Journal of International Information Management

Volume 6 | Issue 2 Article 6

1997

Computer crimes: Taxonomy and prevention strategies

Santosh S. Venkatraman
New Mexico State University

Computer crimes: Taxonomy and prevention strategies

Santosh S. Venkatraman
New Mexico State University

ABSTRACT

Computer and communications networks have greatly enhanced the effectiveness and efficiencies of organizations. They have, however, also created an opportunity for computer criminals. Computer crimes are committed for many reasons: 1) revenge by disgruntled employees, 2) desire for a challenge, 3) to cause mischief, and 4) money. In order to better understand the nature of computer crimes, a comprehensive taxonomy of computer crimes is developed in this paper. Strategies to effectively combat the various computer crimes are then presented. It is hoped that the information provided in this paper makes the readers more knowledgeable on this important topic and motivates them to deploy strategies to secure their organizational information resource from computer criminals.

INTRODUCTION

Computer crimes and frauds are an economic drain (to the tune of a few billion dollars a year) on society. It is especially hard to arrive at a good estimate of the extent of computer crimes because many companies do not report illegal activity for fear of public discredit or notoriety. Another problem with computer crime is that it leaves behind very little evidence, as an "intelligent" criminal can destroy any evidence. The FBI estimates that only 1% of all computer crimes are detected, of which only 7% get reported! Even more dismal is that only 3% of the reported cases end in jail sentences. Clearly, society, managers in organizations, and the current legal system are badly prepared to handle computer crime. A key factor in deterring computer crimes is education - unless we are aware of what computer crime is and how it is perpetrated, we cannot do much to stop it.

A computer crime is "any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution" (Reynolds, 1995). Computer crimes can be committed by individuals outside an organization (*external* crimes) or by employees within the organization (*internal* crimes). The majority of computer crimes are perpetrated by disgruntled employees trying to "get back" at their employers or by external criminals for "money." Information and computers are often abused for either making money (fraudulent electronic fund transfers, industrial espionage, etc.) or for avoiding paying money (software piracy, using employers computing facility for personal reasons, etc.).

The purpose of this paper is to educate the reader on computer crimes and suggest strategies for their prevention. Section 2 introduces the reader to computer crimes by presenting some specific instances and motives of computer criminals. In section 3, a taxonomy of all possible computer crimes is presented, along with various techniques used within each category. Various strategies for preventing or minimizing computer crimes are then presented in section 4. Section 5 summarizes and concludes the paper.

INSTANCES AND MOTIVES OF COMPUTER CRIMES

Hackers are probably the highest profile perpetrators of external computer crimes, even though only 3% of computer crimes are "external." Computer hacking began in the 1970s, when the motivating factor for most early hackers was the *challenge of breaking into a system.* They could have very easily stolen money, information, software, and hardware, but the "true" hacker chose not to (Roush, 1995).

As computers became more prevalent in the 1980s, the "new" hackers took the opportunity to exploit computer systems for personal gain. The new breed of hackers have different factors that motivate them, primarily *mischief and greed.* A 1992 study by USA Research, Inc., a technology consulting firm, found that the number of hacking incidents involving U. S. companies more than doubled from 339,000 in 1989 to 684,000 in 1991 (Roush, 1995). The potential harm hackers can cause has increased because of the proliferation of computers and computer networks in many countries. Computer networks are very accessible to hackers because of the many potential entry points. Computer crimes involving hackers range from the "harmless browser" to the international gangs of criminals who steal data, destroy computer systems by planting viruses, and divert electronic funds (Bird, 1994).

Industrial espionage is another common motive in computer crimes. It involves the theft of customer lists, sales know-how, and research and development (R & D) plans. Many hackers who specialize in industrial espionage are becoming sophisticated marketers, labeling themselves as "information brokers." They obtain information about international companies, institutions, and individuals for a fee. For example, a UK-based shipping company paid a hacker to infiltrate a rival company's database and steal competitive information including business strategy, customer lists, and tariff deals. Hackers are also well known for crimes involving the diversion of funds. A team in Switzerland, for instance, hacked into a bank account of a wealthy individual to discover how his money was transferred and then diverted 1 million pounds (Bird, 1994).

The Internet is now presenting new possibilities for hackers to infiltrate computer systems because it is increasingly being used by organizations and individuals to exchange information, place orders, and make payments. William Cheswick, a network-security specialist at AT&T Bell Labs, said, "the Internet is like a vault with a screen door on the back." International Data Corp. in Framingham, Massachusetts, estimates that the number of Internet users will grow from 38 million in 1994 to about 200 million in 1999. Also, many companies will be offering a diverse line of products via the Internet, particularly on the World Wide Web - the fastest growing sites on the Internet (Markoff, 1995).

Many computer security experts point out that the original intent of the Internet was not for commerce but for academic researchers to exchange information conveniently. Therefore, commerce on the Internet is a very vulnerable target, unless appropriate safety measures are taken. The recent arrest of an "infamous" hacker turned up nearly 20,000 credit card numbers belonging to subscribers of Netcome, an Internet-access provider. An ironic example of the Internet's occurred on Christmas day, 1994. The "victim," Tsutomu Shimomura, happened to be a world renowned computer security expert, who has consulted for the FBI, the U. S. Air Force, the National Security Agency, and also for private companies including Sun Microsystems. The hacker used a sophisticated break-in technique known as "protocol spoofing" to steal personal files and thousands of e-mail messages (Markoff, 1995). Protocol spoofing involves fooling the network into believing the message is coming from an authorized person, and hence grant entry. The Christmas day attack provided a wake-up call to other computer users (universities, government, business) that the Internet was not very secure - if it could happen to a security expert, then it could happen to anyone.

Computer security measures, unfortunately, are reactive and not proactive. Even though the Protocol spoofing technique was published in the 1980s, it wasn't until recently that the Internet protocols have been modified to prevent its occurrence (Wallich, 1995). Another way hackers have attacked the Internet is through "password sniffing." The technique involves hiding tiny programs on a network which are instructed to record log-ons and passwords and then store them in a secret file. The Computer Emergency Response Team (CERT) reports that as many as 10,000 Internet sites were targeted by "password sniffing" in 1994 (Russell & Zwickey, 1995).

Computer viruses are another serious problem organizations and individuals encounter. The typical virus designer is a young, intelligent individual who is using his/her talents to design dangerous computer programs. An infamous virus case involved a Cornell University student, who planted a virus on the ARPAnet network (now the Internet) and caused 6000 computers worldwide to cease operating. Although some viruses are created by hackers, most are placed on computer systems by authorized personnel.

Software piracy, an often overlooked computer crime, is the illegal copying and using of copyrighted software. The Software Publishers Association (SPA) represents nearly 500 personal computer software publishers and is attempting to mitigate the problem by creating awareness of this illegal activity. Unlike theft of physical property, the theft of copyrighted "intellectual property" (software) is not taken seriously by many countries or individuals. Many software companies such as Microsoft Corporation lose billions of dollars of revenue due to software piracy outside the U.S.A. and are trying very hard to educate people and prosecute offenders.

The *theft* of physical computer equipment, especially laptop computers, is on the rise. In Richards (1996), it is reported that 2000 laptops are stolen every day, of which about 10% were stolen at airports. In addition to losing the hardware, important corporate and personal data is also lost during such thefts. The majority of laptop thefts can be prevented if owners are alert. Another solution is to use a software (CompuTrace) offered by Absolute Software of Vancouver, British Columbia. The software, which is installed in the laptop's hard disk, accesses the modem without the thief knowing about it and calls Absolute Software's center from anywhere in North America once a week. The software is free and the monitoring service costs $60 a year.

TAXONOMY OF COMPUTER CRIMES

In the previous section, several instances of crimes were illustrated. However, to formally understand computer crimes, a taxonomy is needed. The taxonomy can be used by managers to determine which type of crimes are most likely in their organizations and then deploy appropriate security measures to minimize or eliminate those crimes. We identify ten different types of computer crimes, which we discuss below.

Altering Data

Organization's records are altered for either personal gains or malicious reasons. There are different techniques in the literature such as *data diddling,* which is changing data/information even before it is entered into a system; and *data leakage,* which involves erasing data records, files, or even databases without leaving a trace (sometimes known as *zapping*) as well. Examples:

- A doctor in a hospital could change patient records so that he/she will not be held accountable for a wrong procedure (personal gains, data diddling).
- A disgruntled employee can delete an entire customer file in the database so that the organization will get into trouble (malicious reason, data leakage/zapping).

Altering Software/Programs

Organization's software are altered for either personal gains or malicious reasons. Different techniques in the literature exist, such as the Trojan Horse, Trapdoor, Salami Slicing, and Zapping. A *Trojan horse* is a program that appears to do one thing while doing something very different. A *Trapdoor* is writing programs with a "secret" entry point into the same or another program so that one can gain entry and alter code after it has been verified by someone else. *Salami slicing* is the writing of programs that secretly "slice" off small amounts of money from accounts/transactions and divert it to a hidden account. Another technique, known as *Zapping,* is the erasing of programs (or part of it) without a trace. Examples:

- A bank manager slicing of a penny from some accounts every time "interest" is credited at the end of each month (personal gains, Salami slicing).
- An information systems department employee who has just been fired by the company can change several programs (malicious reason, Trojan horse).

Stealing Data

This is the act of stealing data (unlike physical property, stealing data might mean just "copying" it, or "printing" it - the original data could still be intact), usually for personal gains. For example, confidential company data can be "sold" to a competitor or even used to blackmail the company.

Software Piracy

This is the act of stealing software. Like data, the theft of software typically involves the illegal "copying" and "using" of software for personal gains. The software could be a "custom" company software, for which a lot of resources had been devoted - the software could then be sold to a competitor. The more common occurrence is for the thief to use the stolen software personally without paying for it. For example, if an employee steals a licensed copy of Microsoft Word from his/her office computer and installs it at home, then she is depriving Microsoft Corporation of the revenue for that product.

Theft of Computer Time

This involves the use of a computer for which the user is not authorized. A private engineering consultant connecting via network to a computer at an engineering organization while pretending to be one of their employees would be considered a "computer time thief." The above technique is known as *masquerading,* where the perpetrator accesses a system by pretending to be an authorized user. An employee (or a friend or spouse) using his office computer for typing up a personal letter, buying stocks on the Internet using an "on-line broker," or using e-mail to keep in touch with personal friends could also be guilty of this crime as the employee is using office equipment (and time) for personal gains. This could potentially be a serious problem for employers of telecommuters, who have been provided office computers at home.

Unauthorized Use of Computer Peripherals

This is related to stealing computer time but involves unauthorized using of computer peripherals such as fax modems, printers (toner and paper), scanners, and plotters. Employees, and their family and friends, are often perpetrators of this kind of crime.

Dispersing Harmful Software

This crime involves a person writing harmful programs for typically malicious reasons. The most common occurrence here is the writing and distribution of *computer viruses.* A computer virus as defined by the FBI is "any computer program that is not readily discernible to the user and which has the capacity to infect other computer systems by recreating itself unpredictably or causing some other specific action under predetermined circumstances." The damage ranges from a harmless annoyance to the massive shutdown of systems and destruction of data. Cleaning the virus from a large computer system may cost thousands of dollars, and there are strains of viruses that are immune to software vaccines and hence cannot be cleaned from a system (Reynolds, 1995).

Even though viruses are created intentionally, they often pass on to other computers unintentionally. A person who has a virus on his disk may go and use someone else's computer and pass on the virus inadvertently. Also, users may inherit a virus when logging onto a network to receive electronic messages (e-mail) or download files, using a network, from other computers. It is therefore possible for an employee to be guilty of this crime because of negligence (to ensure that there is no virus) or ignorance.

Damaging/Destroying Computing Equipment

This type of crime is typically done for malicious reasons. Typically, a disgruntled employee could smash a monitor, drop a laptop computer on the floor, or cut off network cables in order to "pay back" the employer/boss. In extreme cases, it is conceivable, that an unscrupulous competitor destroys the computer facility of another competitor (in order to disrupt business), but such cases are rare.

Stealing Computers and Peripherals

With the advent of smaller and more powerful computers/peripheral devices, it has become relatively easy to steal entire computer systems. Common targets are printers, monitors, mice, and laptop computers. As mentioned before, 2,000 laptops are stolen every day! The laptop thief is often rewarded with a bonus - the software and data residing on the hard disk of the laptop. Stealing can be done by insiders or outsiders.

Snooping

This involves the unauthorized seeking of confidential information. A curious employer looking through some of his employees' e-mail messages is an example of this crime. Another example could be illegally logging into a remote system and browsing through the various computer files. Several techniques such as wiretapping, eavesdropping, scavenging, and piggybacking have been used for snooping.

Wiretapping or *eavesdropping* is intercepting messages as they flow through communication media such as microwaves, infrared waves, radio-waves, coaxial cables, telephone wires, and fiber optic lines. *Scavenging* involves going through users' electronic trash cans (or real trash cans with hard copies) looking for information (discarded memos, letters, etc.), old versions of data files, discarded e-mail messages, and old versions of computer program files. A surprising amount of information can be gained in this way. *Piggybacking* is the technique of "following" the computer operations of a legitimate user. The piggy-backer is able to see everything the legitimate user is seeing. A piggy-backer can alternatively take over the terminal/PC of a legitimate user who might have "just stepped out for a few minutes."

This section developed a taxonomy of major types of computer crimes. The next section suggests approaches to prevent or minimize these crimes.

CRIME PREVENTION MEASURES

Most computer crimes are committed by individuals within a company, yet they have the least publicity and possibly the least adopted security measures. As computer crimes are a relatively new phenomena, organizations have not adopted adequate measures to control them. Internal control mechanisms, or rather the lack of them, have allowed internal fraud to become a major problem in the global economy. Managers across the globe must clearly understand "how fraud occurs," as well as devise "internal control" mechanisms.

The approach taken here is to identify the weak points in a computer system that allow computer criminals to perpetrate the crimes and then suggest ways to minimize the weaknesses. The five types of security measures are: *procedural controls, physical controls, network access/ transmission controls, data/program access controls, and education.* Information systems security should be a holistic one because the weakest link determines the strength of the entire system - organizations should develop a security strategy around all five measures.

Procedural Controls

Many computer crimes can be prevented if managers and employees realize that data and software are critical organizational assets that need to be managed and guarded. A recent survey done by Ernest and Young of 1,271 executives found that 34% responded that information security was only "somewhat important" (Sandberg, 1994). Top management support is critical to change the corporate culture and view information systems as an important asset. The following policies have been effective deterrents of computer crime.

PC1: *All authorized network users should have user-accounts and passwords that must be changed frequently.* Some measures to make password guessing difficult include (1) users may not repeat their passwords, (2) password should not be a word in a dictionary, and (3) passwords must have at least one numeric character. Another important policy is to *immediately* delete user-accounts of employees/users who have left the organization. Many times, disgruntled ex-employees can wreak havoc using their existing accounts.

PC2: *All important data and programs should be backed up frequently.* This policy ensures that accidental or purposeful alteration or deletion of files will not have any long-term consequences on the firm.

PC3: *Partition responsibilities of important data/software related functions among more than one person.* This ensures that one individual does not have sole authority over an entire important function or resource (software/data), and hence cannot perpetrate a major crime without the cooperation of all the related employees (Senn, 1995).

PC4: *All user activities and transactions be recorded and audited periodically.* This allows management to trace fraudulent activities on the system, which itself is a major deterrent to criminals.

PC5: *Have clear guidelines and policies on the use of office equipment, and articulate the consequences of infractions.* Employers can require that employees not use e-mail, Internet, computers, and peripherals for personal purposes. Software can be purchased and used to monitor and block such activities. Management must also actively discourage software piracy. It is important to ensure that all employees understand and agree to this policy (to prevent lawsuits).

PC6: *All electronically networked partners, such as EDI (Electronic Data Interchange) partners, must have stringent security standards.* This policy is an important, but difficult policy to enforce as it spans over multiple organizations. With globalization and enhanced computer networks, many organizations are turning to "on-line partners" to enhance their efficiency and effectiveness. EDI, for instance, is used by organizations to eliminate paperwork (invoices, purchases orders, order changes, etc.); to exchange business data, and to execute transactions electronically (Corriera, 1989).

If an on-line partner does not implement EDI with proper security measures, then the other partners who do will be compromising their computer systems security - computer criminals could gain access via the weak system/EDI network.

Physical Controls

Once the procedural policies are implemented, the next step is to restrict physical access to unauthorized users. The very presence of these controls serves as an effective deterrent to "unprofessional" or "opportunistic" criminals.

PH1: Organizations should make it difficult for unauthorized users to enter areas containing expensive or "mission critical" devices. Biometric security devices such as fingerprint analyzers, retina scans, and speech analyzers, or even a simple lock and key system can be installed to keep out intruders.

PH2: Install surveillance systems such as remote cameras and monitoring systems (monitored by security personnel), unmanned video camera and recording system, and human security guards.

PH3: Office computers can have a key and lock system to prevent unauthorized users from even operating the system. This is especially true for computers that stand freely on desks in open cubicles (not enclosed offices).

PH4: Laptop users can subscribe to remote monitoring software such as CompuTrace, by Absolute Software (as mentioned in Section 2).

Network Controls

Illegal access to computer systems via computer networks is increasing as more users are joining networks. The goal of network security should be to make it very difficult for unauthorized users to access or use the network but at the same time make it reasonably accessible to legitimate users. A balance has to be achieved in making the network a secure system but also user friendly to legal users. After all, networks are intended for information access, not to shut users off. Measures can be devised to prevent access by unauthorized users, and if that fails, then at least have a record that the network had been tampered with.

NC1: Providing each authorized user with unique user-account-name and password will keep most "casual" intruders out of the network. This should be combined with a policy (PC-5) that passwords be changed often and be difficult to guess. By changing passwords often, old passwords that have leaked out will become ineffective.

NC2: Firewall software can be used to shield an organization's internal network from unauthorized Internet access (Paone, 1995). Firewalls ensure that all traffic from the Internet is inspected and has authorization. The Internet, which was initially designed for free flow of information between users, is an insecure environment for classified or private data. Therefore, the best way to stop the free-flow from affecting an organization's internal network is to block unauthorized Internet messages. Some firewall software even feeds intruders with false data and traces it back to the source (Baig & Carey, 1994). Several companies, such as Secure Computing Corporation, Digital Equipment Corporation, IBM, and Raptor systems, sell firewall software.

NC3: Once a user has logged in to a network (and entered the firewall, if using the Internet), it is still possible that an unauthorized user is impersonating an authorized user, or even that an authorized user is impersonating another authorized user to commit a crime. Besides the Internet, it is also possible to use dial-up remote access to gain access to networks. This too could be a potential entry point for criminals. *Remote security access* technology is used to combat the aforesaid crimes.

Call-Back Security is a mechanism in which a user first connects to a remote computer via modem, which then validates the user's authenticity by disconnecting and reconnecting to the user. The computer calls back the telephone number of the authorized user which has been set up in the system. The call-back feature, hence, minimizes unauthorized users (who might be trying to connect from an unauthorized phone line).

Encryption is the process of garbling messages as they are transmitted across networks. If a criminal is tapping the line or snooping the messages, it will not make any sense. For example, when an encrypted credit card number is sent via a network and intercepted by a criminal, it has no meaning for him. Encryption and *digital signatures* (the equivalent of human "fingerprints") can also be used to authenticate messages-- to catch masqueraders who claim that they are somebody else. Many digital signatures employ the public-key encryption method developed by RSA Data Security Inc. (Baig & Carey, 1994). Many software makers are also licensed to use RSA's technology. RSA Data Security Inc. is currently active in making transactions over the World Wide Web servers secure.

NC4: It is wise to maintain a log of all network sessions. The log can maintain information on "who" logged in from "where" at "what time," and "logged out at what time." Regular auditing of the log can determine the level of network usage as well as help in tracking down unauthorized users.

Data/Program Controls

This level of protection attempts to prevent intruders from gaining access to data and files, and also software controls to keep out intruders, or minimize the effect of crimes.

DC1: Databases and files should have *strict access privileges* so that employees or external intruders do not accidentally or otherwise have information that they should not have. Database designers should take extra precautions when designing data files, and software designers can also restrict access (very easy with operating systems such as UNIX, NeXTstep, etc.) to directories and files. Database designers should also tailor "views" of data files (easy in Relational databases) for users so that users only see fields that they need.

DC2: Screen savers with password protection is a simple but effective way to prevent snooping by internal and external people. In many organizations, one can see the computer or terminal through an open door of an empty office (occupant might have "just stepped out"). This can tempt others to "snoop" or even alter data and software. Having screen savers with passwords (i.e, need a password to get rid of the screen saver) will keep away potential "snoopers."

DC3: Automatic virus scanners can be sued to detect "harmful" software (virus) and exterminate it before it spreads. Many times, users inadvertently transmit viruses when carelessly sharing disks and files (through network).

User Education

Organizational employees should be made aware of computer crimes as only informed employees will eventually use the various prevention controls effectively.

UE1: Regular seminars can be held or bulletins (e-mail and/or hard copy) can be distributed to nurture a "safe" computing environment. Employees should be made to realize that organizational computing resources, including information, are critical for the organization's success, and that top management is making all efforts to ensure the safety of this valuable resource. An informed employee is more likely to make judicious use of the various crime prevention mechanisms described in this paper.

Table 1 summarizes the effectiveness of the various types of controls on computer crimes. Uppercase labels "I" (for internal) and "E" (for external) are used when the control has a *major* impact on preventing computer crimes. Similarly, lower case labels "i" (for internal) and "e" (for external) are used when the control has a *minor* impact on preventing computer crimes.

Table 1. Computer Crime Prevention

	COMPUTER CRIME CATEGORY									
	Altering Data	Altering Software	Stealing Data	Software Piracy	Computer Time Theft	Unauthorized Peripheral Usage	Dispersing Harmful Software	Damaging/ Destroying Computers	Stealing Computers/ Peripherals	Snooping
CONTROLS										
1) Procedural Controls										
PC1 - User Accounts & Passwords	E	E	E	E	E	E	E			E
PC2 - Regular Backup	e,i	e,i	e,i							
PC3 - Partition Responsibilities	I	I	I							
PC4 - User log & auditing	I,E	I,E	I,E		I,E	I,E	I,E			I,E
PC5 - Usage Policies & Punishments				I	I	I	I	i	i	I
PC6 - Standards (External Partners)	E	E	E		E		E			E
2) Physical Controls										
PH1 - Prevent Unauthorized Entry	i,e	i,e	i,e	i,e	i,e	I,e	i,e	I,E	I,E	I,E
PH2 - Surveillance Systems	i,e	e	e	e	e	e		I,E	I,E	i,E
PH3 - Computers with Key and Lock									I,E	
PH4 - Monitoring of Portable Computers									I,E	
3) Network Controls										
NC1 - User Accounts and Passwords	i,E	i,E	i,E	E	E	E	E			E
NC2 - Firewalls	E	E	E	E	E		E			E
NC3 - Remote Access Security	I,E	I,E	I,E	I,E	I,E	i,e	I,E			I,E
NC4 - Network Log	i,e	i,e	i,e	i,e	i,e	i,e	i,e			i,e
4) Data/Program Controls										
DA1 - File and Data Access Restriction	I,E	I,E	I,E	I,E						I,E
DA2 - Screen Savers with Passwords	i,e	i,e	i,e	i,e	i,e	i,e				I,E
DA3 - Automatic Virus Scanners							I,E			
DA4 - Team Software Design		I								
5) User Education										
UE1 - Knowledge/Techniques	I,E	I,E	I,E	I,E		I,E	I,E	I,E	I,E	I,E

KEY:

I	Major Impact on Internal Crime
i	Minor Impact on Internal Crime
E	Major Impact on External Crime
e	Minor Impact on External Crime

SUMMARY AND CONCLUSION

Computer-related crimes are becoming serious problems in today's networked, computer-dependent modern society. While computers and networks greatly enhance an organization's operations, they also present some serious threats if proper security measures are not implemented. Billions of dollars are lost every year to computer crimes.

In order to fight computer crime, it is imperative to thoroughly understand the nature of these crimes. Taxonomy developed in this paper identifies *ten* different types of computer crimes ranging from the altering of data and software to destroying computers. For each category of crime, we describe some specific techniques employed by criminals. Then *five* different types of control mechanisms (procedural controls, physical controls, network controls, data/program controls, and user education) were developed to combat computer crimes. To effectively secure computer systems, it is important to use all the five types of control mechanisms. A security system, after all, is only as secure as its weakest component. Table 1 illustrates the degree (major, minor) and type (internal, external) of impact of each control mechanisms on each crime category.

The addition of computer crime into society is a relatively recent development within the past twenty years. Regulation of network and computer usage to deter computer crime has lagged far behind the developments of technology. Only recently have the law enforcement agencies and justice system begun to address the problems of regulating the usage of computer systems and networks. It is time to take computer crimes very seriously, and organizations and societies worldwide should unite to fight them.

REFERENCES

Baig, E. & Carey, J. (1994, November 14). Shielding the net from cyber-scoundrels. *Business Week,* 88.

Bird, J. (1994). Hunting down the hackers out of computer crime. *Management Today.*

Corriera, K. (1989, February 23). EDI: The future frontier" *Purchasing.*

Markoff, J. (1995, January 23). Data network is found open to new threat. *New York Times.*

Markoff, J. (1995, January 28). Taking a computer crime to heart. *New York Times.*

Paone, J. (1995, June). Cyberspace invaders. *Internetwork,* 33-36.

Reynolds, G. W. (1995). *Information systems for managers.* New York: West Publishing Company.

Richards, R. (1995, February 14). Laptop larceny on rise at airports and hotels. *USA Today.*

Roush, W. (1995). Hackers taking a byte out of computer crime. *Technology Review,* 98.

Russell, D. & Zwickey, E. (1995, Summer). How to get a handle on Internet security. *O'Reilly & Associates, Inc.*

Sandberg, J. (1994, November 18). Losses linked to lax security of computers. *The Wall Street Journal.*

Senn, J. A. (1995). *Information technology in business - principles, practices, and opportunities*. Englewood Cliffs, New Jersey: Prentice Hall.

Wallich, P. (1995, May). A rogue routing. *Scientific American, 272*(5).