geniuses (there are probably less than 200 of these individuals) find new weak areas and inform other hackers by posting the weaknesses on the Internet. According to these criteria, the estimated number of hackers (both expert and amateur) is between 35,000 and 50,000 (Winkler, 1997). The popularity of the hacker culture is supported by the news media, web sites, movies, even books. Children who are faced with these types of encouraging information may aspire to join the hacker culture. The most important issue here is that hackers use the weaknesses of computers, computer systems, and software to their advantage. They are able to do these things because of a lack of effective security systems and measures.

Theoretical Explanations of Computer Crime

In explaining computer criminal behavior, there are two main theoretical approaches: social learning theory and routine activities theory. Most computer crime studies have been conducted on the victims (Skinner & Fream, 1997). However, there are a few studies on the perpetrator. A study by Skinner & Fream (1997) examined the relationship between social learning theory and computer crime perpetrators. In a related example, Hollinger (1992) is one of the first criminologists to examine computer crime among college students. These two studies found some explanation to computer crime by using social learning theory.

First, social learning theory claims to be a general theory, which applies to a variety of deviant behaviors (Akers, 1985). Social learning theory has four major elements: differential association, differential reinforcement/punishment, definitions, and imitations (Akers, 1985). In brief, social learning theory argues that criminal behavior is learned interaction with others; indeed, it is learned through the above four factors (Akers, 1985).

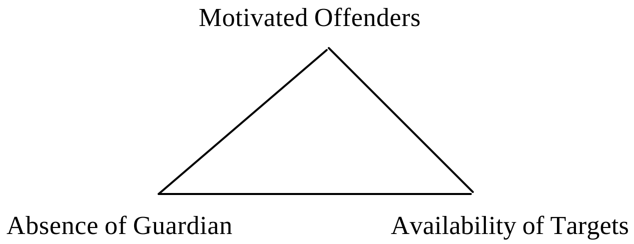
The second major theoretical basis for explaining computer crime is "routine activities theory." The routine activities theory is a criminological theory, and is proposed by Cohen and Felson (1979). Cohen and Felson (1979) explained the theory as follows:

> "The routine activities approach is based on two rather simple ideas. First, it argues that in order for a crime to occur, motivated offenders must converge with suitable targets in the absence of capable guardians. Second, it argues that the probability of this occurring is influenced by our "routine activities"-including our work, family, leisure, and consumption activities."

Figure 2.2. summarizes the “routine activities” approach. These three elements are parts of the triangle of crime.

Figure 2.2.

The “Triangle of Crime” (Cohen & Felson, 1979)



Source: Adapted from information by Cohen and Felson (1979)

The availability of suitable targets is the first factor of this approach. The technological advances produce more organizations that are dependent on computer technology, more people who have access to computers and the Internet, and more computer literate individuals (Adamski, 1998). All of these factors, in turn, increase the number of suitable targets.

The presence of motivated offenders is the second element of the routine activities approach. With the increasing popularity of computer technology and hackers, more and more people have entered the hacker subculture. The exact number of hackers is unknown (Adamski, 1998). A recent study stated that the Internet is an effective way for dissemination of criminal techniques, which facilitates hackers’ computer crime commitment (Mann and Sutton, 1998). Consequently, the Internet provides an opportunity where hacking behavior can be learned through interaction with others. Eventually, this opportunity augments the number of motivated offenders.

The third and final factor is the absence of capable guardians. Law enforcement has not kept up with technological developments. According to the Federal Bureau of Investigation’s (FBI) National Computer Crime Squad (NCCS), between 85 and 97 percent of computer intrusions are not detected (Adamski, 1998). This statistic clearly shows the current situation of law enforcement, and gives us an understanding about the magnitude of the problem.

Conclusion

This chapter provided an explanation about the nature of computer-related crime. Computer-related crime was discussed in three main parts: computer crime, Internet crime, and cyber terrorism. Computer crime is defined as crime committed by the use of computers; Internet crime is defined as crimes involved the Internet; and cyber terrorism is defined as committing computer crime within the goal of terrorism. Illustratives are discussed to give an idea about the extent of the problem. Next, statistics, and profiles of computer criminals were examined. Theoretical explanations of computer crime concluded this chapter.

Prior literature presents several computer crime categories. This study discussed four areas, and focused on a widely accepted category. This widely accepted category classifies computer crimes in term of the role that computers play. Prior research finds a relation between computer crime and social learning theories. In addition, there are some studies on the application of routine activities approach to computer crime. This research finds some explanation to computer crime by these two theories (social learning and routine activities theory). Further, prior research lacks of statistics about computer crime. Scarcity of reliable and accurate statistics undermines the importance of the problem. According to the literature, another important issue is cyber terrorism and information warfare. Advances in the computer and electronics industries give various opportunities to criminals.

Next chapter discusses law enforcement responses to computer crime. What law enforcement agencies must do, computer crime laws, international aspects and jurisdiction issues, detection and investigation of computer crime are the subsections of the next chapter.

CHAPTER 3

LAW ENFORCEMENT RESPONSE TO COMPUTER CRIME

Introduction

"The FBI needs worldwide cooperation among law enforcement agencies to catch bandits in cyberspace – a new frontier where international borders don't exist," said FBI Director Louis J. Freeh (Milton, 1997). This new challenge is similar to the challenges of other crimes, but because criminals are using computers to achieve their goals, law enforcement needs to "play the catch-up game" again (Milton, 1997).

This new issue confronting police is somewhat unusual in nature. Moreover, several factors make the problem difficult to address and exacerbate the situation. Outdated laws and jurisdictional and statutory limitations block law enforcement. Computer crimes do not have traditional geographic boundaries, so the police need to investigate outside of their jurisdictions. However, current regulations usually do not allow this type of cross-jurisdictional investigation. Further, law enforcement personnel are not aware of the importance of the problem. Lack of awareness results in lack of attention. Adding to the problem, law enforcement agencies do not have enough computer-literate investigators. As Internet use continues to increase, the total number of computer crime incidents is also increasing exponentially. As a result, law enforcement caseloads are growing. "The number of cyber crime cases that FBI opened increased from 547 in 1998, to 1154 in 1999," said Louis J. Freeh (Freeh, 2000). Accordingly, the need to hire and train new personnel increases proportionally. In addition, lack of adequate training diminishes the investigative capacity of police agencies. As might be expected, a person's computer knowledge often becomes outmoded because information technology changes so quickly. Therefore, training must be updated and provided regularly. Anonymity is also a noteworthy problem. Time and space dimensions of computer crime incidents are vague, and there may be no witnesses, emphasizing once again, computer crime is not like traditional violations. Another considerable problem is funding. The public does not see computer crime as a serious issue, and this reduces the likelihood of adequate funding. Funding sources must understand the nature and extent of computer crime and its consequences.

In order to protect society, and in spite of these limitations, law enforcement personnel must learn how to investigate and prevent computer crime. Moreover, cooperation with the private sector must be sought. Businesses are often the targets of computer-related crime. A relationship between police and businesses will have a positive impact on confronting this new challenge. It is also beneficial to the police if private sector businesses apply their vast expertise to this problem.

In this chapter, the law enforcement response to computer crime is discussed. Then, the need to equip police personnel with proper training, equipment, and tools for these types of crimes is presented. Laws regarding this subject and prosecution issues are examined. International and jurisdictional issues are explained, and finally, investigating computer crime is discussed.

What Should Law Enforcement Agencies Do?

As studies have shown, law enforcement is not prepared for this new technological challenge. Indeed, the gap between police and computer criminals is widening every day. Further, most police administrators fail to recognize the seriousness of computer crime. Special Agent Guadalupe Gonzalez of the Federal Bureau of Investigation (FBI) expressed two main roles of the police in combating computer crime in his/her testimony to Congress. The two roles are:

> Preventing cyber attacks before they occur or limiting their scope by disseminating warnings and advisories about threats so that potential victims can protect themselves; and responding to attacks that do occur by investigating and identifying the perpetrators. (Gonzalez, 2000)

These responsibilities can be carried out in the following ways: Distribute the information to the public via news media, sharing information and building partnerships with industry and academia, and warning every possible victim by using threat assessments. The public is informed, primarily, through the news media. Most possible cyber victims or criminals read newspapers or watch television every day. The media provides a vehicle for law enforcement to send warnings to victims and criminals alike. Informing them about laws and the detection capabilities of law enforcement may prevent criminal acts. Similarly, potential victims may shield themselves from attack if they are made aware of their vulnerability. According to the 2000 Computer Crime and Security Survey, 32% of the respondents reported they did not know if there had been unauthorized access or misuse of their computer systems within the last 12 months (Power, 2000). Determining the security measures taken by businesses is not the role of police. Nevertheless, the police can encourage the private sector to revise or develop security measures, and this is an urgent need of many businesses.

A partnership with the private sector is critically important for the police. This liaison provides information sharing between the two parties. Police have not given much attention to this partnership. However, this cooperation is greatly needed. Gonzalez presented three reasons in support of this partnership. First, private sector businesses are the main victims of computer crime. Second, the police need the help of companies or Internet Service Providers (ISPs) for detection and investigation of cyber crime. Finally, the technical capabilities and expertise of the private sector are much more advanced than that of the police.

Police can also provide crucial information to potential cyber victims by making threat assessments. Some larger companies may not need security threat assessments, but there are still some companies or governmental agencies that need the help of the police. Police must provide information about cyber intrusions, physical infrastructure threats, and vulnerabilities to these businesses.

The second role of the police can be done in three ways. As previously mentioned, computer training for personnel may have a significant impact on investigation and detection. Training issues are discussed in the next section. The recruitment of new personnel who have computer expertise is another factor in computer crime detection and for successful investigations. Finally, law enforcement agencies must build investigative and technical capacity through the acquisition of proper equipment.

Equipping Law Enforcement

Equipping law enforcement for the investigation of computer crime is comprised of four stages: providing adequate training, providing proper equipment, allocating resources, and supplying well-defined personnel policies.

Training

Public familiarity of computer technology is increasing. As a direct result of this, there is an increasing need for computer technology and expertise in police agencies. In order to enforce law and protect society adequately, agencies must be more advanced than the general public. Training among police is seen as the best answer to this problem.

Every police officer should receive computer training since most organizational operations rely on computers. Nonetheless, computer training is much more valuable and important for computer crime investigators. Investigators must acquire an expert understanding of computers, computer networks, different software packages, databases, electronic transmission, etc. If a police agency has a computer forensic laboratory, it is vital that the agency have trained computer forensic analyst(s).

Steele and Pearson (1981) proposed three levels of training for law enforcement investigators: awareness level, comprehensive level, and specialized level. The awareness level addresses the investigation of more simple or less-sophisticated misuse of computer technology. The comprehensive level addresses the investigation of the modification of programs and auxiliary storage devices. The specialist level, which is the most advanced level in the curriculum, attempts to develop an investigation model for the most complex incidents such as modification of operating systems (Steele & Pearson, 1981). Overall, these training categories aim to assist law enforcement investigators, and the authors claim that those provided with level two training can effectively investigate 93 percent of reported computer crime incidents.

The FBI's computer crime investigator courses have a similar structure. The FBI offers two courses (the basic computer skill course and the advanced investigative course) to investigators and agents at their Academy in Quantico, Virginia. The first course focuses on basic computer skills. In this course, the students become familiar with various computer software, hardware, databases, and operating systems. The second course focuses on advanced investigative techniques. With this course, students learn how to investigate complex computer crime incidents (Sessions, 1991).

These two courses show the general structure of computer crime training courses. In the United States Manual on the Prevention and Control of Computer-Related Crime, it is proposed that an appropriate training program should cover the following five areas: technology, how to obtain and conserve computer evidence, the differences between criminal and civil laws, international issues and jurisdiction problems, and the rights and privileges of the victim and the accused (United Nations, 2000).

The World Wide Web can be utilized for the training of investigative personnel. There are a few web sites offering a collection of information for law enforcement investigators. Some of these web sites even provide online courses to law enforcement personnel and provide certificates upon successful completion. For instance, www.cybercrime.org, www.cops.org, and www.nctp.org are a few of the many web site resources.

Finally, law enforcement can use the help of dedicated training organizations, such as the National White Collar Crime Center (NW3C) or the National Cybercrime Training Partnership (NCTP), headquartered in Fairmont, West Virginia. These entities train law enforcement personnel. Their primary mission is to train computer crime investigators and prosecutors at local police levels.

Equipment

Investigative personnel must be supplied with supportive tools. Without proper equipment and supportive tools, it would be difficult to perform good investigations. For instance, the FBI supports its investigators with CASIAT (Computer Assisted Security Investigative Analysis Tool) - the FBI's investigation tool (Sessions, 1991). The CAISAT is a group of experts that assist investigators in analyzing computer crime incidents and developing profiles of computer criminals. The CASIAT experts also work on viruses and malicious software. Moreover, the CASIAT experts are studying the methods that computer criminals are using for committing computer crime.

Investigators should also be supplied with manuals and computer science publications. As computer science is a very dynamic discipline, computer technology changes rapidly. For example, every month many new hardware and software products emerge and spread among computer users. Keeping up with these advances requires dynamic training.

Funding

Despite the advantages of training and updating printed resources, there are some other important issues as well. Training personnel and supplying them with continuously updated manuals and other publications may lead to budget shortages. Not all agencies will have access to the needed funds. However, with good planning and by redirecting some resources, agencies may be able to overcome these problems. But the awareness issue still remains that computer-related crime is not viewed as important as traditional crimes in most agencies. If law enforcement agencies examine the total cost of traditional crimes to the public, computer crime would probably be considered the highest priority. Criminal justice administrators must consider these issues in detail. Donations may be a source to acquire some of the necessary funding and equipment. Grants may also be used to eliminate the funding problem.

Personnel

Another problem confronting law enforcement agencies is the turnover of personnel. Personnel management policies may require officers to change departments at regular intervals. On the other hand, it will result in a crisis situation when departments lose their specialized investigative personnel. After spending money, time, and other resources to train investigators, it is not wise to send them "back to patrol." Hiring technical persons from outside of the department to perform investigations may solve the problem to some extent. Employee retention is also an issue confronting police. The salaries of many law enforcement personnel are often not sufficient to encourage personnel to remain with their respective agencies. The amount of money paid in the private sector may be much more attractive than the salaries available in law enforcement. The problem requires some criminal justice administrators who can think “outside the box” and dedicate themselves to control and prevent computer crime.

Computer Crime Laws

Beginning with Edwin H. Sutherland’s studies in the 1930s, criminologists became interested in the study of white-collar crime. Further, the news media brought the issue to the public. Similar to police personnel, legislators have not been adequately concerned about computer crime. In spite of recent legislative efforts to address computer-related crime, the development of computer laws has fallen behind the development of new and increasingly complex computer technology. In order to enact computer crime laws, legislators must be educated and proactive. There is a debate about the strength of the government regulations and laws on computer crime. Individuals think that their privacy is invaded with these laws. On the other hand, the government wants more controls on individuals’ actions.

If one looks at the development of computer crime laws, it is apparent that First and Fourth Amendment considerations are the most important aspects of guiding the police in these types of investigations. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 is perhaps the first federal computer crime law. In 1986, Congress expanded the scope of the computer crime law and passed the Computer Fraud and Abuse Act of 1986. The Computer Fraud and Abuse Act of 1986 was revised in

1988, 1989, and 1990. Finally, the National Information Infrastructure Protection Act of 1996 (NIIPA) was passed. Also of note, the federal government uses a special code for child pornography. In the next section, these laws will be discussed. In addition to these federal laws, all states except Vermont (which has now) have computer crime laws (Goodman, 1997).

Computer Fraud and Abuse Act

In 1984, President Reagan signed the first computer crime law, the Computer Fraud and Abuse Act of 1984. This statute is contained in Section 1030 of Title 18 of the United State Code (18 U.S.C. ξ 1030). The main purpose of the 1984 Act was to prohibit unauthorized access into any "protected computers," which are computers used by government and financial institutions (Rosenberg, 1997). The 1986 Act prohibits six types of computer abuse:

- Knowingly accessing a computer without authorization and obtaining restricted information with the intent to use that information to the detriment of the United States.
- Intentionally accessing a computer without authorization and obtaining information in the financial record of a financial institution.
- Intentionally, without authorization to access any computer of a department or agency of the United States, access[ing] such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer.
- Knowingly, and with intent to defraud, accessing a Federal interest computer and obtaining something of value, unless the value so obtained is limited to the use of computer time.
- Intentionally accessing a Federal interest computer without authorization, and by means of one or more instances of such conduct altering, damaging, or destroying information in any such Federal interest computer, or preventing

authorized use of any such computer or information and thereby causing damage in excess of $1,000 or damaging records.
- Knowingly, and with intent to defraud, trafficking in computer passwords (Rosenberg, 1997).

There were some limitations to the Act. The explanation of computer crime and the words used to depict them hampered the prosecution of some crimes. For instance, the wording "protected computers" includes governmental computers, but excludes personal computers and computers used by corporations. Another limitation of the Act was that unauthorized access was not defined as a crime. Considering that the Act emphasizes the value of information, it is interesting that access issues were not addressed in the Act. The Act also did not mention computer viruses.

In 1996, Congress updated existing law, and this became known as the National Information Infrastructure Protection Act of 1996 (NIIPA) (Hatcher, McDannell, & Ostfeld, 1999). The 1996 NIIPA Act addressed many of the issues the previous Acts failed to cover. One of the most important changes was replacing the phrase "protected computers" with "federal interest computers" (Hatcher, McDannell, & Ostfeld, 1999). With the "protected computers" phrase, only crime against governmental computers could be prosecuted. Additionally, the NIIPA addressed computer hacking (Hatcher, McDannell, & Ostfeld, 1999). The 1994 Act did not include computer hacking, which was an increasing crime type, and caused problems in prosecution under the 1994 Act. Also, wording problems of the prior Acts were clarified. "Defenses based on intent" and "implied authorization" were two important wording changes (Hatcher, McDannell, & Ostfeld, 1999).

Child Pornography Prevention Act of 1996

The Child Pornography Prevention Act of 1996 (CPPA) attempts to prevent the transmission of computer-generated pornographic images of children (Hatcher, McDannell, & Ostfeld, 1999). This statute is contained in Section 2252 of Title 18 of the United State Code (18 U.S.C. ξ 2252). The criminalization of the possession of and the distribution of images are currently among the biggest disputes in the courts (Hatcher, McDannell, & Ostfeld, 1999). Some argue that government should not regulate only possession of obscene material (Taylor, 2000). Preventing possession of such material is thought to be some form of privacy invasion.

Privacy Issues and Electronic Communications Privacy Act

Privacy issues in cyberspace have raised special problems. There are several statutes that cover privacy rights. The Electronic Communications Privacy Act (ECPA) is one of the statutes that deal with privacy issues extensively. Enacted in 1986, the ECPA prohibited the interception of electronic transmissions (Hatcher, McDannell, & Ostfeld, 1999). The Act also criminalized accessing a system without authorization (Hatcher, McDannell, & Ostfeld, 1999). Moreover, according to the ECPA, it is a federal offense to access and read electronic mail that is not one's own. The ECPA was reviewed in 1996, and Congress passed it as the Communications Decency Act of 1996 (CDA). The CDA prohibits the transmission of "indecent" telecommunications.

The ECPA provides a remedy for damages caused by the interception of communication (Aldrich, 2000). For instance, the U.S. Supreme Court decided that the

Secret Service agents violated privacy rights in the Steve Jackson Games vs. Secret Service case (Aldrich, 2000). The Secret Service was sentenced of $51,040 fine. Steve Jackson Games was a publishing company in Austin, Texas, raided by the Secret Service agents in 1990 (Shap, 1993). The Secret Service seized company's computer system as a whole even if only one employee was suspected to be involved in an illegal activity (Shap, 1993).

International Aspects and Jurisdictional Issues

International Aspects

With the growth in the use of computer networks and the Internet, international aspects of computer crime have received the attention of officials. Computer crime has recently been seen as a global problem. The global nature of computer crime makes domestic solutions inadequate. The identities of perpetrators are often initially unknown, and the space and time dimensions of the intrusions may be unclear. Computer systems can be accessed or destroyed from anywhere and by anyone in the world. This results in complex jurisdictional issues. These issues require immediate solutions in the international arena. In other words, global issues require global strategies.

The economic systems of nations are often heavily dependent on computers. International access to information is an unavoidable fact of current economic systems. In considering the international aspects and complex nature of the computer crime problem, it is vital to develop international cooperation and coordination. To bypass the weaknesses of computer crime laws and the rules of evidence in many countries, a global framework to address all types of computer crime must be developed. This transnational framework must provide new penalties and codes to apply to computer crime cases without causing any difficulties, misunderstandings, or breaches of individual human or democratic rights. In addition, international organizations and private institutions should assist governments in harmonizing their laws. As an example, the Business Software Alliance is one organization that enforces international copyright laws.

If a governmental body is not prepared for computer crime, it is important for others to assist them. Further, if a country does not have any computer crime laws or existing laws do not adequately address the problem, other, more prepared nations should present their experience to this country to assist them in developing adequate laws. Similarly, within the nation, organizations and agencies must assist one another in developing a collective and cohesive framework.

The United Nations Manual proposes eleven advantages of having common definitions and harmonization among laws. These advantages are:

- Without common understanding there will be no international cooperation
- Increasing dependency of society on computers, and the increasing concern for privacy require international laws
- International harmony can provide the stability of the international market while thwarting possible perpetrators with international laws
- Harmonization can facilitate the development of international standards of computer usage and conduct
- Harmonization can prevent the free flow of illegally obtained information

- Harmonization can encourage competition.
- Harmonization can inhibit some countries from harboring offenders
- Harmonization can facilitate the extradition of offenders
- Harmonization can facilitate mutual assistance between countries
- Harmonization of offenses may lead to common procedural laws (United Nations, 2000).

Nevertheless, the issue brings to the international arena, including governments, law enforcement agencies, and private industry, a number of problems. For instance, there is currently very little harmony between nations' computer crime laws. Only a few countries, the United States, Austria, France, Greece, Denmark, Germany, Italy, Finland, Turkey, Australia, Sweden, Canada, Switzerland, and Japan, have adequate laws to address the problem (Rai, Duabsh, & Chaknavarti, no date). There are also problems with locating and identifying perpetrators across borders. International organizations, such as Interpol, have had difficulties with these issues (Security, 1996).

Currently, there is no international consensus on the regulation of encryption (the transformation of original text (called plaintext) into unintelligible text (called ciphertext) (Icove et al., 1995)), which is another aspect of cooperation. The encryption debate is occurring between businesses, citizens, and law enforcement officials, and each side wants control of the regulation of data encryption. Businesses are concerned with the security of their commercial transactions, citizens are interested in the privacy of their communications, and law enforcement officials want to regulate data encryption for national security reasons. Law enforcement personnel argue that encryption also protects computer criminals, organized crime groups, and cyber terrorists. The U.S. appears to favor law enforcement officials regulating data encryption. However, without international cooperation and consensus, the system will not work since a user could easily access encryption software from elsewhere.

Jurisdiction

Jurisdiction is one of the biggest challenges to law enforcement in the information age. “Jurisdiction is the lawful ability of a government to subject a person to that government’s legal processes“ (Carter & Katz, 2000). Many computer crime incidents involve more than one jurisdiction, which makes it difficult to determine the *locus delicti*. It is even more difficult if the crime involves jurisdictions across international borders.

Currently, only serious crime cases are investigated multi-jurisdictionally. Extraterritorial jurisdiction principles should be applied in case of multi-jurisdictional incidents. In the United Nations Manual, it is argued that before deciding jurisdictions, four principles should be considered. These four principles are:

- The active nationality principle, which is determined according to the nationality of the offender.
- The passive personality principle, which is determined according to the nationality of the victims.
- The protective principle, which is determined according to the protection of the vital benefits of a government.
- The universality principle, which is determined according to the protection of

universal values (United Nations, 2000).

In sum, to solve extraterritorial jurisdiction problems, legislation should be harmonized. Agreements on mutual assistance must be reached. In addition, when required, extradition principle, and exchange of the offenders, should be utilized.

Detecting Computer Crime

Detecting computer crime is very challenging to organizations and investigators. These crimes are very different than traditional crimes in that they involve specialized detection and investigative measures.

Parker (1981) offered two general categories of detection measures, proactive and reactive measures. Proactive measures aim to detect computer crimes before they are committed. Intrusion detection tools may be either hardware devices or software programs. Intrusion detection tools may be installed over the local network to control and detect intrusions. The intrusion detection software can also check the local system and in case of an intrusion notifies the system operator. For instance, almost all system login attempts and unauthorized access to sensitive data, (e.g. payroll or personnel files), are controlled. However, proactive measures are ineffective if someone obtains passwords through social engineering (breaking an organization's security by interactions with people; for example, tricking someone into giving out a password) or some other technique and commits an intrusion.

Reactive measures aim to detect ongoing crimes or crimes which have already been committed. This includes auditing the system and checking log files.

Doney (1998) states that most computer crime is discovered by chance. Nevertheless, there are some protective detection measures that managers should be aware of to help them detect computer crime. In an early study, Allen (1977) suggested managers be wary of suspicious employees, a seemingly greedy employee's error, the suspicious result of an audit, a seemingly suspicious wife of a manager, and a suspicious result of an Internal Revenue Service (IRS) investigation.

Bequai (1983) listed seven basic rules to be followed in the event of an intrusion or computer-related crime. Administration should identify the nature and extent of the problem (e.g., was is intentional or accidental), record every observation, interview the suspect(s), design all the questions to be asked, and do not forget to obtain personal information, narrow the subject list by looking at job descriptions and the persons who had the opportunity (e.g., the list may include hardware personnel, software personnel, operations personnel, or management personnel), be aware of the legal issues (privacy rights of suspects or witnesses), and finally, prepare a well-organized and detailed report.

Investigating Computer Crime

Investigating a computer crime is a serious challenge to both police and private investigators. Most organizations are not prepared to investigate a computer crime (Stephenson, 2000). Having resources does not always mean that an organization can do in-depth technical investigation. Effective computer crime investigation has two main parts: being aware of the key components of a computer crime investigation, and making sure that computer crime investigators have the required specialized skill.

Investigating computer crime involves a series of processes. Indeed, the investigation includes identifying the extent of the problem, conducting the search and/or seizure, and preparing the search warrant. Experts or consultants may also be used. These processes combine to answer the classic questions in any investigation: who, why, when, where, and how?

Computer crime investigation is generally divided into three main phases. First, the investigation team must consider what type of system is going to be seized. If the investigator knows the configuration of the system, the investigation can be done more effectively. Therefore, the investigator should know the system, the system operators, the security level of the system, the location of the system, and the type of media used by the system. Next, the members of the search and seizure team must be determined. To obtain evidence based on probable cause (according to the Fourth Amendment), the investigative team should consist of members with different expertise. Members should include a team leader, an information security expert, a legal counselor, and a technical assistant. Last, the risks of the evidence being destroyed by the suspect must be identified. If there is a possibility that the suspect can destroy the evidence, a search warrant should immediately be prepared. This happens when the suspect engaged the criminal activity at home or a place where s/he thinks the evidence is ‘safe’ (Computer Crime, 1997).

Parker (1981) identified the key components of a computer crime investigation. First, there should be a proper team for investigation. Technical advisors may be included to the team. Advisors may assist to preserve electronic evidence with their special knowledge. Second, records should be checked in detail. Third, informants should be interviewed. Fourth, crime scenes should be carefully studied. Fifth, suspects and bulletin board activities may be tracked with various surveillance tools. Sixth, search warrants should be prepared. Seventh, evidence should be collected and preserved (Parker, 1981).

Additionally, computer crime investigators should have several skills. Investigators should have an understanding of new methods of computer-related crime. Investigators should have adequate knowledge of computers. Investigators should know that computer crime investigation includes protection of the resources and interests of society, as well as protection of the rights and freedoms of citizens. Investigators should be trained regularly to keep up with advances in computer technology. Investigators should avoid causing damage while conducting an investigation (Parker, 1981).

Bequai (1983) discusses several preliminary investigative considerations. It should be made sure that a crime has occurred. The nature and type of crime committed must be identified. The technical skills required to investigate the alleged criminal(s) must be identified. All suspects and witnesses and their respective job roles in the system must be identified. The possible motives must be identified. The physical evidence must be identified. All suspects, and record the interviews must be interviewed. The crime scene must be secured. Similar occurrences in the past must be checked for. All prior occurrences to find similarities among the incidents must be reviewed. Personnel data of all suspects must be checked. A list of business competitors, and their possible motives must be made. The possible impact of the incident on the organization in the marketplace must be identified. The relationship of the incident with any possible larger fraud—what has occurred may be part of a more intricate or complex crime must be made. The type and amount of organizational support for law enforcement investigators must be determined. The organization’s overall policies and focus on the security and audit policies must be reviewed.

Conly (1989) explains the nature of computer crime investigations as having four key elements. First, computer crime investigation is a time consuming process. Second, interaction with victims is much more important in this type of investigation than in a traditional investigation because victims can assist in the identification of suspects, and may provide technical support. Then, there is a huge amount of traditional police work involved in computer crime investigations (some say that it is 90 percent traditional police work, and 10 percent technical skill). Last, the nature of computer crime requires a proactive investigative approach because after the incident, the evidence may be gone.

Not only must computer crime investigators have technical capabilities, but they should also have adequate knowledge of computer crime laws (McKee, no date). Further, investigators must know basic police work (e.g. how to investigate, how to preserve evidence, how to present evidence, and how to deal with those in the judiciary). Therefore, law enforcement agencies cannot hire a strictly technical person to perform investigations. Agencies must prepare their own investigators with the proper knowledge of computer technology, computer crime laws, and related police work.

In case of an incident, companies and organizations have three choices. They can perform their own investigations, or they can either notify law enforcement or hire private investigators. The best private investigators may be found within the computer security community (Stephenson, 2000). Investigation should start immediately whenever a computer crime incident occurs. Time is very important in computer crime investigation. In a fraction of second, a whole computer system can be wreaking havoc locally, or around the world. Moreover, investigation should be conducted thoroughly. Conly (1989) lists three reasons to conduct a thorough investigation: more information (type of activity, type and amount of equipment used, and the number of persons engaged in the activity) results in better and more specific search warrants; if investigators know what to search at the crime scene, there will not be time delays; and having some information about the crime scene before an investigation may assist investigators in determining whether or not there is a need for technical experts.

After planning the investigation processes, the final step is to execute the plan. Executing the plan includes the following steps:

- The crime scene should be secured: The crime scene includes the computer systems, power systems, and network and telecommunication equipment. The suspect should be removed from the area if s/he is close to the system. It should not be forgotten that the suspect might have access to the system even after the search has been conducted.
- The Investigative team should enter the crime scene slowly so that they do not destroy any evidence: A small touch to a keyboard during the search may destroy all evidence. Hence, investigators must be very careful. Any active computer, monitor, or other peripherals should not be turned off before the search is completed.

- The crime scene should be photographed or videotaped: This may help in cases that go to court. However, while taking photographs remember that a flash may "white-out" the image on the screen.
- The investigator should label everything: The investigator should identify and mark all evidence. This labeling includes computer systems, documents, cables, and various auxiliary devices (storage systems, printers, modems, etc.) (Computer Crime, 1997).

This study discusses computer crime investigation based on in five essentials: search, seizure, evidence, expert selection and use, and search warrant. However, before getting into details, some definitions that are specific to computer crime investigation are needed. A list of these definitions is contained in Appendix.

Search and Seizure of Computers

Searching and seizuring a computer or computer systems is different from traditional searches and seizures. However, in general, similar rules apply to computer crime searches. For instance, searching a computer must be conducted in the same way as one would search and secure a physical crime scene. Even though investigating a computer crime entails searching mostly intangible 'objects' (data, e-mails, bulletin boards, etc), there are tangible objects (papers, pamphlets, media, filing cabinets, desk drawers, and all physical peripherals of computers) as well. In some incidents, investigators may need to search already deleted files. With the help of specific operating system tools, investigators may be able to recover some of the deleted files.

The first consideration in any search is that it must be conducted with a probable cause adhering to the Fourth Amendment, most safely through assigned and properly authorized search warrant. Without probable cause, the evidence collected in searches may be considered illegally obtained evidence, which would subject the evidence to the "exclusionary rule." On the other hand, there are some cases that a search can be done without probable cause. For example, a search can be performed without probable cause if a person has consented to the search (Federal Guidelines, 2000).

The U.S. Secret Service lists two steps in preparing for a search in a computer crime investigation (Conly, 1989). First, information about the occupants of the crime scene should be obtained. For instance, the number of residents, and their educational and employment backgrounds should be known. Then, the telephone records for every line for the crime scene should be obtained and reviewed.

Depending on the search of computer crime scene, seizure of computer equipment may be necessary. Seizure has two facets: seizure of hardware, and seizure of information (Federal Guidelines, 2000). No matter what is seized, the items are seized as evidence, and must be stated in the search warrant.

Seizing Hardware

*S*eizing hardware is the seizure of any physical components of computer systems, such as the keyboard, printer, media, CD-ROM, modem, hard drive, backup units, and diskettes. The idea of seizing hardware is based on three theories (Federal Guidelines, 2000).

1. The hardware is illegal: The hardware is criminally possessed, and its seizure may prevent a crime.

2. The hardware is used as an instrument: The hardware is a means to commit a criminal act, or acts.

3. The hardware is a part of the evidence: The hardware is a piece of evidence that may assist in the conviction of a suspect.

A challenging issue arises at this point. Having probable cause to seize a "computer" does not mean seizing all of its peripheral devices. It is not acceptable to seize everything connected to the target computer unless the warrant so stipulates for said devices.

Seizing Information

Compared with hardware seizure, seizing information is much more complex. Indeed, the seizure of hardware relates to physical and tangible parts, whereas information seizing relates to intangible components, such as data or software. The information to be seized may exist on the computer or device located at the crime scene or another computer or device at another location (Federal Guidelines, 2000). The three theories mentioned for seizing hardware also apply to the seizure of information. The information itself may be illegal (e.g., software piracy), the information may be used as a means to commit a crime (e.g. viruses or worm programs), or the information itself may be considered evidence (e.g. picture of child pornography).

Evidence

Evidence is defined as:

> “Any species of proof of probative matter, legally presented at the trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, and objects for the purpose of inducing belief in the minds of the court and jurors as to their contention” (Computer Crime, 1997).

Carefully collected evidence in computer crime cases is as important as in any other criminal case. This evidence may be essential for successful prosecution. Evidence assists in establishing facts. Indeed, the goal of evidence is to prove whether or not a crime occurred.

Computer (or electronic) evidence is different than other sources of evidence in following ways. First, computer evidence can easily be altered, copied, stored, or moved (Federal Guidelines, 2000). Second, since computers use electricity, power interruption may cause harm to computer evidence (Conly, 1989). Then, computers may be harmed even when they are turned off (e.g., dispositioning the hard drive heads) (Conly, 1989). Last, magnetic fields may harm or destroy magnetic storage media (e.g., hard drives or floppy diskettes) (Conly, 1989).

Types of Evidence

Many forms of evidence are being used in the courts. In general, there are four types of evidence: direct evidence, real evidence, documentary evidence, and demonstration evidence (Computer Crime, 1997). Direct evidence is an oral testimony by a witness. Real evidence is also called physical evidence, which is composed of tangible objects. Physical evidence is used to prove or disprove guilt. Documentary evidence is the evidence composed of business records, any printouts, books, manuals, etc. These materials are presented to the court to support an idea. Demonstration evidence is a number of visual objects to assist people understanding the incident by depicting a situation. These objects may be a chart, an illustration, or a model.

However, the evidence in computer crime cases may be somewhat different. Therefore, evidence types specific to computer crime investigation may be listed as files and documents, e-mail, login/logout events, and web access (Hosmer, Feldman, & Giordano, no date). Files and documents of the computer system may contain valuable information (e.g., financial information, information about meetings, and information about people, such as addresses or phone numbers). Nowadays, e-mail messages are being used for almost every type of communication. Thus, they contain important personal information. A striking example: Oliver North and John Poin-Dexter communicated via e-mail by using the computer systems of National Security Council. Even though they deleted the e-mail messages, the messages were recovered from the backup files and used as evidence in the Iran-Contra investigation. Logging into or logging out of a network may contain some time and place information, which can be used as evidence. Operating systems keep a record of the web pages that a computer access. Similarly, special auditing programs may also keep the history of sites that are browsed by a user. Moreover, Internet Service Providers (ISPs) can store and check the Internet Protocol (IP) addresses that a computer contacts. All these may be used as evidence.

Evidence may be considered legal evidence, in the courts, after a series of steps. First of all, it must be relevant and competent, and more importantly, it must be compliant with the Rules of Evidence. An investigator should have a thorough understanding of the Rules of Evidence so that evidence may be accepted in the legal process. The Rules of Evidence relevant to our discussion or computer crime is briefly presented.

Rules of Evidence

Rules of Evidence are the guidelines by which evidence may be allowed or disallowed. Some of these rules are: hearsay rule, best evidence rule, distinctive evidence rule, authentication, and distinctive evidence rule.

1) Hearsay Rule

The first problem that computer-related crime cases presents is the hearsay rule of evidence. By definition, under the Federal Rules of Evidence, all business operations and records are “hearsay” because of the lack of firsthand proof that they are reliable, accurate, and trustworthy (Icove, Seger, & VonStorch, 1995). Computer records are included in this consideration. Indeed, computer-generated evidence is only a representation of the original evidence because the original is stored as an electronic bit on the magnetic storage device (Computer Crime, 1997).

Generally, hearsay evidence is not admissible in court, but there are some well-established exceptions to this rule. First, evidence must be in compliance with best evidence rule. Second, evidence must be authenticated. Third, evidence must be in compliance with distinctive evidence rule. Then, evidence must be a part of the general business processes. Last, reliability of witnesses can affect admissibility of evidence (Icove, Seger, & VonStorch, 1995)

2) Best Evidence Rule

Another problem facing computer evidence is the best evidence rule. The best evidence rule requires that a photocopy of a document is not admissible if the original of the document exists (Icove, Seger, & VonStorch, 1995). This rule states, "to prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required" (Federal Guidelines, 2000). Accordingly, computer evidence must meet the best evidence rule. In other words, if the evidence is not the 'original', it must be the best copy available. This rule is established to prevent any intentional or unintentional alteration of evidence (Computer Crime, 1997). The Federal Rules of Evidence provide some exceptions to the best evidence rule. First, Federal Rules of Evidence state that "if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'" (Federal Guidelines, 2000). Second, when the original is lost or destroyed by manmade or natural disasters (e.g., fire, flood, and earthquake) the court will accept a duplication (Computer Crime, 1997). Then, when the original is destroyed in the course of business transactions, a duplicate is acceptable (Computer Crime, 1997). Last, when the original, in the possession of a third party, is not readable by the court's power, a duplicate is acceptable (Computer Crime, 1997).

3) Authentication

The prosecutor must authenticate computer evidence. There should be a clear and satisfactory explanation that evidence is unaltered and pristine (Stephenson, 2000). When presenting computer logs, printouts, files, and records, there should be provided a satisfactory explanation of the information collection method, the input and output storage system, and the information retrieving method, used in preserving the computer record (Conly, 1989).

4) Distinctive Evidence Rule

Showing some “distinctive” characteristics of evidence is a common way of authenticating evidence (Federal Guidelines, 2000). Federal Rules of Evidence require an item to be “distinctive” in “its appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances (Federal Guidelines, 2000).

5) Evidence must be a Part of the General Business Process

Evidence must be produced during the course of general business processes. Federal Rules of Evidence state that the court may admit a business document “at or near the time, by or from information transmitted by, a person with knowledge, if kept in the course of regularly conducted business activity, and if it was the regular practice of that business activity to make the [report or document], all as shown by testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness” (Computer Crime, 1997).

Chain of Custody

The hand-to-hand 'chain' process that evidence goes through is called the "chain of custody." When presenting evidence to a court, the prosecutor must be able to prove accountability and protection of evidence by all persons who accessed the evidence (Computer Crime, 1997). The prosecutor must show that the evidence presented in court is the same evidence that was seized (Federal Guidelines, 2000). The chain of evidence documentation must show three important things (Computer Crime, 1997). Who collected the evidence, who protected the evidence, and who possessed the evidence.

Relying on the Victim

Investigators cannot know every computer system or every operating system (Conly, 1989). They may encounter various systems, hardware, software, and peripheral equipment. Hence, investigators may need assistance from victims. Even though relying on a victim to get information about a system may be beneficial, there are some concerns with using victims in this way. For instance, the victim may be the perpetrator; therefore, investigators should be very careful while using victims to aid in the investigation.

Evidence Life Cycle

The final issue concerning evidence is its life cycle. The evidence life cycle is the combination of series of processes that each piece of evidence progresses through. These processes are collection and identification, storing, preservation, and transportation, presentation in court, returning evidence to the victim (Computer Crime, 1997).

Collection and identification is the step involving the proper labeling of evidence properly during collection. Storing, preservation, and transportation are the processes of packing and protecting evidence. Evidence may be affected by cold, heat, humidity, magnetic fields, or water. If the evidence is not properly preserved, persons within the chain of custody may be held liable for damages. Presentation in court involves presenting evidence to the court. Each piece of evidence may be used in the courts. After the trial is over, the evidence is returned to the owner (or victim). Returning evidence to the victim is the step of returning evidence back to the victim. Except with some types of evidence (such as illegal drugs) all evidence should be protected and finally returned to the victim.

Use of Experts

The diversity of computer hardware and software challenges investigators of computer crime. It is not uncommon for investigators use experts from other investigative agencies, the private sector, or universities while conducting computer crime investigations (Conly, 1989). Indeed, the utilization of experts is a requirement due to the comprehensiveness of computer crime investigations.

Experts can help investigators to search, protect, and analyze data (Conly, 1989). Even the most experienced investigator cannot know all the different types of hardware and peripheral equipment. Hence, the use of experts is generally unavoidable in computer crime investigations. It is impossible to know all person(s) who committed the crime in advance, so investigators must be extremely careful when using expert assistance they may have perpetrated the crime.

Search Warrant

When the suspect has vital evidence, and there is a possibility that the suspect may cause damage to the evidence, a search warrant is needed. Before preparing a search warrant, some decisions must be made by investigators and prosecutors. First, search warrants should be as specific as possible (Conly, 1989). Investigators, prosecutors, and law enforcement personnel should participate in the search warrant preparation to include all evidence required.

If the warrant is not specific enough, law enforcement agencies may inadvertently conduct an illegal search. The United Nations Manual on Computer-related Crime notes:

> "Application of the traditional powers of search and seizure might; however, cause problems…If the legal principle of minimum coercion or of proportionality makes it unlawful to seize comprehensive data carriers, or complete computer installations, in order to gather only a small amount of data. Similarly, search and seizure of comprehensive data carriers could cause serious prejudice to business activities or infringe the privacy rights of third parties" (United Nations, 2000)

Law enforcement agencies and the judiciary, therefore, must be highly sensitive and insist on specificity while drafting search warrants for computer systems (Computer Crime, 1997). Another decision involves about the security of the system (Computer Crime, 1997). If the system is at risk, the investigation team should act quickly and be prepared to perform the search and seizure. Whether or not the system is networked is also a consideration. The physical location of information may be difficult to find in networked environment, so a search warrant team must consider this and prepare a plan

(Federal Guidelines, 2000). In all, the search warrant preparation is another challenging process to law enforcement personnel, prosecutors, and investigators.

Conclusion

This chapter discussed computer crime as it related to the criminal justice system, especially law enforcement. Law enforcement personnel, investigators, prosecutors, judges confront the new technological challenge, namely computer crime. Current situation of the entire criminal justice system is reviewed. Law enforcement personnel should be equipped with proper training, necessary equipment, and computer-literate personnel. Computer crime laws and international aspects of the computer crime problem are examined. Finally, detection and investigation of computer crime are explained.

Next chapter discusses the problems of the criminal justice system. Problems related to law enforcement, prosecutors, and judges are going to be argued separately. In addition, some general problems (international problems, difficulty of detection, inadequacy of laws, and vulnerabilities of computers) are also going to be discussed. As a result, a brief summary of problems concludes the chapter.

CHAPTER 4

PROBLEM ANALYSIS

Computer crime presents several challenges to the criminal justice system. In this chapter, these challenges are discussed. The problems are divided into four categories: 1) problems related to law enforcement, 2) problems related to investigators, 3) problems related to prosecutors and judges, and 4) general problems.

Problems Related to Law Enforcement

It is not unreasonable to say that law enforcement agencies face the greatest challenges. Similar to the situation with traditional crimes, law enforcement agencies are seen as the primary responsible agency for detection, prevention, and investigation of computer crime. Each step has unique problems that must be solved. Moreover, law enforcement or agencies in general, are not ready for this new challenge in terms of personnel, equipment, and funding.

Training

The ever-changing and complex nature of computer technology requires law enforcement personnel to develop new skills to keep up with the fast pace of technology. The increasing sophistication of computer technology requires dynamic and ongoing training. Police personnel must regularly receive training for successful investigation, detection, and prevention of computer crime. Most people who address the computer crime problem agree that criminal justice officials should receive proper training (Conly, 1989). Initially, high priorities must be placed on police personnel having a basic understanding and knowledge of computer systems and programs. After these basic skills have been learned, specialized training programs relating directly to computer crime may be implemented.

Equipment

Because of the complex nature of the computer crime problem, law enforcement personnel need to utilize several tools. Personnel should be supplied with various equipment such as Net Threat Analyzer (forensic Internet analysis software used to identify Internet threats), Seized (a program used to lock and secure evidence computers), and Text Search Plus (a text search utility used to locate key strings of text and graphic files). In addition, manuals and computer science publications should be provided to personnel.

Funding

Lack of funding restricts law enforcement by several ways. Allocating resources to a computer crime unit or division for small agencies is more difficult than is for larger agencies. Relatively small computer crime budgets may be caused by the perceptions of these types of crimes. Most people do not see computer crime as serious issues. Another issue with the funding is that high-tech equipment, required for complex computer crime investigations, tends to be more expensive than other police equipment.

Personnel

Law enforcement agencies need computer literate personnel for computer crime investigation. An average police officer may not have the required skills and abilities to perform computer crime investigations. Police agencies should hire or recruit computer literate personnel. Hiring an expert to perform investigations may cause problems. Retaining and keeping specialized personnel after training is another problem. It is agreed that one of the greatest weaknesses of computer crime investigation is that investigation and prosecution depend on particular individuals (Conly, 1989). If these individuals leave the agency, investigations or prosecutions in these types of cases may cease.

Problems Related to Investigators

Investigating computer crime incidents pose some specific problems as well. First, searches should be done in accordance with the laws of evidence and the Fourth Amendment. Evidence will be illegal without probable cause. Second, evidence should be collected carefully, and preserved correctly. Conly (1989) discusses two problems of computer crime investigations: 1) there is a reluctance to report, and 2) computer-related crime investigations are time consuming.

Victims of computer-related crime are reluctant to report these incidents to law enforcement. There are several reasons for this. First, corporations have the threat of negative publicity which may block their business operations. Another reason is that some victims say law enforcement agencies are not capable of performing thorough investigations. Many times victims may not know the proper agency to contact, especially when incidents involve more than one state (Conly, 1989). Even when they do, many believe that computer criminals do not receive commensurate punishments (Bequai, 1983). Victims may be anxious about the results of investigations because sometimes investigations reveal companies' "dirty laundry" (Bequai, 1983). Finally, victims fear that they may be held liable for not establishing proper security provisions

According to the Computer Crime and Security Survey done in 1999, organizations did not report intrusions to law enforcement mainly for four reasons (Power, 1999): negative publicity, the idea that competitors would use to their advantage, they were unaware that it could have been reported, and civil remedy appeared to be the best course of action.

Computer-related crime cases require a huge amount of time to investigate. Specifically, if computer crime investigation involves massive amount of storage devices and several computers, investigations may take a much longer amount of time. Additionally, law enforcement personnel end up with relatively small number of arrests in these cases, and numbers of arrests continue to be used as a measure of success in law enforcement agencies (Conly 1989). Therefore, this gigantic amount of time that agencies spent to investigate and detect computer crime may not be well appreciated.

Problems Related to Prosecutors and Judges

The prosecution of computer crime is a new challenge to the judicial system. Similar to the scarcity of the specialized law enforcement officers in investigating computer crime, there are few prosecutors or judges who have expertise in computer crime cases.

As the number of computer crime incidents increase, the need for prosecution and the demand for specialized prosecutors increases as well. Nevertheless, judges and prosecutors cannot confront the increasing demand facing them every single day. The criminal justice system and society fails to provide them with proper training and equipment. Also, as previously noted, society does not view computer crime as a serious issue. Since prosecutors reflect the ideas of the general public, they have the general perception that society is more threatened by "street crimes." Everybody can see and understand damage that street crimes cause; however, this is not the case for computer-related crime.

Prosecuting a computer crime case is much more complex than prosecuting a traditional crime. The number of successfully prosecuted computer crime cases demonstrates this difficulty. Indeed, it is reported that only one in twenty thousand computer crime criminals receive an active prison sentence (Wyatt & Farrar, 1994). There are many reasons for this low relatively small rate. Computer crime cases require detailed case preparation, attention, understanding of business operations, extensive paperwork, and diligent examination of data. There are also problems with the reluctance of victims to report such incidents, and jurisdictional problems such as state versus local. In addition, other limitations block prosecutors and judges.

Icove, Seger, and Vonstorch (1995) list several limitations for prosecution. First, computer crime prosecution requires special technical skills and preparation. Second, the nature of the computer crime evidence causes problems with searching for, seizing and preserving evidence. Third, there is a need to cooperate with experts and to have experts provide testimony. Fourth, problems with testimony--testifying without traditional physical evidence may make it difficult to convince the judge and jury

Judges are also faces with several difficulties while hearing computer crime cases. First, judges may not have the knowledge to understand the technical details that are presented during the trial. Second, law schools are only recently offering computer law courses. Third, it is difficult to manage a trial laden with technical details. Fourth, confusing technical details may lead the judge or jurors to reach an erroneous conclusion. Finally, sometimes federal and local laws may be conflicting

Prosecutors are an integral part of the judicial system that must deal with the computer crime problem. August Bequai (1983) discussed factors influencing prosecutors in his classic book, <u>How to Prevent Computer Crime: A Guide For the Managers</u>. The first factor is that the public does not accept computer crime as a threat if the offender is a juvenile. Second, a computer criminal having no prior criminal record is usually far from incarceration--this may discourage prosecutors from pursuing a criminal case against them. Third, computer crime cases lack traditional witnesses and adequate numbers of witnesses. Finally, evidentiary problems--prosecutors do not like “hearsay” or “best evidence” rules (Bequai, 1983).

General Problems

For government officials and organizations it is difficult to address computer-related crime problems for several reasons. These reasons include: the weaknesses of computers, lack of experience on how to investigate, prosecute, and prevent computer crime, scarcity of computer-literate personnel, shortage of funding, low security awareness, inadequacy of laws, and international problems and the jurisdiction dilemma.

International Problems and Jurisdiction Dilemma

Computer networks and the Internet provide criminals with the opportunity to commit crimes internationally. A computer user in one country can access a system in another country and easily cause great harm. This transnational nature exacerbates problems with the detection, investigation, and prosecution of computer crime. In the United Nations Manual, the following seven issues are discussed as problems with international cooperation regarding computer crime (United Nations, 2000). There is a lack of consensus on the types of computer crime, and on the definition(s) of computer crime(s). There is a scarcity of specialized personnel in police agencies, courts, and other related areas. There is a lack of the legal powers to access and investigate computer systems. In addition, lack of harmony among the procedural laws of different nations exacerbates the situation. The transnational structure of computer crime, and lack of proper mutual assistance and extradition rules make difficult to combat against computer crime.

As discussed above, international computer crime can be effectively addressed only with cooperation between nations. However, this cooperation may lead to other problems. Cooperation can cause dual criminality, which is result of the jurisdictional dilemma (United Nations, 2000). Also, mutual assistance can be a problem in cases involving the transmission of sensitive data, such as financial data (United Nations, 2000).

Computer crime cases often involve several jurisdictions because of the interstate and international nature of the offense (Conly, 1989). The jurisdiction dilemma may cause similar problems within a same nation. Identifying a responsible jurisdiction for computer crime cases may be difficult. Local, state, and federal governments may all contend to have jurisdiction in some cases. Additionally, some federal laws (e.g. Title 18 Section 1029, Title 18 Section 1030) allow some federal agencies (e.g. Postal Inspectors, and the Drug Enforcement Administration) to investigate computer-related crime (Conly, 1989). Some governmental agencies do not want to encompass other jurisdictions or investigate jointly; sometimes they even reject prosecution (Conly, 1989).

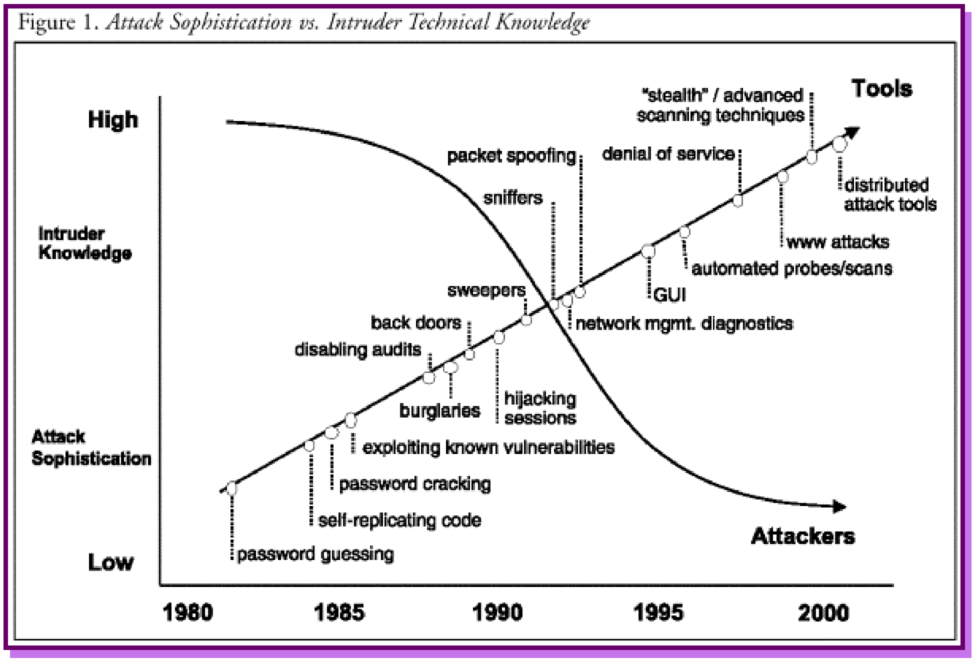
Difficulty of Detection

Computer crime detection may be very difficult when committed by insiders who know the system well. These kinds of insiders can misuse the system through its vulnerabilities without leaving any trace of their involvement. Managers should regularly monitor and control the actions of system operators, system managers, and employees. This audit may be conducted through the establishment of a computer security policy for the organization. As Barrett (1997) noted, the most distressing feature of computer crime detection is “the absence of a ‘smoking gun’.” In other words, there is difficulty in tracing or locating the perpetrator. Hence, computer security experts advise organizations to focus on prevention (Barrett, 1997).

Another important aspect of computer crime is that breaking into systems is getting easier every day. In the 1980s, intruders were highly knowledged expert; however, today almost anyone with proper tools can break into systems (Allen, Alberts, & Behrens, 2000). This situation makes detection more difficult. Allen and her colleagues (2000) illustrated this relationship in Figure 4.1.

Figure 4.1.

Attack Sophistication vs. Intruder Technical Knowledge



Source: Allen, Alberts, and Behrens (2000). Reprinted with permission of the author.

This figure shows that breaking into systems is getting easier every day. Today, almost any computer user can break into systems. Finding proper tools is more important for current computer users. If they can find the appropriate tools, they can easily commit computer crime.

Inadequacy of Laws

Former Attorney General Janet Reno explained, “The fight against lawlessness on the Internet will be one of the greatest law enforcement challenges of this century” (Clarker, Dempsey, & O’Connor, 1998). In a rush to cope with the computer crime problem, legislators have quickly enacted several laws over the last two decades. Some of these laws are rarely used because of their poor structure or wording. Because of the rapid pace of change in computer technology, recent developments are not addressed in current laws. Indeed, new technology has outmoded some existing laws. Laws that address older technology may actually restrict law enforcement personnel, prosecutors, judges, and investigators. Successful prosecution and investigation require very well defined laws (Conly, 1989). Laws should be general enough to cover developments in the computer industry so the laws do not need frequent amendments (Conly, 1989).

Vulnerabilities of Computers

Hardware and software weaknesses arise from several sources. One important reason is the corporate desire to make as much money as possible while spending the least amount possible. Security and performance are often two opposing ends of a continuum. Companies must find an appropriate balance between the two. Unfortunately, but not surprisingly, companies choose performance over security. Security often suffers in this scenario. Also, the pressure of competition in the market place forces companies to produce new products very rapidly. Sometimes this means the products will not be inspected thoroughly. In addition, software developers usually add loopholes in program for their own access and later use. With these loopholes, programmers can bypass security measures while they are performing system maintenance. There are also physical security problems with computer systems in addition to weaknesses often found in computer networks.

The biggest vulnerability in a computer system is the user (human being). The people who manage or use computer networks and systems often exploit the vulnerabilities of the computer system. They may produce the vulnerabilities by leaving their machine unsupervised while they are logged in, or by using very simple passwords. Another problem with the human factor is trust. When we trust people to use a system, they may learn the secrets or weaknesses within that system. Lack of a security conscious culture is a significant vulnerability.

Hardware security problems result from several factors, including the poor control of the accesses to the systems or transactions, the low public awareness of computer operations, or not separating the key responsibilities within organizations.

Software security problems often result from giving the responsibilities of the entire system and its programs to a single person. Providing oral (instead of written) instructions to the machine operators, and combining program maintenance with production also may cause software security problems (Bequai, 1983). Data security problems result from the scarcity of control over input documents, lack of control over output documents, and ease of access to the disks, tapes, etc (Bequai, 1983). Transmission security problems result from the infrequent changing of passwords, failing to use cryptography, or lack of firewalls, etc (Bequai, 1983). Hackers use these weaknesses and vulnerabilities. They are very organized and share information using web sites, e-mail, electronic meetings, and even written magazines.

Conclusion

Computer crime presents several challenges to the criminal justice system. In this chapter, these challenges were discussed. The problems were divided in to four categories: problems related to law enforcement, problems related to investigators, problems related to prosecutors and judges, and general problems. General problems were examined in four categories: international problems and jurisdiction dilemma, difficulty of detection, inadequacy of laws, and vulnerabilities of computers. Law enforcement agencies are not ready for this new challenge in terms of personnel, equipment, and funding.

Next chapter is focused on solution analysis of computer crime problem. First, computer crime handling procedures will be discussed. Then, specific solutions to the problems of criminal justice components are going to be examined. Finally, general solutions will conclude the next chapter.

CHAPTER 5

SOLUTION ANALYSIS

Each part of the criminal justice system attempts to provide its own solutions to the computer crime problem. However, there are some procedures that apply to every solution process. In this chapter, these procedures are explained. Specific solutions for each component of the criminal justice system are also discussed.

Computer Crime Handling Procedures

Conly (1989) proposed a comprehensive approach composed of nine core and six optional steps in her "Organizing for Computer Crime Investigation and Prosecution" book. First, highest-level justice officials (e.g. District Attorneys, Chiefs of Police, and Sheriffs) should be persistent and dedicated in addressing the computer crime problem. Second, the appropriate level of commitment to the problem should be decided by considering four elements. These four elements are agency size, shared resources (e.g., personnel, information, and task forces), functional specialist, and full-time assignment. A small agency does not need to acquire a functional specialist and a full-time investigator. A small agency cannot acquire necessary sources, and may not have enough computer-literate personnel to solely devote to computer crime unit. Therefore, it is better for a small agency to get help from other agencies or federal agencies. James Conser offers a grid (Table 5.1) to depict the relationship among these four elements (Conly, 1989).

Table 5.1.

Computer Crime Handling Strategy

Agency Size	Shared Resources	Functional Specialist	Full-time Assignment
Small	High Recommendation	Low Recommendation	Not Recommended
Medium	Moderate Recommendation	High Recommendation	Low Recommendation
Large	Low Recommendation	Moderate Recommendation	High Recommendation

Source: Modified from Catherine H. Conly, Organizing for Computer Crime Investigation and Prosecution

Third, administration should identify at least one investigator and prosecutor who are interested in computer crime. These persons may be identified through the use of a survey. Fourth, investigative personnel should receive at least one computer crime training course. Fifth, trained staff should be introduced to all other departments and personnel. All employees should understand the responsible person or unit to contact in case of a computer crime incident. Sixth, technical capability and resources of the department should be identified. Technical person(s) should assist staff with investigation and prosecution. Then, when appropriate, law enforcement and prosecution personnel should work together. Next, if appropriate, an association should be developed with other local and state agencies to combine resources and assist every agency in the association.

Last, contact should be made with potential victims to increase awareness and to gather information about unreported incidents.

Conly (1989) proposed also six optional steps. First, an investigation and prosecution team may be established for computer crime cases. This team should be entirely responsible for the investigation. Second, a technical staff may be developed to assist in investigations and prosecutions. Third, continued training may be supplied to investigative and prosecutive personnel because of the rapid change of computer technology. Fourth, basic computer crime investigation training may be supplied to every individual in a department beginning with those who work at the crime scenes. Next, equipment of the investigative personnel may be updated regularly. This new equipment may be obtained through forfeiture or donation. Finally, federal and state efforts in investigation and prosecution may be combined by sharing resources, personnel, and technology. This resource sharing is important in training. Small agencies may not have training resources, and they may benefit from this type of coordination and collaboration.

Specific Solutions to the Criminal Justice Components

Specific solutions to computer related crime is very similar to other problems confronting the criminal justice system. The solutions are divided in to four categories: solutions for law enforcement, solutions for investigators, solutions for prosecutors and judges, and general solutions.

Solutions For Law Enforcement

Personnel should be given the necessary training to deal with computer-related crime. They must be knowledgeable of security issues, investigative techniques and procedures, and computer laws and policies. Without well-trained law enforcement personnel, well-written laws and policies will mean nothing.

At the federal, state, and local levels, law enforcement is highly decentralized. There is little cooperation and coordination among agencies. As with many transnational type crimes, this causes problems for the investigation of computer crime incidents. To achieve successful prosecution of computer crime incidents, cooperation and consensus are of the utmost importance. Therefore, to bypass the weaknesses of such a diverse structure, new organizations and new teams should be developed to harmonize the agencies. Moreover, these new teams must be empowered with laws to work effectively without random power struggles so often observed between federal and local agencies.

Law enforcement administrators must allocate funding resources accordingly. Administrators may circumvent funding problems by increasing public awareness. Increased awareness may help agencies received additional resources and training through donations and grants.

Finally, cooperation, coordination, and consensus among law enforcement agencies are essential. Additionally, cooperation and collaboration with private industry should be sought. Often times, corporate security personnel are much better trained than local and federal officials.

Equipment is also required for success. Equipment is used for investigation, prosecution, prevention, and security. Hence, within the agencies, personnel should be supplied with the proper tools and equipment such as Net Threat Analyzer (forensic Internet analysis software used to identify Internet threats), Seized (a program used to lock and secure evidence computers), and Text Search Plus (a text search utility used to locate key strings of text and graphic files).

Solutions For Investigators

Specialized training is the key to solving many of the problems faced by investigators. Investigators must receive training in accordance with their job duties. Retention of expertise is another important challenge facing administrators. Criminal justice administrators must find ways to attract and retain qualified investigative personnel such as selecting computer-literate personnel after making good advertisements, providing them ongoing trainings, and supplying them with proper equipment and attractive salaries.

Solutions For Prosecutors and Judges

Paralleling the increase in computer crime incidents, the demand for successful prosecution has also grown. However, to achieve a successful prosecution, prosecutors and judges should be aware of several potential problems. First, as with investigators there is a need for special training to understand computer crime and the sophistication of such incidents. Further, judges must manage complex cases, and prosecutors must present the case as simply as possible for jurors to understand. They must ensure that they are not overwhelming the jury (or judge) with technical details. Eventually, public awareness will be increased, and this will have a positive impact on the prosecution of computer crime cases.

General Solutions

The criminal justice system must adapt to changes in computer technology. Criminal justice managers without adequate knowledge and skills cannot help agencies maintain knowledge relating to computer technology.

Computer crime results from a trade-off between costs of security implementation and the risks of not using any security counter measures. Governmental agencies, corporations, and individuals consider must these two sides and balance them according to their own policies. Indeed, this is risk analysis: analyzing risks and finding proper solutions to potential vulnerabilities.

For instance, a personal computer user identifies the level of threat to his/her computer. Threats may include unauthorized access to the information in his/her computer via the Internet, viruses, and system crashes. The personal computer user decides a course of action after evaluating these risks and the importance and secrecy of his/her personal data. As a result, that user can take the proper action by purchasing anti-virus programs, or by installing encryption programs. However, it is almost impossible to achieve a 100% risk free system. Yet, it is possible to control and minimize the exposure of computer systems. Hence, risk management aims to balance the cost of exposure and the cost of prevention. Icove (1997) claims that periodic risk analysis is "... the best pro-active weapon against computer crime."

Hence, the first step to combating computer crime is identifying the risks and vulnerabilities to a system and enacting appropriate preventive measures. There are many approaches to protect computer systems. Three major prevention models are increasing awareness, use of technology, and governmental regulations-laws and rules. Increasing awarenes is enhancing awareness about threats of computer crime by informing the users. Use of technology means that using technology for the protection of computer systems. Governmental Regulations-Laws and Rules is enacting laws and developing rules to deter computer criminals from committing computer crime, and to prosecute them adequately. The following sections discuss these three prevention models accordingly.

Increasing Awareness

Awareness of computer crime was first seen in the early 1960s (Parker, 1976). Increasing awareness or common sense prevention measures are the first and foremost measures. Common sense precautions imply that computer system users must be aware of simple but helpful prevention methods, such as changing passwords regularly, not leaving machines on without supervision, locking the server room, not taping passwords to monitors, and so on.

Low security awareness is one of the most important problems among institutions according to several scholars (Farmer, 1996; Icove, Seger, & VonStorch, 1995; Mendell, 1988, etc.). For example, according to a survey conducted by Farmer (1996) 60% of 1700 highly sensitive websites (such as government agencies, newspapers, credit unions, and banks) can be destroyed because of the poor access control. Lohr (1997) estimated that only one percent of all computer crime is detected by management.

Donn B. Parker explains the solution to the computer crime problem very clearly. In his Computer Security Management book, he contends the solution is as following:

> "If any single solution is to be drawn from the 11 years of research and consulting, it is that computer security is not primarily a technological subject. It is a subject of psychological and sociological behavior of people. As I have said repeatedly in my worldwide lecturing, computers do not commit errors, omissions, or crimes; only people can do these things that may subsequently be manifested in computers. Solutions to these problems also must come from people, their actions, and their attitudes" (Parker, 1981).

Wayne Spinak found that 80% of intrusions happen within the local area network (LAN), not from the Internet (as cited in Cohen, 1997). Icove, Seger, and VonStorch cite a study conducted by the Computer Security Institute. Results of the study reveal the following computer crime percentages are shown in Table 5.2.

Table 5.2.

Sources of Computer Crime Incidents

Sources of Incident	Percentages
Human Errors	55%
Physical Security Problems	20%
Dishonest employees	10%
Disgruntled employees	9%
Viruses	4%
Outsider Attacks	1-3%

Source: Adapted from information by Icove et al. (1995).

Mendell is yet another author who emphasizes awareness as the most effective prevention method. Mendell (1988) claims, “Computer crime is about people.“ He also adds that whatever security countermeasures are developed, computer criminals always appear to be one step ahead (Mendell, 1988).

Some scholars express the idea that education is the way to increase awareness. Kizza (1994) sees education as a long-term solution, and asserts that building fences cannot solve computer crime. However, educating the public, beginning with youths, can be the first step in prevention (Kizza, 1994). Benjamin and his colleagues (1998) express that security awareness training should include regular briefings and simulated attacks. Moreover, computer ethics courses should be offered at beginning in high school and continuing through graduate levels. With these courses, students can become more aware of computer crime problems and issues.

Solutions Based on the Theoretical Explanations of Computer Crime

Social learning theory has four major elements: differential association, differential reinforcement/punishment, definitions, and imitations (Akers, 1985). College students are always in contact with peer groups. Skinner and Fream (1997) concluded that friends and acquaintances are a good source for learning how to commit different computer crime techniques. Moreover, in the peer group an individual can learn positive and neutralizing definitions. These positive and neutralizing definitions rationalize illegal behaviors, and encourage that individual to commit computer crime. Skinner and Fream

(1997) found in their multivariate analysis that social learning theory was very effective in explaining computer crime.

The second major theoretical basis for explaining computer crime is “routine activities theory.” The routine activities theory is a criminological theory, proposed by Cohen and Felson (1979).

If we apply the routine activities theory to computer crime, we will see that the availability of suitable targets (more opportunities for computer abuse), the presence of motivated offenders (hacker subculture), and the absence of capable guardians (ineffective law enforcement response) may lead to more computer crime incidents. If these three factors converge (availability of suitable targets, presence of motivated offenders, and absence of capable guardians), then the likelihood of occurrence of computer crime increases. Therefore, to reduce the number of computer crime incidents, these three factors should be considered in detail. Target hardening and opportunity reduction are two basic methods for computer crime prevention. Some ways of target hardening are: increasing security, establishing a well-defined policy, and developing password selection and usage policies.

Methods to Increase Security Awareness and Reduce the Likelihood of Occurrence

Bologna (1993) lists eight factors that increase the probability of computer crime occurrence: 1) Inadequate rewards, 2) Inadequate management controls, 3) Inadequate support, 4) Inadequate operation reviews, 5) Inadequate enforcement of disciplinary rules, 6) Inadequate reinforcement and performance feedback mechanisms, 7) Fostering hostility, and 7) Other motivational issues.

These eight factors increase the probability of computer crime, so every organization must revise their policies according to these factors. Interestingly, most of the factors are related to problem is awareness.

For total security, all these functions should be in operation. Awareness has impact on the first three functions.

Doney (1998) discusses deterrence (deterrence is defined as crime prevention achieved through the fear of punishment) and its six strategies: reducing the likelihood of crime occurrence, make it more difficult to commit computer crime, enhancing detection tools, prosecuting and incarcerating computer criminals, using forensic accountants, reducing the losses. First, effectively managing disgruntled employees and training employees can assist in reducing the likelihood of crime occurrence. Further, recruitment should be conducted to identify potentially dishonest employees, such as using polygraph examination for sensitive positions. Second strategy is implementing an efficient computer security policy, and using technological tools to protect computer systems such as firewalls. Third strategy is using effective tools for detection (such as network analyzer). Fourth strategy is not letting perpetrators get away with their crimes, but instead adequately prosecuting and charging computer criminals to have a positive deterrent effect. Fifth strategy is using specialized persons to effectively investigate the incident. Last strategy is disseminating the authority and power, and developing a good system of controls. Of these six strategies, the first two and the last issue are related to awareness issue.

Skinner and Fream (1997) declared that the greater the perceived certainty of apprehension and severity of punishment, the greater the deterrent effect. Rosenblatt (1990) also expressed the same idea. He stated that certainty of apprehension and severity of punishment are the two main elements of deterrence. Moreover, it should not be forgotten that most computer crime incidents are discovered accidentally. An excellent example is Dennis F. Moran (explained in Chapter 2, Illustrative Cases, Case 4). Hence, the first task of management is to practice internal auditing. Auditing cannot detect all computer crime, but it may deter some acts.

Mass media may be one of the most influential factors in computer crime (Hollinger & Lanza-Kaduce, 1998). With various sources, such as TVs, movies, books, and magazines, media can manipulate perceptions about computer crime. A recent survey also found the importance of mass media for reporting information technology news (Dowland et al., 1999). Dowland and his colleagues (1999) added that both sides of the public awareness of computer crime should be considered in mass media usage. The two sides are: awareness can be increased so that people take proper precautions, and awareness should not be so intense that it unduly scares people and organizations (Dowland et al., 1999).

In addition, various types of security countermeasures can also be developed to protect systems: physical security, personnel security, communications security, and operations security (Icove, Seger, & VonStorch, 1995). The three authors define and explain these security countermeasures as physical security, personnel security, communications security, and operations security. Physical security is the protection of the physical environment of computer systems (the building, the server and server room, and computer accessories such as disks, tapes, diskettes, and documentation). In other words, it concerns the protection of physical assets. Natural and man-made hazards should be considered while site planning. Possible damage by power problems or environmental issues must be assessed. Personnel security is monitoring personnel to prevent employee theft and insider crime. Personnel should be given adequate security training, and access of personnel to critical systems and their passwords should be audited regularly. Personnel should be aware of social engineering, which is a technique used to obtain legitimate passwords (Icove, Seger, & VonStorch, 1995). Communications security is the protection of telephone, Internet, and fax communications, and prevention of illegal data transmissions. In protecting communications, the issues of the misrouting of data and wiretapping should be considered. Operations security is monitoring all the operations within the company, creating audit trails, and conducting electronic surveillance. Operations security ensures that proper policies and procedures are in place. Policies should also clearly identify the tasks and duties of each employee.

With these types security countermeasures, the possibility of computer crime incidents can be reduced. In summary, these security countermeasures are the issues to be considered when developing or implementing security policies.

Governmental agencies, corporations, and individuals must become more aware that even with the best technology, security countermeasures of the fail because of careless actions by employees. Therefore informing the users about potential threats, warning them regularly with reinforcing positive behavior, and maintaining good security countermeasures can reduce the problem. In short, identifying weaker areas, and finding proper solutions to those weaknesses will reduce computer crime incidents.

Use of Technology

The second prevention model is use of technology. Since computer crime is committed against computer systems, by definition, it should also be prevented by technology. There are some scholars who think that computer crime can be prevented by implementing computer security countermeasures, such as password authentication, firewalls, and data encryption (Adamski, 1997). Virus checkers are another form of technological security countermeasures.

Password Authentication

Passwords are a combination of various characters used to gain access to computer systems and to authenticate the identity of users. Password protected devices are among the first and easiest security countermeasures. They may be the weakest parts of the computer system for break-ins. Nevertheless, password authentication is reported as the leading countermeasure, as it is used by 76% of companies surveyed (Joutsen, 1999).

Encouraging users to engage in proper password practices is a pervasive problem. Many users do not want to select and change their passwords in a careful and regular manner. Since memorizing many passwords for various access controls (different computer programs, credit cards, debit cards, etc) is challenging enough, most computer users use personal information, such as names of loved ones, names of family members, birthdays, and other important days as their passwords. Moreover, people often write down these passwords and tape them to monitors, keyboards, or terminals. Users also fail to change passwords regularly. Technology cannot secure systems if people do not adhere to proper password practices.

Another important source of concern is the management of passwords of dismissed employees (Cohen, 1997). A disgruntled employee, whose password has not been cancelled, can intentionally or unintentionally do much more harm than a hacker. Therefore, all passwords for any employee leaving a company for any reason must be removed.

For password authentication countermeasures to be effective, a number of issues should be considered. Icove and his colleagues (1995) offered some of them as following: 1) System-generated passwords should be used, 2) Passwords should be at least 6 characters, 3) Nondictionary words should be used as passwords, 4) Password aging and expiration techniques should be in use, 5) Number of login attempts should be restricted (limited login attempts), 6) Login messages should be audited, 7) Password files should be stored and encrypted, and 8) If needed, time-based passwords should be used (i.e., password valid for only two weeks).

Firewalls

Firewalls are hardware or software (sometimes a combination of both) that controls the access to a computer system. Icove (1997) defines firewalls as security interfaces that stay between the Internet user and local systems. Authenticated users are allowed to enter the system, while others are not allowed to use the system. After password authentication, firewalls are the second most viewed countermeasure. That is, 65% of respondents use firewalls as a security countermeasure (Joutsen, 1999).

On the other hand, since firewalls are products of technology, they have antidotes too, such as “password sniffer”, or “password breaker” programs. Further, computer criminals can develop some creative programs that can penetrate firewalls. In addition, firewalls are relatively expensive in comparison with other technological prevention tools.

The advantages of firewalls are: 1) Firewalls can protect a system from attacks, 2) Firewalls can compensate for other security problems in the system, such as file sharing without passwords, and 3) Firewalls can protect the system from trojan horses (Denial of Service, 2000)

The disadvantages of firewalls are: 1) Personal firewalls (firewalls running on personal computers) cannot prevent serious attacks against the computer, 2) Firewalls cannot find or remove viruses, and 3) Firewalls are confusing to many people, and they take time to set them up and run them.

Firewalls are not the ultimate solution, but they can be used as a first line of defense against external computer criminals.

Encryption Software

Encryption is the transformation of original data ('plain text') into a meaningless form ('ciphertext') that others, without the proper decryption tool, cannot decipher (Newburger, 1999). Both sender and receiver of data use compatible passwords ('keys') to encrypt and decrypt (Newburger, 1999). If used effectively, encryption can reduce the incidents of computer crime and specifically intellectual property theft. Even if the file or data are accessed, they cannot be interpreted without the appropriate decryption mechanism.

However, like every other technological innovation, encryption has some shortcomings. Ever-advancing computer technology makes it easier to crack encryption codes. For instance, in 1977, it was predicted that RSA-129, a popular encryption algorithm, would be almost impossible to crack (in 40 quadrillion years). In 1994, 600 Internet users cracked it (Carter & Katz, 1996).

There is also much debate on the regulation of encryption, which hampers the use of encryption programs. This debate focused on control between the private and public sectors. Government wants to regulate encryption, and increase techniques to gather intelligence, whereas the private sector would like to manage encryption to increase privacy and protection of data (Aldrich, 2000). In any event, if reviewed and updated on a regular basis, using encryption programs may be an efficient way to protect confidential information.

Anti-Virus Programs

Anti-virus programs, also called virus checkers, are another way to protect computer systems. These programs are especially important for individual personal computer users. Because of their low cost, an average computer user can afford to have at least one anti-virus program.

The Internet facilitates contact with several other users and systems, and the sharing of files among them. Internet users are exposed to viruses because of this file sharing among Internet users. The World Wide Web is sometimes called "Worldwide Virus Distribution Mechanism" (Ritchey, 1996).

Recently, anti-virus programs moved into a new realm, the entire Internet. These programs began to scan websites and e-mails. Most recently, several harmful computer-related crimes have been viruses distributed over the Internet.

However, viruses do change rapidly. Every day, several new viruses emerge. Therefore, anti-virus programs should be updated frequently to keep pace with the increasing number of viruses. As a result, anti-virus programs offer a relatively cheap means to computer protection.

Governmental Regulations – Laws and Rules

Law is the third approach to protect computer systems. This is not a stand-alone solution. Laws are related to awareness and technology. To increase computer security awareness, laws must be enacted. Without proper laws, some technological tools cannot be used. For instance, recently a major university conducted a study to review the FBI's

Internet-snooping device, which is called Carnivore, and released a report on the findings. This caused a dispute over the legality of this type of application. As a result, the FBI was scrutinized by the news media.

Adequate laws are also required for effective investigation and prosecution of computer crime. The vague language of some laws may impede the application of laws to certain incidents.

In addition to laws, every organization must have a computer security policy to regulate computer system management. Without a well-defined policy, no one would know what to do. Indeed, in case of an incident, it would be chaos.

Coordination and Cooperation

As previously discussed, the United Nations Manual posits several factors to develop coordination and cooperation at the national and international levels (United Nations, 2000). First, information about judicial, legislation, and law enforcement procedures should be exchanged. Second, there should be international cooperation in sentencing—including the prevention of the harboring of computer offenders. Third, laws and policies should be reviewed regularly. Fourth, encourage educational institutions, hardware and software manufacturers, and data processing corporations to offer computer ethics courses. Next, potential victims of computer crime (financial institutions, governmental agencies, etc.) should be knowledgeable about those crimes. Then, there should be universally accepted standards in information systems that facilitate legal information sharing. Next, voluntary security measures could be offered to private sector entities. Next, national computer security policies and rules should be developed. Managers should be informed to develop security measures in their organizations. The public should be educated to increase awareness of the problem. Victims should be encouraged to report incidents. Law enforcement and related personnel should be trained. The laws between cooperative nations should be harmonized. Finally, the balance of human rights and privacy principles while enforcing international laws should be balanced.

Efforts To Increase Enforcement Of Computer Crime Laws

Governmental agencies, private corporations, and public organizations must be informed of the threat of computer crime and its impact on society and national security. New laws and policies should be developed where voids exist. For example, the 1984, and 1986, Computer Fraud and Abuse Acts were seen as inadequate to address the scope of the computer crime problem (Computer Crime, 1997). Without adequate laws, even the best prosecutorial and investigative structure will fail.

Adequate laws must be in place so that agencies may efficiently investigate, prosecute, and sentence computer criminals. Outdated laws should be revised, and new laws that are well designed and incorporate a new technology must be enacted.

Conclusion

This chapter presented solutions for the problems in the identification, investigation, and prosecution of computer-related crime. The solutions are: increasing awareness, increasing deterrence using appropriate technology such as firewalls and encryption, increasing governmental regulations, and increasing coordination and cooperation between agencies. This study sees the human factor is the main source of the problem. Consequently, increasing awareness would be the best solution to the computer crime problem in general.

Next chapter discusses the problems related to computer crime, and their solutions are briefly argued. The necessary steps to address the problem are examined. Ten priority needs are recommended (based on a study sponsored by National Institute of Justice) to better address the computer crime problem

CHAPTER 6

DISCUSSION/CONCLUSION

Review of the Chapters and Basis for Each Chapter

This study discussed computer-related crime in three main areas: computer crime, Internet crime, and cyber terrorism. Lack of an universally accepted definition leads researchers to develop categorizations to cover different types of computer crimes. This study discussed four major areas, and focused on a widely accepted one, which classifies computer crimes in terms of the role that computers play.

To accomplish success, law enforcement agencies must recruit personnel who have the technical and analytical capabilities to conduct computer crime investigations. Without these specialized personnel, police agencies cannot investigate and detect computer crime efficiently and effectively. Acquiring the appropriate people and providing proper training are the first steps in building good investigation and detection teams.

Computer crime detection and investigation are, and will be, impossible without proper equipment. Police agencies must utilize various hardware, software, encryption systems, and support services. Louis J. Freeh (2000) announced that the Congress authorized $80 million to the FBI’s Technical Support Center for four years to acquire needed equipment (Freeh, 2000).

Police agencies store and utilize highly sensitive information on agency computers. Agencies must protect this information from criminal access. This extremely important information may be used against the police and the public, resulting in loss of privacy and lowering the public opinion of police agencies. It is imperative that police be aware of potential problems and issues arising from computer-related crime.

Companies should report incidents to law enforcement officials. It is impossible to understand the size of the problem if we do not know the actual number of incidents. The Federal Bureau of Investigation (FBI) estimates that only 17 percent of the computer crime victims report incidents to law enforcement agencies (Stambaugh et al., 2000).

Computer crime investigations must be conducted thoroughly, and evidence should be collected and secured carefully. Since many computer crimes involve computer networks, investigators should have a good understanding of networks. Further, investigators should be ready to investigate different types of computer systems (e.g., personal computers, mainframes, microcomputers, and client-server systems). Investigators and law enforcement personnel should follow rules of evidence with an important emphasis on safeguarding privacy and individual rights. A recent incident has showed again how important this issue in the successful prosecution of case. A hacker named Maxim stole 300,000 credit card numbers from Internet retailer CD Universe. He first wanted $100,000 from the music retailer for the credit card information he stole. After failing to extort this money, he posted information to a Web site about 25,000 credit cards. Unfortunately, since the chain of custody was not kept properly, and the evidence was not protected, authorities will not be able to prosecute 19-year-old Russian hacker (Maxim) (Brunker & Sullivan, 2000).

In order to combat transnational computer crime, there must be cooperation and consensus among nations to better assess and address computer-related crime. Then, international frameworks must be developed by these nations. The framework must develop and provide well-regulated solutions, mutual cooperation agreements, and possibly new penal codes. For instance, the FBI Legal Attaches in 35 different embassies try to build cooperation among several law enforcement agencies (Gonzalez, 2000). Moreover, to enhance the security of information systems, internationally agreed upon security countermeasures should be used. Without international coordination, the computer crime problem can have a detrimental impact on the economies of all nations. Cooperation within nations is another necessity for success in addressing computer-related crime. Private industry and governments should work together to better detect, investigate, and prevent computer-related crime.

Even though most computer-related crime types are traditional in nature and committed only in a new manner (facilitated by computers), there are some unique crimes to cyberspace (e.g. cyber stalking, denial of service attacks). Therefore, a primary action for government should be focused on adapting existing policies and laws to address these new types of crimes.

There must be a strong cooperation and coordination among law enforcement agencies at the international level, and a framework must be developed to better assess and evaluate computer-related crime and investigative technique.

The jurisdiction issue should be solved by clearly defining responsibilities, and explaining how and when cooperation and information sharing will be conducted. Additionally, direct access to information across national borders must be provided for evidentiary purposes.

This study emphasizes recruiting computer literate personnel, training those personnel on a regular basis, and supplying with proper equipment. For investigation, instutions should focus on human factor. This research sees the human error is the main cause of computer crime incidents. To prevent these incidents, increasing awareness is seen as a major preventive counter measure.

Minimizing vulnerabilities (using cabinets, alarms, and drive lockers), target hardening (increasing the barriers, physically separating computer system rooms, and controlling circulation of personnel), developing security policies (selecting good passwords, and backing up systems regularly), and using technological countermeasures (using anti-virus software, and firewalls) are some actions that every organization can perform. Weaknesses, or vulnerabilities of computers, computer systems, and software programs attract criminals. Computer criminals and hackers exploit these weaknesses to achieve their crimes. Even our most secure agencies (NASA, Pentagon, FBI) have become victim to such criminal attacks.

This study explained several problems of computer crime related to the criminal justice system. Of these problems, lack of adequate training is the top problem of law enforcement. Lack of security awareness is the most important problem of investigators and prosecutors. In addition, difficulty of detecting computer crime incidents makes the problem worse.

This study offered solutions to these problems. Increasing awareness is the ultimate solution. However, use of technology makes difficult to perpetrate crime. Among the technology prevention countermeasures, password authentication is the easiest to develop. Moreover, anti-virus programs and firewalls should be used to protect systems. Further, if available encryption software can be used to better protect systems and information.

Recommendations

This study offers several recommendations which are increasing public awareness, structuring a computer crime unit and management assistance to this unit, updating laws, providing proper training, increasing data and reporting, cooperation between public and private sectors, and supplying proper equipment.

Increasing Public Awareness: General public, appointed and elected officials, the entire criminal justice community, and the private sector should be informed about the amount, importance, and impact of the computer-related crime. Many people are unaware about the seriousness of the problem. Being unaware of the extent of the problem results in lack of actions. As this study indicated, human error is the main cause of the computer crime incidents. Apparently, human factor could be overcomed by increasing awareness and developing a good security conscious culture.

Structuring a computer crime unit and management assistance to this unit: According to size and resources of agencies, law enforcement agencies should establish a computer crime unit. The duties of this dedicated unit should be clearly documented, and experiences of these units should be shared among agencies. Management should provide full support to computer crime units. Inadequate support of management results in awareness issues among employees.

Updating laws: Federal and state computer crime statutes must be updated regularly to keep pace with the advances in computer industry. Without effective and uniform laws, the problem cannot be addressed.

Providing proper training: Law enforcement personnel, police and private investigators, prosecutors, and judges should get appropriate training on a regular basis. Training assists individuals and institutions to keep up with the advances in the computer industry. To adequately address the computer crime problem, individuals should have information about the new technology. Training provides opoortunity to individuals to learn the ever-updating technology.

Increasing data and reporting: In order to assess and address the computer-related crime problem, more comprehensive information is needed. Without detailed information, it is difficult to depict the trends in computer-related crime.

Cooperation between public and private sectors: Neither the criminal justice system nor the provate sector can address the computer crime problem alone. Entire criminal justice system (law enforcement personnel, prosecutors, and judges) needs support of high-tech industry. Cooperation and support can provide investigators, prosecutors, and judges proper training programs, and equipment. Moreover, this cooperation may encourage institutions to report computer crime incidents.

Supplying proper equipment: State and local law enforcement agencies need investigative tools to conduct effective investigations. Without proper forensic tools most computer-related crime cannot be investigated thoroughly.

Computer crime cannot be controlled by traditional methods alone. Indeed, using new technology and public awareness are two important prevention tools. The use of technology to prevent computer crime needs to be expanded. Furthermore, a more security conscious culture must be developed and awareness of the problem must be enhanced. Computer crime certainly represents one of the greatest challenges to the criminal justice system in the 21st century.

Future Research

Investigators, prosecutors, and forensic specialists need highly specialized information to combat computer-related crime. The Federal Government, state governments, and universities must provide opportunities to perform research, and results of these studies should be published. Researchers may focus on how to establish state of the art training facilities, and how to develop training courses. More research should be done in the area of law enforcement response to computer crime. Specifically, new research is needed in equipping law enforcement.

APPENDIX

DEFINITIONS

Computer: “an electronic device for performing high-speed arithmetic and logical operations” (Icove et al., 1995).

Computer Abuse: “The misuse, alteration, disruption, or destruction of data processing resources” (Icove et al., 1995).

Computer Crime: “Crime in which the perpetuator uses special knowledge of computer technology” (Parker, 1998).

Computer Fraud: “Computer-related crime involving deliberate misrepresentation, alteration, or disclosure of data in order to obtain something of value (usually for monetary gain)” (Icove et al., 1995).

Computer Peripheral: “Any part of a computer other than the CPU or working memory, i.e. disks, keyboards, monitors, mice, printers, scanners, tape drives, microphones, speakers, and cameras” (Foldoc, 2000).

Computer-Related Crime: “Any illegal act for which knowledge of computer technology is involved for its investigation, perpetration, or prosecution” (Icove et al., 1995).

Cybercrime: “Crime in which the perpetuator uses special knowledge of cyberspace” (Parker, 1998).

Cyberspace: “The virtual universe, created by online human computer interaction, where physical actions are encompassed by electronic actions” (Department of Justice, 1999). William Gibson introduced this term in 1984 in his novel, Neuromancer.

Data: “A formalized representation of facts or concepts suitable for communication, interpretation, or processing by people or automated means” (Federal Guidelines, 2000).

Documentation: “Documents that describe technical specifications for computer-related products and how to use hardware components and/or software applications” (Federal Guidelines, 2000).

Encryption: “The transformation of original text (called plaintext) into unintelligible text (called ciphertext)” (Icove et al., 1995).

Fax Peripheral: “A device, normally inserted as an internal card, that allows the computer to function as a fax machine (an abbreviation of ‘facsimile’)” (Federal Guidelines, 2000).

Hacker: “A computer enthusiast who is especially proficient; also, a person who experiments with or explores the contents of computers using unorthodox methods” (Parker, 1998).

Hardware: “The physical components or equipment that make up a computer system” (Federal Guidelines, 2000).

Input/Output (I/O) Device: “A piece of equipment which sends data to, or receives data from, a computer. Keyboards, monitors, and printers are all common I/O devices” (Federal Guidelines, 2000).

Modem: “A device (‘modulate/demodulate’), which allows one computer to communicate with another computer, normally over standard telephone lines” (Federal Guidelines, 2000).

Network: “A system of interconnected computer systems and terminals” (Federal Guidelines, 2000).

Software: “The programs or instructions that tell a computer what to do” (Federal Guidelines, 2000).

System Administrator: “The individual responsible for assuring that the computer network is functioning properly. He is often responsible for computer security as well” (Federal Guidelines, 2000).

REFERENCES

Adamski, A. (1997). R. Scherpenzeel, G. Quirchmayr (Eds.). Legal and Security Aspects of Information Management. United Nations Crime and Justice Information Network: Providing Information to and from Developing Countries, A Resouce Book, Seoul, The Hage, Vienna, Summer 1997.

_________. (1998, December). Crime Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Unpublished Paper Presented to the Proceedings of the VI European Colloquium on Crime and Criminal Policy. Helsinki, Finland.

Akers, R.L. (1985). Deviant Behavior: A Social Learning Approach. (3d ed.). Belmont, CA: Wadsworth.

Aldrich, R.W. (2000, April). Cyberterrorism and Computer Crime Issues: Issues Surrounding the Establsihment of an International Legal Regime. A Paper Presented to the U.S. Air Force Institute for National Security Studies (INSS). U.S. Air Force Academy, CO: U.S. Air Force Institute for National Security Studies.

Allen, B. (1977, May). The Biggest Computer Frauds: Lessons for CPAs. Journal of Accountancy,52-62.

Allen, J, Alberts, C., & Behrens, S. (2000, October). Improving the Security of Networked Systems. [online]. Available:http://www.stsc.hill.af.mil/crosstalk/2000/oct/allen.asp. (2001, January 4).

Barrett, N. (1997). Digital Crime: Policing the Cybernation. London: Kogan Page, Ltd.

Benjamin, R., Gladman, B., & Rundell, B. (1998). Protecting IT Systems from Cyber Crime. The Computer Journal, 41(7): 429-443.

Bequai, A. (1983). How to Prevent Computer Crime. New York: John Wiley & Sons, Inc.

Bologna, J. (1993). Handbook on Corporate Fraud. Stoneham, MA: Butterworth-Heinemann.

Broad, W. J. (2000, April 15). Files in Question in Los Alamos Case Were Reclassified. [online]. Available: http://www.fas.org/sgp/news/2000/04/nyt041500.html. (2000, December 21).

Brunker, M., & Sullivan, B. (2000, June 8). CD Universe Evidence Compromised. [online]. Available: http://www.zdnet.com/zdnn/stories/ news/0,4586,2584330,00.html. (2000, December 20).

Caeti, T. J. (2001). Pornography-Child. In Encyclopedia of Criminology and Deviant Behavior (Vol 3). Bryant, C. D. (ed.). Philadelphia, PA: Brunner-Routledge.

Cain, W., Fousek, L., Kim, M., Levitt, B., & Pearson, M. (1999, March 16). Computer Crime: The Wave of the Future. [online]. Available: http://cs-eduaction. stanford.edu /class/cs201/projects/computer-crime/intro.html. (2000, March 20).

Carter, David L. (1995, July). Computer Crime Categories. FBI: Law Enforcement Bulletin, 64(7), 21-26.

Carter, D. L., Katz, A. J. (1996). Computer Crime: An Emerging Challenge for

Law Enforcement. FBI: Law Enforcement Bulletin, 65(12),1-9.

Carter, D. L., & Katz, A. J. (2000). Computer Crime: A Forecast of Emerging Trends. Unpublished Paper Presented at the Annual Meeting of the Academy of Criminal Justice Sciences, New Orleans, LA.

Clarke, R., Dempsey, G., & O'Connor, R.F. (1998, February 16-17). Technological Aspects of Internet Crime Prevention. Presented to the Australian Institute for Criminology's Conference on "Internet Crime." [online]. Available: http://www.anu.edu.au/People/Roger.Clarke/II/IcrimPrev.html. (2001, January 21).

Cohen, A. (1997, November 10). Battling the Cyber-Terrorist: Internal Breaches Pose Greatest Threat. [online]. New York Law Journal. Available: http://www.nylj.com/tech/111097t1.html. (2000, June 28).

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: a Routine Activity Approach. American Sociological Review, 44: 588-608.

Collin, C.C. (1998). CyberTerrorism From Virtual Darkness: New Weapons in a Timeless Battle. [online]. Available: http://www.nici.org/Research/Pubs/98-5.htm. (2000, March 10).

Computer Crime Investigation and Computer Forensics. (1997, Summer). Information Systems Security, 6(2): 56-80.

Conly, C. H. (1989). Organizing for Computer Crime Investigation and Prosecution. Washington, D.C.: U.S. Department of Justice, National Institute of Justice.

Cox, D.T. (1999, Summer). Litigating Child Pornography and Obscenity Cases in the Internet Age. Journal of Technology Law and Policy, 4(2). [online-serial].

Available: http://grove.ufl.edu/~tachlaw/4-2/cox.html. (2000, December 4).

Cyber Crime Conference. (2000, September 28-29). [online]. Available: http://www.iqpc.com. (2001, January 20).

Deborah, R., & Gangemi G.T. (1994). Computer Security. O'Reilly & Associates.

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

Denial of Service or "Nuke" Attacks. (2000, April 10). [online]. Available: http://www.irchelp.org/irchelp/nuke. (2001, January 20).

Doney, L. D. (1998, May-June). The Growing Threat of Computer Crime in Small Businesses. Business Horizons, 41(3): 81-86.

Doty, P. (1982). The Role of the Evaluation Research Broker. Saxe, L, & Kroetz, D. (Eds). New Directions for Program Evaluation (No.14). San Fransisco: Jossey-Bass.

Dowland, P.S., Furnell, S.M., Illingworth, H.M, & Reynolds, P.L. (1999). Computer Crime and Abuse: A Survey of Public Attitudes and Awareness. Computers and Security, 18(8): 715-726.

The E-mail Abuse FAQ. (1998, June 25). [online]. Available: http://members.aol.com/emailfaq/emailfaq.html. (2001, January 20).

E-mail Spamming Countermeasures. (1997, November 25). [online]. Available: http://ciac.llnl.gov/ciac/bulletins/I-005c.shtml. (2001, January 20).

Farmer, D. (1996, December 18). Security Survey of Key Internet Hosts and Various Semi-Relevant Reflections. [online]. Available: http://www.troule.org/survey.

(2000, March 10).

Federal Guidelines For Searching And Seizing Computers. (2000, April 24). [online]. Available: http://www.usdoj.gov/criminal/cybercrime/search_docs/ toc.htm. (2000, June 30).

Flusche, K.J. (1998). Computer Crime and Analysis of Computer Evidence: It Ain't Just Hackers and Phreakers Anymore! Information Systems Security, 7(1): 27-33.

Foldoc Computing Dictionary. (2000, July 18). [online]. Available: http://foldoc.doc.ic.ac.uk/foldoc/index.html. (2001, January 27).

Freeh, L. J. (2000. March 28). Statement for the Record of Louis J. Freeh. [online]. Available: http://www.fbi.gov/pressrm/congress/congress00/ cyber032800.htm. (2000, October 16).

Gonzalez, G. (2000. April 21). Statement for the Record of Guadalupe Gonzalez. [online]. Available: http://www.fbi.gov/pressrm/congress/congress00/ gonza042100.htm. (2000, October 16).

Goodman, M.D. (1997, Summer). Why the Police Just Don't Care about Computer Crime. Harvard Journal of Law and Technology, 10(3): 465-494.

Government Prepares to Battle Cybercrime. (2000, Feb 17). [online]. Available: http://www1.pcworld.com/pcwtoday/article/0,1510,15337,00.html. (2000, March 2).

Government Sees Cyber Attacks as Disruption of Commerce. (2000, Feb 9). [online]. Available: http://cnn.com/2000/US/02/09/cyber.attacks.fbi.02. (2000, March 20).

Harrison, A. (2000, February 14). FBI Issues Software to Help Detect Web Attacks. Computerworld, 34(7): 14-16.

Hatcher, M., McDannell, J, & Ostfeld, S. (1999). Computer Crimes. American Criminal Law Review, 36(3): 397-444.

Hoaxbusters: A Public Service of the CIAC Team and the U.S. Department of Energy. [online]. Available:http://hoaxbusters.ciac.org. (2001, January 20).

Hollinger, R.C. (1992). "Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access." Security Journal, 2(1):2-12.

Hollinger, R.C., & Lanza-Kaduce, L. (1998). The Process of Criminalization: The Case of Computer Crime Laws. Criminology, 26: 101-126.

Hosmer, C., Feldman, J., & Giordano. J. (no date). Advancing Crime Scene Computer Forensic Techniques. [online]. Available: http://www.wetstonetech.com/crime.htm. (2000, November, 20).

Husman, H. (2000, October 28). Introduction to Denial of Service. [online]. Available: http://www.di.uoa.gr/~stud1085/info/denial_of_service.html. (2001, January 20).

Icove, D., Seger, K., & Vonstorch, W. (1995). Computer Crime: A Crime Fighter's Handbook. Sebastopol, CA: O'Reilly & Associates, Inc.

Icove, D. J. (1997). Collaring the Cybercrook: An Investigator's View. IEEE Spectrum, 34(6): 31-36.

Joutsen, M. (Ed). (1999). Five Issues in European Criminal Justice: Corruption, Women in the Criminal Justice System, Criminal Policy Indicators, Community Crime Prevention, and Computer Crime. Helsinki, Finland: Proceedings of the VI European Coloquium on Crime and Criminal Policy.

Kizza, J. M. (1994). Combating Computer Crimes: A Long Term Strategy. [online]. ACM Transactions on Computer Systems. Available: http://www.acm.org/ pubs/articles/ proceedings/cas/199544/p166-kizza/p166-kizza.pdf. (2000, October 4).

Kovacich, G.L., & Boni, W.C. (2000). High-Technology Crime Investigator's Handbook: Working in the Global Information Environment. Boston: Butterworth-Heinemann.

Laquer, Walter. (1987). The Age of Terrorism. Boston: Little, Brown.

Levesque, N. (2000). Cybercrime Dot Com. [online].

Lohr, S. (1997). Be Paranoid. Hackers Are Out to Get You. New York Times Ondisk, AccessNo. 13503819970317.

Majchrzak, A. (1984). Methods For Policy Research. Newbury Park, CA: SAGE Publications, Inc.

Mann, D., & Sutton, M. (1998). Net Crime: More Change in the Organisation of Thieving. British Journal of Criminology, 38(2):201-229.

McKee, A. (no date). Computer Crime: The Unmet Challenge to Law Enforcement. [online]. Available: http://ocean.otr.usm.edu/~ajmckee/ computercrime.html. (2000, February 12).

Mendell, R. L. (1998). Investigating Computer Crime: A Primer for Security Managers. Springfield, Illinois: Charles C. Thomas Publisher, Ltd.

Milton, P. (1997, March 5). FBI Director Calls For Effort to Fight Growing Danger of Computer Crime. [online]. Available: http://www.capitaljournal.com/intsource/030597/fbi.html. (2000, June 28).

National Consumer's League (NCL). (1999, Feb 16). NCL's Internet fraud watch. [online]. Available: http://www.fraud.org/internet/99final.htm. (2000, March 10).

Newburger, C. (1999). Encryption. [online]. Available:http://www.cybercrimes.net/Cryptography/Artickes/NewburgerPaper.html. (2000, December 12).

Office of Juvenile Justice and Delinquency Prevention. (1999, May 7). Internet Crimes Against Children Task Force Program. [online]. Available:http://ojjdp.ncjrs.org/fedreg/icac.pdf. (2001, January 20).

Parker, D. B. (1976). Crime By Computer. New York: Scribner.

__________. (1981). Computer Security Management. Reston, Virgnia: Reston Publishing Company, Inc.

__________. (1981). How Much Computer Abuse is There? Menlo park, CA: SRI International.

__________. (1989). Computer Crime: Criminal Justice Resource Manual. Washington D.C.: National Institute of Justice.

__________. (1998). Fighting Computer Crime: A New Framework for Protecting Information. New York: John Wiley & Sons, Inc.

Perry, R.L. 1986. Computer Crime. New York: Franklin Watts.

Peters, W. T. M. (1997, October 20). Further Study In White Collar Crime: Hacking & Criminal Hacking - Computer Crime - Kevin Mitnick - Regulation and Control of White Collar Computer Crime. Available: http://www.ozemail. com.au/~wtmp/wcc.html. (2000, December 21).

Pollitt, M. (no date). Cyberterrorism – fact or fancy? [online]. Available: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html. (2000, March 12).

Power, R. (1997). CSI/FBI 1999 Computer Crime and Security Survey. Computer Security Journal, 13(2), 77-86.

_______. (1999). CSI/FBI 1999 Computer Crime and Security Survey. Computer Security Journal, 15(2), 29-45.

_______. (2000). 2000 CSI/FBI Computer Crime and Security Survey. Computer Security Journal, 16(2), 77-86.

Prevent Unauthorized Access. (2000, July 17). [online]. Available:http://www. concordia.edu.ca. (2001, january 20).

Ritchey, B. D. (1996, September 23). Computer Crimes and How to Prevent them. [online]. Available: http://disc.cba.uh.edu/~rhirsch/fall96/barba.htm. (2000, February 11).

Rosenberg, R. S. (1997). The Social Impact of Computers. New York: Academic Press.

Rosenblatt, K. (1990). Deterring Computer Crime. Technology Review, 93(2):35-40.

Sandberg, J. (2000, Feb 21). Holes in the Net. [online]. Available:

http://newsweek.co/nw-srv/printed/us/st/a16375-2000feb13.htm. (2000, March 20).

Schwartau, W. (1996). Information Warfare. (2nd ed.). New York: Thunder's Mouth Press.

Security in Cyberspace: Statement of U.S Senate Permanent Subcommittee on Investigations. (1996, June 5). [online]. Available:http://www.fas.org/irp/1996_hr/index.html. (2000, May 12).

Sessions, W. S. (1991). Computer Crimes: An Escalating Crime Trend. FBI Law Enforcement Bulletin, 60(2): 12-19.

Shap, D. (1993). Search and Seizure of Canadian Computer Environments. [online]. Available:http://www.catalaw.com/logic/docs/ds-srch.htm. (2000, December 11).

Skinner, W.F., & Fream, A.M. (1997). A Social Learning Theory Analysis of Computer Crime Among College Students. Journal of Research in Crime and Delinquency, 34(4): 495-519.

Sorkin, D. E. (2001). Spam Laws. [online]. Available: http://www.spamlaws.com. (2001, January 27).

Stambaugh, H., Beaupre, D., Icove, D.J., Baker, R., Cassaday, W., & Williams, W.P. (2000, August). State and Local Law Enforcement Needs to Combat Electronic Crime. [online-serial]. National Institute of Justice. Available:http://www.ojp.usdoj.gov/nij. (2000, November 12).

Stephenson, P. (2000). Investigating Computer-related Crime. Boca Raton, FL: CRC Press LLC.

Steele, G.T. & Pearson, A.L. (1981). Case for Training in Computer Crime Investigation. Law Enforcement Data Processing Symposium-Fifth Annual, 219-231.

Strothcamp, D.A. (1998, April 17). [online]. Fraud and computer crime. Available: http://www.csuohio.edu/accounts/Strothcamp/TOPIC07/tsld001.htm. (2000, April 1).

Talwar, S.S.P. (1999, February 14). Inaugural Address at the National Seminar on Computer-related Crime. [online]. Available:http://www.securities.ru/ Public/Public98/RBI/Speech/Speech990224-1.html. (2000, December 4).

Taylor, R. W. (2000). Computer Crime, In Swanson, C. R., Chamelin, N.C., & Territo, L. (Eds.), Criminal Investigation (pp.511-536). Boston, MA: McGraw-Hill Companies, Inc.

Teen Hacker Denies Involvement in Crippling Internet Assault. (2000, March 3). [online]. Available: http://www.foxmarketwire.com/wires/0302/f_ap_0302_44.sml. (2000, March 20).

Tenhunen, M. (1994). Updating Computer Crime and Information Security Strategies. Paper presented to Kriminalistik und Forensische Wissenshcaften, Internationale Schriftenreihe.

United Nations. (2000, April 25). International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime. (25 Apr, 2000). [online]. Available: http://www.uncjin.org/Documents/irpc4344.pdf. (2000, May 12).

U.S. Programmer Charged with Computer Sabotage. (2000, Feb 17). [online]. Available: http://www.zdnet.com/zdnn/content/reut/0217/285787.html. (2000, March 19).

Wyatt, J. E., & Farrar, P. H. (1994). Cultural Perspectives of Computer Security. ACM Transactions on computer systems, 204-207.

Winkler, I. (1997). Corporate Espionage. Prima Publishing.

Yin, R. (1994). Case Study Research: Design and Methods (2nd Ed). Thousand Oaks, CA: Sage Publishing.