A DESCRIPTIVE ANALYSIS OF COMPUTER SECURITY MEASURES IN MEDIUM-SIZED TEXAS COUNTIES

BY

RALPH E. REVELLO

AN APPLIED RESEARCH PROJECT (POLITICAL SCIENCE 5397) SUBMITTED TO
THE DEPARTMENT OF POLITICAL SCIENCE
SOUTHWEST TEXAS STATE UNIVERSITY
IN PARTIAL FULFILLMENT
FOR THE REQUIREMENTS FOR THE DEGREE OF

MASTERS OF PUBLIC ADMINISTRATION

(SPRING 1996)

FACULTY APPROVAL:

Pat Shields

Geo. Weinberg

This research is dedicated to my Lord and Savior, Jesus Christ, my sweet wife, Kathy, who worked hard while I attended school, and to my professors, who dedicated their time and efforts in helping me achieve my goals.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

CHAPTER 1

STATEMENT OF THE PROBLEM

In the past thirty years, computers have increasingly been the targets of criminal activity, as well as, actually being used in the perpetration of crime. One of the major problems associated with computer security is the fact that many, if not most, managers are unaware of, or unconcerned with the problem. As a result, computer security is usually assigned a much lower priority as compared to other tasks associated with day-to day activity.[1]

Computer crimes are more common than most people realize. Every year in the United States billions of dollars are lost by way of computer crime. Estimates range anywhere from between 2 billion dollars to more than 40 billion dollars annually. Even though no one knows the exact amount of money that is lost annually, it is generally considered to be a problem that is growing rapidly. (Mandell, 1992, p. 437)

In the days of the "wild west," criminal activities such as bank robbery were much more common than they are now in modern times. In those days, cash was stored in large banking institutions. Due to the difficulty involved in tracing cash and the slow nature of communication and transportation, bank robberies were much more easily facilitated. However, with the increase in the use of checks and advances in communication and transportation, bank robberies declined. This was due to the ease of tracing checks, and the ease in

---

[1]See for example, Bradbard, Norris, & Kahai, Jan. 1990, p. 11; Business Week, Sep. 26, 1983, p. 126; Rice, Alsobrook, & Weinberger, Mar/Apr. 1982, p. 100.

which criminals could be apprehended, due to faster communication and transportation. (Pfleeger, 1989, p. 1)

In terms of security, the computing environment is very close to the "wild west." Criminals can easily gain illegal entry into a computer system and quickly make off with valuable assets (such as money), or destroy information that is valued by the user. This type of crime involves no face to face contact, and can happen so quickly that it can be months or even years before the violation becomes noticed. With no real "trail" to follow, criminals can easily "make their escape." (Pfleeger, 1989, p. 2)

There are many examples of computer crimes. One example in the private sector involved a product support engineer who was fired for "non-performance." This former employee was later caught in the act of downloading her former employer's proprietary software into her own personal computer. She was able to accomplish this by using the "secret" password that her former employer never bothered to change once she was fired. Another example involved a Dallas petroleum consultant who became suspicious when he discovered that his computer was being used at odd hours of the night. He learned later that a group of computer "hackers" had gained illegal entry into his computer system. One example of a computer crime which involved the federal government was a U.S. Department of Defense fuel supply employee who sent fraudulent payment vouchers to fictitious companies. All of these

examples point out the fact that no one is immune from computer crime, even the federal government.[2]

In spite of the recent publicity concerning computer system vulnerabilities and attacks, most system violations go unreported. Some experts believe that as much as 90 percent of all computer system violations go unreported. Both government agencies and private businesses are hesitant to report these violations due to a fear of adverse publicity. Some organizations are so afraid of this adverse publicity that they have even gone as far as paying the perpetrators "hush money" to keep the incident secret. (Pfleeger, 1989, p. 2; Russell & Gangemi Sr., 1991, p. 8)

Even though the most publicized computer security violations generally involve the private sector, violations such as fraud and embezzlement can also have devastating effects on governments. These effects can range from severe monetary loss to loss of the Public's confidence toward their particular government. The purpose of this research, therefore, is to determine, or describe, what type of security measures are in place to prevent such occurrences at a particular level of government. The focus of this particular research is aimed at medium-sized counties within the state of Texas, ranging in population from between 100,000 to 700,000 in population.

Computer crime, refers to any criminal act which is perpetrated either directly against a computer system, such as sabotage, or an act committed through the use of a computer, such as illegal access with the intent to commit fraud or other acts of deceit. Computer security

---

[2]See for example, Businessweek, Sep. 26, 1983, p. 126; Forester, Mar. 1990, p. 2; Rice, et al., 1982, p. 100.

refers to those technical and administrative efforts required to safeguard the basic components of the computer system. Those basic system components consist of hardware, software, personnel, and data. (Mandell, 1992, p. 438, 443)

Chapter 2 discusses the historical and legal background of computer crime and security. Chapter 3 consists of an in depth discussion of the concepts and protective measures available to guard against computer crimes. Chapter 4 is a brief discussion of the background and particular functions performed by counties in the state of Texas. Chapter 5 consists of a discussion of the methods used to study the computer security of medium-sized Texas counties. Finally, chapter 6 presents the results of the study and closes by discussing the implications of the research findings.

CHAPTER 2
COMPUTER CRIME AND SECURITY: HISTORICAL/LEGAL BACKGROUND

The purpose of this chapter is to provide some historical and legal background regarding computer system security. Specifically, this chapter provides information regarding the development of both Federal and Texas state computer security laws. The legislation presented here is not all inclusive. However, they do represent the most major legal attempts to come to grips with the challenge of keeping computer systems secure.

Information security is not a new phenomena. As long as people have stored and transmitted data there has been an interest in keeping that data secure. For example, one year after the Telegraph was invented by Samuel Morse, a commercial encryption code was developed to keep that information secure. As technology progressed, other laws were enacted to control such things as wiretapping and dissemination of sensitive government information. (Russell & Gangemi Sr., 1991, p. 2-4)

In the early days of computing, computer security was a much simpler task. Computers were rather large, and their operation required a special level of skill. Further, computers were not hooked up to communication lines. To keep a computer system secure, an organization merely had to control access to the physical structure itself. This is no longer the case. Advances in telecommunications, miniaturization of data storage in the form of disks, etc., and the

standardization of operating systems, have made it easier to illegally access a computer system. (Russell & Gangemi Sr., 1991, p. 25)

Computer Security and Federal Legislation

Computer related security activities began in the 1950's, with the development of the first TEMPEST security standards which mandated limits on electro-magnetic emanations coming from computer systems.[3] With the Cold War heating up, the United States government was concerned that Soviet agents would be able to monitor those emanations, and so deduce secret information from them. Also occurring in the 1950's, was the establishment of the first government security organization, the U.S. Communications Security Board (COMSEC), which oversees the protection of classified information. See Appendix A for a list of all acronyms. (Russell & Gangemi Sr., 1991, p. 27)

The 1950's set the stage for later security advances in the 1960's. Computer security really began to expand in the 1960's with initiatives by the Department of Defense (DOD), the National Bureau of Standards (NBS), and the National Security Agency (NSA).[4] As a result of the Brooks Act of 1965, NBS/NIST became responsible for developing standards for computer purchases by federal agencies, as well as, publishing standards for computer use and security, Data Encryption Standards (DES), and safeguarding unclassified information. The NBS/NIST publications which disseminate this information are known as Federal Information Processing Standards

[3]All electronic equipment emanates electro-magnetic energy. In computer equipment, those emanations can be read and information gathered.

[4]The National Bureau of Standards (NBS) is now called the National Institute for Standards and Technology. NIST falls under the authority of the Commerce Department.

publications (FIPS PUBS). (Russell & Gangemi Sr., 1991, p. 32; U.S. Congress, OTA Update, Jun. 1995, p.106-107)

As part of the Paperwork Reduction Act of 1980, the Office of Management and Budget (OMB) was given the responsibility for developing and implementing uniform information resource management policies. By 1985, OMB, through Appendix III of OMB Circular A-135, assigned the Commerce Department the responsibility for establishing security standards for federal information systems, as well as, standards for processing "sensitive" information, and providing technical support to agencies implementing those guidelines.[5] The Defense Department, however, was given the responsibility for establishing standards for the security of telecommunications and information systems, including information that was unclassified but considered "sensitive," and providing technical assistance for the implementation of those standards. (U.S. Congress, OTA Update, Jun. 1995, p. 107- 108)

The Computer Fraud and Abuse Act of 1984, was the first federal computer crime statute. Under provisions of this act, it became a felony to access, without authorization, classified information in a government computer, and a misdemeanor to trespass at all into a government computer, or access credit histories and financial records stored in financial institutions. Two years later the Computer Fraud and Abuse Act of 1986, was enacted to modify the wording and expand the prohibitions and penalties of the 1984 act. The 1986 act made it a first offense felony to knowingly access a

[5]OMB Circulars are used to disseminate information and standards to departments of the Executive Branch.

federal interest computer without authorization, with intent to defraud or damage information. Further, it became a first-offense misdemeanor to traffic in government computer password information, with intent to defraud. (U.S. Department of Justice, Nov. 1988, p. 3-5, 3-6)

The Computer Security Act of 1987, was a legislative response to overlapping computer security responsibilities among federal agencies. The Computer Security Act of 1987, expanded the role of, and gave final authority to, the NBS/NIST in developing government-wide standards and training, regarding the protection of unclassified, yet sensitive information. This act requires every U.S. government agency processing unclassified, sensitive, information to identify their systems and maintain a customized computer security plan for those systems. It also requires that periodic training in computer security be provided for all federal employees and contractors who use, manage, or operate federal computer systems. Finally, this act more firmly delineates the leadership responsibilities for developing security measures. The Department of Commerce (through NBS/NIST), and the Department of Defense, have their responsibilities delineated according to whether or not particular information is within, or outside, the area of national security.[6]

See Figure 2.1 for list of major federal computer laws.

---

[6]See for example, Russell & Gangemi Sr., 1991, p. 41; U.S. Congress, OTA, Sep. 1994, p. 13, 138-140; U.S. Congress, OTA Update, Jun. 1995, p. 105, 108-110.

Figure 2.1: Major Federal Computer Laws

LEGISLATION	MAJOR ASPECTS
1965-Brooks Act	NBS/NIST-responsible for standards regarding computer security
1980-Paperwork Reduction Act	OMB-responsible for implementing uniform info. resource policies 1985 OMB Circular A-135-assigns responsibility for standards and technical support to NBS/NIST
1984-Computer Fraud and Abuse Act	Felony-to access classified info. in a govt. computer without authorization Misdemeanor-to access any govt. computer or financial or credit history without auth.
1986-Computer Fraud and Abuse Act	Felony-to access govt. computer knowingly with intent to defraud or damage info. Misdemeanor-to traffic in govt. password info. with intent to defraud
1987-Computer Security Act	NBS/NIST-given expanded role regarding security of unclassified-sensitive data NBS/NIST-required to provide security training and standards for federal personnel DOD-responsible for all information affecting national security-thus delineating roles of NBS/NIST and DOD

Computer Security and Texas Legislation

After the initiation of several computer security related laws by the federal government, several states have now followed by enacting their own computer security legislation. Texas is among these states. By 1985, the 69th Texas Legislature added Section 33 to the Texas Penal Code. This law defined several different types of harmful access computer crimes, as well as, the penalties involved in their commission. For example, damage to a computer of more than $2,500 was considered a third degree felony. By 1989, however, the 71st Texas State Legislature added an amendment which broadened the scope of crimes and sanctions provided by section 33. For example, damage to a computer system of more than $750 was now considered a felony. (Vernon's, 1994, Tex. Penal Code Ann., Sec. 33)

In 1989, the 71st Legislature also passed the Information Resource Management Act. This act established the Department of Information Resources (DIR), and required them to develop and publish procedures, as well as standards, related to information resources management. In accordance with this act, DIR established the Information Security Standards (1 TAC 201.13(b), a Texas Administrative Code, which requires state agencies to provide for the security and confidentiality of state owned information and information resources.[7]

[7]See for example, DIR, Feb. 1990, p. A-1; DIR, Nov. 1990, p. 1; DIR, Mar. 1993, p. 1.

The Department of Information Resources, through 1 TAC 201.13(b), assigns the responsibility for assuring the security of data information resources, information technology resources, and risk management, to the head of each state agency. Under the Information Resource Management Act, a state agency is defined as any department, commission, board, office, or council, within the executive or judicial branch of the Texas state government. Information resources have been defined as any procedure, equipment, or software, that are designed to collect, process, and transmit information. Information resources technologies have been defined as data processing and telecommunications hardware, software, personnel, etc. (DIR, Feb. 1990, p. A-2; DIR, Mar. 1993, p. 1, 7)

See Figure 2.2 for list of Texas state computer laws.

Computer security is a varied and prolific topic. There are many aspects to be considered when looking at the problem of computer security. The following chapter provides a thorough examination of those computer security aspects.

Figure 2.2: Texas State Computer Laws

Law/Act/TAC	Major Aspects
1985-Section 33 Tex. Penal Code	Computer crimes defined Sanctions prescribed
1989-Section 33 Tex. Penal Code	Definition of computer crimes expanded Sanctions expanded
1989-Info. Resources Management Act	DIR established DIR made responsible for info. resources
1990-1 TAC 201.13(b)	DIR directive Establishes state agency heads as responsible for info. resources

CHAPTER 3
COMPUTER SYSTEM VULNERABILITIES AND SECURITY MEASURES

Literature Review Intent

The intent of this literature review is to explore the issue of computer security. Specifically, security vulnerabilities which are unique to the computer environment are examined, as well as, methods currently used to deal with these vulnerabilities. These vulnerabilities are examined briefly in the *Conceptual Framework* section and more thoroughly later, along with the protections available to counteract them. It can be stated with reasonable certainty that there are no computer systems which are completely invulnerable. However, with a basic working knowledge of the types of security vulnerabilities associated with the computing environment, an administrator should be able to identify and reduce those associated risks.

Conceptual Framework

The conceptual framework in which the computer security of medium-sized Texas counties is examined includes the four basic components of all computer systems. Also included within the conceptual framework is an examination of those security auditing and evaluation methods employed to assess the amount of risk a particular computer system has. The basic components of all computer systems consists of hardware, software, data, and personnel.

Hardware consists of the physical components of the computer system, such as the monitor or hard-drive. In addition, hardware consists of the storage media used to store data and software, such as disks, disk packs, and tape reels. Hardware is generally vulnerable to either direct physical destruction (accidental or intentional), or environmental calamities, such as floods and fires.[8]

Software consist of those programs which either direct the computer to perform certain operations (operating system software), or assist the user in performing certain tasks (application and utility software). Software is surprisingly vulnerable to deletion, modification, and theft. Deletion can occur when someone erases a file or destroys a good copy of a program. Modification can occur when something like a computer virus gains entry into the system and reeks havoc. Both deletion and modification can render an entire computer system inoperable, because without instruction, the computer will not be able to process commands. Finally, software is very vulnerable to theft/unauthorized copying (AKA software piracy). Software piracy is especially prevalent today because of the ease in which software can be copied, due to standardized software systems.[9]

The terms data and information are usually used interchangeably. Data, however, consists of raw, unprocessed facts, whereas, information is data that has been processed and is now in a usable form. Data is vulnerable to interception, unauthorized access,

---

[8]See for example, Mandell, 1992, p. G-6; Pfleeger, 1989, p. 6; Russell & Gangemi Sr., 1991, p. 12.

[9]See for example, Forester, Mar. 1990, p. 2-4; Mandell, 1992, p. G-1, G-9, G-11; Pfleeger, 1989, p. 7-8; Russell & Gangemi Sr., 1991, p.12.

and modification. Phone-lines which carry data can be tapped and signals can be sent which change its meaning. Equipment used to transfer data emanate electromagnetic radiation, which, with the proper equipment, can be monitored.[10]

Finally, personnel who actually use an organization's computer system may represent one of the greatest vulnerabilities of all. Personnel who are improperly trained or incompetent, can accidentally damage or destroy computer assets. Further, disgruntled current or former employees may also represent a danger, due to criminal intention. Personnel vulnerabilities may be one of the most difficult to control, because malicious intent and accidents (due to negligence) are harder to control. (Rice et al., 1982, p. 101; Russell & Gangemi Sr., 1991, p. 13)

See Figure 3.1 for list of computer components and their vulnerabilities.

[10]See for example, Mandell, 1992, p. G-3, G-6; Pfleeger, 1989, p. 8-10; Russell & Gangemi Sr., 1991, p. 12.

Figure 3.1: Computer System Components and Vulnerabilities

COMPONENT	VULNERABILITIES
HARDWARE	Physical Destruction Accidental or Intentional Environmental Calamities Fires, Floods, Etc.
SOFTWARE	Deletion Program Files Erased Modification Viruses Theft or Piracy Illegal Copying
DATA	Interception Tapping, Bugging, Monitoring Electro-Magnetic Emanations Modification Unauthorized Manipulation Unauthorized Access
PERSONNEL	Improper Training Incompetence Disgruntled Employee Current or Former

Hardware Security

Hardware are the actual, physical components of the computer system, such as the monitor and hard-drive, and includes even tapes and diskettes. When dealing with hardware security, it must be kept in mind that it is one of the most simple points of vulnerability, due to its visibility. However, due to this same visibility, it is also one of the most easily protected. The most common types of hardware vulnerabilities include physical destruction (either accidental or intentional), environmental vulnerabilities (water pipes, electric motors, etc.), and natural disasters (floods, fires, etc.), all of which result in physical destruction. (Mandell, 1992, p. 438; Pfleeger, 1989, p. 6-7)

Pfleeger (1989, p. 6) maintains that accidental destruction of hardware should be one of the easier calamities to deal with. Many times this accidental destruction is due to something as seemingly innocuous as people spilling their soft-drinks or food onto computer equipment. Policies which restrict the intake of food or beverages in areas where computer equipment or storage devices are used can easily remedy this problem, especially if those policies are enforced. Finally, policies that mandate the protection of equipment through the consistent use of dust covers and other protective covering devices, provide a simple and inexpensive method of preventing accidental hardware destruction. (Pfleeger, 1989, p. 6)

There are many measures available to guard against the intentional destruction of hardware. The main idea is to limit the available access to this equipment. The most advanced protection systems employ a layered defense against such actions. There are three general layers of defense, object defense (the system or room where the system is located), area defense (the building), and perimeter defense (the area between an outer fence and building). Object defense simply consists of security measures such as terminal locks or detection devices which sound an alarm when sensitive objects are approached. (Lobel, 1986, p. 102)

Both DIR (Mar. 1993, p. 39) and Lobel (1986, p. 100-102), maintain that to provide for area defense, access to computer equipment and facilities should be limited to authorized personnel only. They further argue that computer facilities should have measures in place which control computer system access. For example, identification badges, guards, biometric devices (devices which scan physical or voice characteristics), and television cameras, can all be employed to control access. Further, all visitors should be identified and be under escort at all times. Items which can hide computer equipment, such as briefcases, etc., should be inspected for stolen items (mainly going out) or destructive devices (mainly going in). Other area protection devices include such things as metal detectors at entryways, magnetic contact devices at windows and doors, vibration and audio detectors, as well as optical devices, and infa-red devices which can detect body heat.

Perimeter defense usually consists of a fence around the area of the facility housing the computer system. Perimeter defense may employ some of the same measures found in area defense. For example, closed circuit television cameras can be employed to view those who are entering the grounds on which the facility is located. Other measures may include guards patrolling and limiting access to facility grounds, as well as, bright lighting to detect and discourage potential intruders. (Lobel, 1986, p. 102-103)

Both DIR (Mar. 1993, p. 42-43) and Mandell (1992, p. 444) maintain that to prevent environmental calamities, areas where computer systems are intended to be located should be thoroughly inspected. Many buildings that house computer systems were not originally designed for their use. Buildings where hardware is to be housed should be inspected for such things as water pipes which can burst and drench equipment, or electric motors that adversely affect magnetic storage media. Electrical power used to supply the computer room should be isolated from all other building electrical loads. Further, these authors maintain that electrical power used to supply the computer itself should be isolated from all other building circuits, including computer room circuits. Finally, they argue that the computer room must maintain a controlled environment. This means that the computer room should be properly air-conditioned, heated, and ventilated, as deficiencies in this area are a major cause of environmental problems.

Natural disasters include such things as floods and fires. There are many common sense precautions which can be taken to reduce the dangers posed to computer systems by these calamities. Both Mandell (1992, p. 444) and DIR (Mar. 1993, p. 41, 45) maintain that computer rooms should, preferably, be located above the first floor in case of flooding. An even more common sense idea would be to make sure that computer equipment is not located in a basement. Computer equipment, and media storage rooms should have firewalls which are fire resistant. They further argue that storage media containing data and back-up programs should be stored in a safe location off premises. Another precaution is to make sure that all perimeter walls extend from the floor to ceiling, so as to prevent fire from spreading as easily to the computer room. Finally, fire detection devices and fire extinguishing equipment, are a must to ensure the preservation of computer systems. Fire extinguishing chemicals should preferably consist of an element other than water, such as halon, so as to prevent damage to computer equipment.

See Figure 3.2 for list of hardware vulnerabilities and protections.

Figure 3.2: Hardware Vulnerabilities and Protections

Vulnerabilities	Protections
Physical Destruction Accidental	Policies-restricting food or drink near equip. Protective covering devices over equipment
Physical Destruction Intentional	Equipment- locks and sensing devices Policies-allowing use only by authorized personnel Buildings-monitored by closed circuit TV. Guards at entryways badges required for entry Perimeter-enclosed by fencing, patrolled by guards, and protected by bright lighting
Environmental Destruction	Building inspection-for water pipes, electric motors and other computer hazards Electric power-computer room and computer should have own power source with back-up Controlled environment-air conditioning and heating to protect sensitive equipment
Natural Disasters	Site Selection- computer room location above first floor in case of flood or water leak Fire Protection-from fire detection and extinguishing equipment Computer room-wall should be of fire retardent material and extend to ceiling Storage media-both software programs and data back-up, off premises

Software Security

Software are composed of those computer programs which either direct the computer to perform certain operations (operating system software), or assist the user in performing basic tasks (application and utility software). Application software is used to solve a basic user problem, such as an accounting program, whereas, a utility program is used to perform a specialized function, such as transferring data between files. Software vulnerabilities generally include deletion, modification, and theft. Each of these vulnerabilities and protections are examined separately.[11]

Software deletion occurs when program files are erased. The main emphasis in this situation is controlling access to program files. Personnel can accidentally erase or replace good files. Configuration management, is a method of structuring files into memory in such a manner that they can not be easily erased. Configuration management is also used to control access to those program files. (Pfleeger, 1989, p. 7; Rice et al., 1982, p. 101)

Organizations can purchase hardware that structures memory into privileged and non-privileged areas, or provides a key-like protection method. Hardware systems must be periodically checked for any failure which can leave software open to attack. This failure can be due to something as simple as improper wiring. One of many devices used to physically protect software programs, besides just hardware wiring, are known as dongles. Dongles simply attach to the computer hardware, and prevent the unauthorized use of software

[11]See for example, Forester, Mar. 1990, p. 2-4; Mandell, 1992, p. 259, G-1, G-9, G-11; Pfleeger, 1989, p. 7-8; Russell & Gangemi Sr., 1991, p.12.

by unlicensed users. Though they prevent unauthorized use, dongles do not prevent the unauthorized copying of programs. (Grover Ed., 1989, p. 58; Pfleeger, 1989, p. 7-8)

Other software vulnerabilities include such things as "trap doors" and "spoofs," which are used to gain unauthorized access to computer software. Trapdoors are mechanisms built into a system program by the designer which allow them access in a manner which circumvents normal system protection devices. Spoofs are programs that trick a user into giving away privileged access information (such as a password). Many times this is done through the use of a "masquerade," where someone pretends to be another user (one who has authorized access).[12]

To deal with the trapdoor problem, organizations must ensure that those who design their programs are carefully supervised, and any access afforded, should be limited to the design, implementation, and testing of the system. Russell and Gangemi Sr. (1991, p. 85-86) maintain that any access mechanisms which were put in place during a software program's design phase should be either deleted or closely guarded. This is especially true when those access methods circumvent normal procedures. Finally, to deal with the spoof problem, program information and access may simply be encrypted, or software access programs incorporated, to limit access to authorized users only.

---

[12]See for example, Grover, Ed., 1989, p. 79-81; Pfleeger, 1989, p. 7; Rice et al., 1982, p. 101; Russell & Gangemi Sr., 1991, p. 85-86.

Software modification occurs when a working program is either caused to fail during execution, or to perform some unintended task, such as erase files that were not meant to be erased. With just a bit (single basic building block of computer language, 0's or 1's) or two of data, a program that works smoothly can be converted into one that fails. The most common type of malicious code used for modification is known as a virus. A virus is not an independent program. A virus executes when a host program is run, replicating itself and infecting other programs as it reproduces. Viruses can infect computer memory, floppy disks and any other type of storage. (Pfleeger, 1989, p. 7-8; Russell & Gangemi Sr., 1991, p. 80-81)

Other types of software modification devices include worms, Trojan horses, and logic bombs. Worms are independent programs that replicate themselves in a full blown fashion, tying up resources and eventually shutting down the whole system. A Trojan horse is a fragment of a code which is hidden inside a legitimate program. Along with this legitimate program function, however, the Trojan horse will perform some other unauthorized function. Finally, a logic bomb is a type of Trojan horse which is used to release a worm, virus, or other form of system attack. Logic bombs will activate (release their destructive function) usually as a result of a period of time, or some particular logical function performed by the computer. (Pfleeger, 1989, p. 7-8; Russell & Gangemi Sr., 1991, p. 84-85)

There are many precautions that can be taken to avoid all of these data modification devices. Russell & Gangemi Sr. (1991, p. 87) maintain that only licensed software should be installed into the computer system. Second, software whose packaging has been

opened before arriving at the organization should not be used. Organizations should be wary of shareware software brought from home, and finally, computer systems should be "vaccinated, "in case it does become infected.

Another software problem, software theft (AKA software piracy), is a major growth industry in this country and around the world. Software theft has caused the loss, to those who design it, of over four billion dollars annually. Most of this theft results from people sharing programs, which is made possible by common operating systems. Other types of software theft occur when someone illegally gains access to a computer system by telephone, or some other form of electronic access, and "down-loads" those programs onto their own storage device, usually a floppy-disk or hard drive. (Forester, Mar. 1990, p. 2-3; Pfleeger, 1989, p. 8)

There are several ways to combat these problems. Both floppy and hard disks, where software programs are stored, can be formatted or sectored so that when transferred to other disks they will not run. Further, special hardware can be employed that only works with particularly formatted software programs. Finally, any software developed by the organization should have a copy-write, or patent application pending. Employees should be required to sign a condition of employment form which recognizes the right of the company over all software developments generated by the employee. (Forester, Mar. 1990, p. 4-12; Grover Ed., 1989, p. 6, 178-195)

See Figure 3.3 for software vulnerabilities and protections.

Figure 3.3: Software Vulnerabilities and Protections

Vulnerabilities	Protections
Deletion	Configuration Management-files structured to avoid accidental deletion Access Control Hardware Wiring Dongles or other "key"-like device to prevent unauthorized use Close supervision of program designers to guard against trapdoors Program info. and access encrypted to control for spoofs Software access programs
Modification	Vaccinate-programs Use-only licensed software Avoid-using software with open packaging Avoid-shareware and programs from home
Theft	Format or sector-floppy or hard disks so stolen programs are unable to be run on another's equipment Use-special hardware that runs only the organizations software Apply-for copy-write or patent protection of developed programs Programmers-should be made to sign an agreement giving organization rights to soft.

Data Security

Data consist of raw, unprocessed facts, whereas, information is data that has been processed into a usable form. Data itself has no intrinsic value, such as hardware. Nevertheless, data does have a cost, such as the cost in time it takes to pay employees to reconstruct lost or modified data, or data that has fallen into the hands of people who use that data for unscrupulous gain. The value of data declines more rapidly than the value of hardware or software programs. Even when the value of particular data is high, its relative worth may be high only for a short period of time, such as inside stock information. (Pfleeger, 1989, p. 8-9)

Data can be gathered in many ways, such as, tapping wires, planting bugs inside output devices, sifting through trash receptacles, reading it off of computer monitors, or simply stealing it off of desk tops. Many of these types of data gathering methods require no particular technical sophistication. When it comes to data modification, however, a higher level of technical expertise is needed, even more so in comparison to data interception. (Pfleeger, 1989, p. 9-10)

Protecting computer systems that are not linked is a much easier task than those that are. Data can still be gathered from these systems, as well, through the use of some of the unsophisticated gathering methods mentioned earlier. Generally, however, in today's modern era of communication, data is communicated through some form of linkage. This includes computers communicating with each other in a small building to computers communicating across the globe. In fact, it is generally agreed that the area of data

communications is the weakest link in many information systems. Some of those information systems include LAN's, MAN's, and WAN's. LAN's are local area networks which serve a small geographical area such as an office building. MAN's are metropolitan area networks which may serve an intermediate area such as a small city. Finally, WAN's are wide area networks that span a large geographical area or even the world. (Lobel, 1986, p. 104; Russell & Gangemi Sr., 1991, p. 210)

There are four general physical areas in which computer data communications are vulnerable. The first area is that of communication devices. Communication, or source and destination devices (AKA nodes), include such items as computer terminals, personal computers, modems, etc. The second general area is that of communications lines within or between buildings, such as copper wire, twisted pair (two insulated wires), or coaxial cable (made of copper and aluminum). The third problem area consists of the linkages between communicating parties. This includes telephone lines made of copper, and satellite and microwave linkages. Finally the fourth general physical area of vulnerability consists of those devices (usually other computers) used to relay information between communicating source or destination devices. (Lobel, 1986, p. 105-107)

There are several ways to deal with the problem of data interception as they relate to the four general physical areas of data communication. These types of attacks (interception) on data security are known as passive attacks, or attacks on confidentiality, because the theft is through monitoring, or listening in, on communication. Security services used to prevent such attacks involve the protection of single messages to entire message streams, as well as, the traffic flow (direction of communication) generated by those messages. Hardware items such as computer terminals, modems, relays, and other data communication hardware, that produce electro-magnetic radiation should be shielded.[13] Many government agencies today are required to purchase equipment that has a certain "TEMPEST" (shield) rating. Shielding equipment in this manner, keeps those who have the equipment to read such emanations from doing so. (Lobel, 1986, p. 106; Stallings, 1995, p. 8, 10)

Other types of interception include the tapping or bugging of communication lines and the interception of microwave and satellite transmissions. Local telephone cable, coaxial cable, and twisted pair cable, are all easily tapped into. Some of the methods used to protect against communication line vulnerabilities include burying cable under ground (avoid running it along the ceiling), running it through shielded electrical pipe, or for the more security conscious, running the cable and its connectors through pipe filled with pressurized gas

[13]To reiterate, all electronic equipment emanates electromagnetic radiation. With the right equipment, these emanations can be read and confidential information deduced. By shielding computer equipment in a manner that reduces those emanations, security is enhanced. This shielding has nothing to do with safety.

with a sensor that detects pressure change and sounds an alarm when tampered with. Lines protected in this manner are harder to tap into or read any electromagnetic radiation from. (Lobel, 1986, p. 107; Russell & Gangemi Sr., 1991, p. 213-214)

Another way of protecting line communication is to use fiber-optic cable. Fiber optic cable is difficult to tap because it is not electrical, therefore, it does not radiate. Finally, microwave and satellite communications (terrestrial and orbital relay stations) are vulnerable to interception, and the only way to effectively deal with this problem is through the use of message encryption, whereby messages are transmitted in an unreadable form to those who do not possess a decryption key.[14]

Unlike interception, modification of data involves an active attack on the integrity of the data stream. When a message is modified, it is generally either altered, delayed, or reordered, so as, to produce an unauthorized effect. For example, a person who is unauthorized to access certain data may intercept a message which authorizes someone else to access certain files. After the message is intercepted, it is altered, enabling the unauthorized individual to access the particular files. (Stallings, 1995, p. 9-10)

Other active attacks include masquerades (similar to a software attack) in conjunction with replays, and denial of service. Similar to an attack on software, a masquerade occurs when someone pretends to be someone else. For example, a person may capture authentication sequences used to gain access to data, then replay that

[14]See for example, Lobel, 1986, p. 107; Purser, 1993, p. 9-10; Russell & Gangemi Sr., 1991, p. 213-214.

sequence to gain unauthorized access. Finally, the denial of service involves the prevention or inhibition of the normal use of computer communication facilities. For example, someone may try to suppress messages to particular destinations, or they may try to disrupt an entire network by either disabling it or overloading it with messages. (Stallings, 1995, p. 10)

The security services available to deal with active attacks include authentication, integrity assurance, non-repudiation, availability, and access control (discussed more thoroughly later). Authentication involves the use of an authentication service which ensures that the two entities communicating with each other are who they say they are. Authentication begins at the time a connection is initiated and, further, ensures that the connection is not interfered with in any manner, such as through a masquerade. The security techniques involved include message encryption, passwords, digital signatures, and time stamps. (Russell & Gangemi Sr., 1991, p. 229; Stallings, 1995, p.10-11)

Integrity assurance is simply a service which ensures that messages have not been tampered with in any manner. The main security technique used to guard against tampering is that of message encryption. Non-repudiation is a service which ensures that neither the sender, or the receiver, can deny that a message was sent or received. The security techniques involved with non-repudiation include message encryption, or some form of electronic or digital signature, which ensures that messages were sent and received. This last protection guards against such things as someone denying that

they had received an electronic funds transfer when they actually had. (Russell & Gangemi Sr., 1991, p. 229; Stallings, 1995, p. 11)

Availability assurance ensures that networks will have all the services they need for smooth operation, fully available to them. Some of the security techniques involved with availability assurance are redundant back-up systems, detection devices (such as transmission rates), and detection of overall network performance. Finally, access control assures that only those who have a legitimate need to access a computer system are able to do so. The main access control technique used in the '90's (other than manufacturer supplied hardware and software) is that of passwords and the structuring of access into levels of authorization managed through some type of access control software.[15]

In the realm of network security, access control means the ability to limit access to computer systems via communication links. To attain this type of control, anyone trying to gain access to the system must be uniquely identified, and authorization access tailored specifically to what each individual is permitted to do. The access control system is required to mediate between authorization and access to each one of its individual components, such as personnel, equipment, programs or data. In other words, it identifies who is allowed to access what equipment, data, or programs, and during what time frame? Finally, all access control systems must not only detect and prevent violations, but must report them as well.[16]

---

[15]See for example, Lobel, 1986, p. 125-126; Russell & Gangemi Sr. 1991, p. 229-230; Stallings, 1995, p. 11-12.

[16]See for example, Lobel, 1986, p. 127; Srinivasan & Dascher, Aug. 1986, p. 41-42; Stallings, 1995, p. 11-12.

There are two basic types of access controls for computer systems that provide different levels of data protection. The first is *discretionary access control* (DAC), where the data owner decides how they want to protect their files and whether or not to share their data. The second type of access control is called *mandatory access control* (MAC), where different data is assigned a corresponding security label and access is authorized accordingly. This latter type of access control is more complex. (Russell & Gangemi Sr., 1991, p. 66)

There are various types of discretionary access control. The first type consists of the ownership of files, directories, and computer devices. This type of system allows access and ability to manipulate data based on the user's identification. One problem with this type of system, however, is that it does not permit file sharing. Other, more workable, types of DAC's include File Types and Protection Classes, Self/Group/Public Controls, and Access Control Lists. (Russell & Gangemi Sr., 1991, p. 66-71)

File Types and Protection Classes allow the user to limit access to others based on the assignment of data into the categories of public, semi-public, and private. Self/Group/Public Controls simply allow the user to divide access to their files based on three categories. The owner of the file assigns themselves, particular groups, and the general public, particular access capabilities. Finally, Access Control Lists simply consist of lists of users and groups with their corresponding levels of access. (Russell & Gangemi Sr., 1991, p. 66-71)

Mandatory Access Control (MAC), briefly, is an access policy normally associated with very sensitive data such as classified government or sensitive corporate information. MAC's involve the assignment of sensitivity labels to all subjects (users and programs), and all objects (files and directories). Personnel are allowed access to files based on the sensitivity of objects and their (personnel's) corresponding levels of access. (Russell & Gangemi Sr., 1991, p. 66-71)

Passwords (a major data access control device), whether associated with access control software or other access control measures, serve the purpose of uniquely identifying each individual that is trying to log onto a system and are further used to determine what the particular individual is permitted to do. Besides keeping passwords confidential, other considerations should be taken into account. First, passwords should be changed periodically to help deter unauthorized access due to disclosure. Second, in order to avoid ease of guessing, they should consist of at least six or more alpha-numeric symbols or other special characters. Third, passwords should not consist of easily guessed names, such as names of loved ones, etc. Fourth, the access control system should keep a list of all attempted uses of outdated passwords to determine possible security problems. Finally, passwords should be encrypted to further ensure confidentiality. (Neumann, Apr. 1994, p. 126; Srinivasan, & Dascher, Aug. 1986, p. 43)

To safeguard the data of computers hooked to the Internet (AKA, the "Net"), many organizations are finding the installation of "firewalls" and "filters," and the encryption of data sent across the Net, to be good compliments to their organization's data access security.[17] Further, there are now widely available programs which allow systems users to test the security of their computer systems, so as, to find and fix uncovered problems. Firewalls consist of dedicated computers which screen incoming computer traffic and only allow entry into the system by "trusted" computers only.[18]

Firewalls are not completely safe, however, because they can be "spoofed" (discussed earlier), and unauthorized access achieved. Firewalls can be complimented by filters which ensure the accurate origin of messages, and also block outgoing data which is unauthorized to do so. Encryption (discussed earlier) protects the confidentiality of data sent across the Net, and if intercepted, is unintelligible to unauthorized users. Finally, software programs like Tripwire and SATAN (Security Administrator Tool for Analyzing Networks) allow systems users to uncover vulnerabilities in their computer data and network systems, and remedy those weaknesses.[19]

See Figure 3.4 for list of data vulnerabilities and protections.

---

[17]See for example, Muir, Apr. 1994, p. II-1. This book explains that the Internet is a network of interconnected computers. Messages can be sent between computers, via tele-communications lines. Messages sent across the Net can travel by many pathways to the final destination. In other words, if a user sends several different messages, those messages will travel through the most available path, not necessarily the same one. Messages sent across the Net are not secure unless they are properly encrypted.

[18]See for example, Cortese, Mar, 1995, p. 93; Daly, Feb. 14, 1994, p. 14; Neumann, Jun. 1995, p. 138.

[19]See for example, Cortese, Mar. 1995, p. 93; Daly, Feb. 14, 1994, p. 14; Neumann, Jun. 1995, p. 138.

Figure 3.4: Data Vulnerabilities and Protections

Vulnerabilities	Protections
Interception Tapping, Bugging, Monitoring E. M. Rad.	Shield-equipment and commo. lines from E. M. radiation (TEMPEST) Shield-commo. lines in electrical or gas filled pipes with detectors and alarms to thwart tapping and bugging Use-fiber optics- hard to tap Encrypt-data
Modification Masquerades, Replays, Repudiation, Denial of Service	Use-authentication services and digital signatures to verify and confirm message origins Use-time stamps to verify contacts-guards against repudiation Use-access control software Employ-back-up services in case services are disrupted
Unauthorized Access	Use-access control software DAC-user chooses protection MAC-system based on security labels and data sensitivity Use-passwords (preferably encrypted) Employ-"filters" and "firewalls" Employ-sec. test software (Tripwire, SATAN)

Personnel Security

The people who design, operate, or maintain the computer system of any organization are those personnel who are most intimately acquainted with the system. These people are, at the same time, the most valuable asset, as well as, crucial weak point of any computer system. Outsiders may break into a computer system in a variety of ways, but the fact remains that most computer system violations occur from the inside. These threats can come from many different sources, such as, disgruntled current or former employees, employees being black-mailed, etc. Some of the most dangerous personnel, however, may be those that are lazy, untrained, or simply incompetent. The fact remains, however, that in spite of this latter category of threat, a lot of white collar crime begins with access to a computer. It is, therefore, imperative to hire those who will not even be tempted to engage in such malicious activity.[20]

Recruitment is one of the major functions of most organizations. Compounding the problem of recruitment in the computer industry is the large turnover of computer personnel. As a consequence of this turnover, there is a constant demand to fill vacant positions with qualified and experienced personnel. Due to shortages in computer personnel, there is the temptation by many organizations to hire personnel that are not quite up to expectations. These are the same personnel with direct access to computer data and equipment. (Buss & Salerno, 1984, p. 118; Guynes & Vanecek, 1981, p. 72)

---

[20]See for example, Guynes & Vanecek, 1981, p. 71; Pfleeger, 1989, p. 11; Russell & Gangemi Sr., p. 16; Watson, Jan. 1985, p. 73.

Several authors argue that to effectively recruit qualified, competent, and honest personnel, organizations should institute an effective screening and hiring process. First, accurate job descriptions should be designed for specific functions, and selection of candidates based on those specific functions. Second, applications should be checked for their completeness, and gaps in employment history should be fully explained. Potential employers should be aware of frequent job changes and lack of positive comments from former employers. Third, both credit and criminal history should be checked for any signs of problems. Organizations should be especially alert to drinking and drug problems. For the most sensitive positions, consider the use of polygraph examinations and hand writing analysis. Finally, when a new person receives a position from an organization, that position should be contingent upon the signing of a "non-disclosure agreement," which is an agreement to keep all information gained from the employment experience, secret.[21]

Several authors further argue that all personnel hired, whether experienced in computers or not, should be required to undergo a training period based upon their particular level of expertise. This training should involve both equipment and security training, and should be an ongoing activity. There are many ways to train personnel in the use of equipment, such as, through colleges, seminars, adult education programs, or on the job, by other personnel. Security should be a part of the training of all computer

---

[21]See for example, DIR, Mar. 1993, p. 33-34, 36; Guynes & Vanecek, 1981, p. 73, 77; Miller, Aug. 1978, p. 40.

personnel. All new employees should be required to attend an orientation which spells out the organization's security requirements, policies and procedures.[22]

Besides training those who are newly hired, an organization would be wise to continue training their personnel on a regular basis. The training which fosters competence in equipment operation would be the same as for newly hired personnel, such as, through colleges, etc. To spread security awareness, however, organizations can make use of such things as seminars, newsletters, bulletin boards, etc. Topics should include such items as passwords, message authentication and encryption, work habits and how they relate to security, and other topics concerning security. Finally, organizations should periodically distribute their security policies and procedures, and at the same time, obtain signed acknowledgment from employees that they read those policies and procedures. All of these measures ensure that security awareness is spread, as well as, places responsibility for security on individual employees. (DIR, Mar. 1993, p. 35)

Both DIR (Mar. 1993, p. 36) and Guynes & Vanecek (1978, p. 40), maintain that when determining the amount of access that an employee should be allowed to have to computer equipment and data, organizations should assess that access according to the principle of "need to know." In other words, employees should only be given enough access to computers and data , so as, to permit them to complete their assigned tasks. Further, management should assign

---

[22]See for example, DIR, Nov. 1990, p. 8; DIR, Mar. 1993, p. 34; Guynes & Vanecek, 1981, p. 77; Mandell, 1992, p. 209.

individual personnel the responsibility for particular components within the system, and one individual, such as a data processing or security manager, should be given the assignment of overall computer security responsibility.

Finally, these same authors argue that management should take the responsibility of assigning individual responsibility for the security of particular data. Records or journals should be kept which track the use of equipment (terminals, etc.) and data (files, etc.). Provisions should be made to track any variations or deviations of access protocol. Finally, if an employee is terminated, measures should immediately be implemented which protect computer equipment and data. These measures include such things as immediate denial of access to computer equipment and data, changing of passwords, and the return of locks, keys, and identification badges. (DIR, Mar. 1993, p. 36; Guynes & Vanecek, Aug. 1978, p. 40)

See Figure 3.5 for personnel vulnerabilities and protections.

Figure 3.5: Personnel Vulnerabilities and Protections

Vulnerabilities	Protections
Improper Training	Training Policies-equipment training based on current level of expertise Security training-at time of orientation and ongoing
Incompetence	Hiring Policies-specific job descriptions Thorough screening-and background checks Polygraph, etc., for most sensitive positions
Disgruntled Employee Current or Former	Access Policies-"need to know basis" Track-use of equipment and data with logs and journals Assign-personnel responsibility for individual computer components and data Upon termination-immediate revocation of access to equipment and data Change locks, keys passwords, etc.

Security Evaluation and Auditing

In spite of the best intended preventive measures, losses to computer systems still occur. It is, therefore, imperative to conduct regular audits and evaluations to determine what particular system vulnerabilities may exist, and what measures are necessary to correct them. Security evaluation begins at the beginning of the life cycle of a computer system (even before a system is purchased) and continues throughout. There are three general stages of security evaluation development, the initial stage, the development stage, and finally, the operation and maintenance stage. Each of these stages are discussed, along with the evaluation focus of each particular stage.[23]

During the security evaluation initiation stage the main emphasis is on what is called "risk analysis." Risk analysis involves identifying what systems and components are in need of protection (obviously the four basic components of a computer system), what types of hazards they face, the frequency in which these components face particular hazards, the cost to repair or replace items that are damaged or lost, and finally, the cost to protect such items. The tools used in risk analysis are items such as checklists and work-sheets which help in the identification of systems and computation of costs, both to protect and to replace.[24]

Several authors maintain that the computer systems and components which should be evaluated include everything from

---

[23]See for example, Rice et al., 1982, p. 101-102; U.S. Dept. of Comm., FIPS PUB 102, Sep. 27, 1983, p. 19.

[24]See for example, DIR, Mar. 1993, p. 20-25; Miller, 1978, p. 40-41; Purser, 1993, p. 4-6.

computer hardware and software, to buildings and continuity of service. Hazards which should be assessed are such things as accidental and intentional destruction of equipment, to natural and environmental catastrophes. The frequency in which hazards may be faced are usually figured on an annual basis, and once figured, a dollar amount is estimated for both the loss and protection of these assets. The authors reason that costs to protect items should, obviously, not exceed the cost of the particular asset.[25]

During the development stage of security evaluation implementation, security evaluations and applications are validated, verified, and tested, to determine their efficacy. This type of evaluation is not only used to assess security measures that have been put in place as a result of risk analysis (quantitative measurement), but also, to evaluate those which are purely qualitative measures of security performance. For example, not all security and loss controls lend themselves to evaluation through risk analysis, due to the fact that the baseline of "expected loss" is not always easily quantified. The solution, therefore, is to validate that a particular security system is the correct response for a particular hazard, and verify that the system is as complete as possible, by testing its performance. The baseline for performance evaluation in this scenario shifts from expected loss, to that of "correctness of the system," as measured against explicitly stated security requirements, as determined by both management and technical experts. (U. S. Dept. of Comm., FIPS PUB 102, Sep. 27, 1983, p.19-20)

---

[25]See for example, DIR, Mar. 1993, p. 20-25; Miller, 1978, p. 40-41; Purser, 1993, p. 4-6; U.S. Dept. of Comm., FIPS PUB 102, Sep. 27, 1983, p. 18-19.

During the operation and maintenance stage of security evaluation (the final stage of security evaluation implementation), the main emphasis is on reassessing security risks, as well as, safeguards. During this stage of evaluation, assessment will consist of not only the presence and adequacy of controls, but also, compliance with security policies. For example, during this stage, a "security safeguard evaluation" is used to divide security problems into smaller, more specific areas, such as hardware, software, security management, etc. Each section is then evaluated through the use of a checklist, so as, to eventually gain a larger picture of security issues within the organization. Finally, results are checked against stated policies. (U. S. Dept. of Comm., FIPS PUB 102, Sep. 27, 1983, p. 20-21)

Another evaluation technique used in this stage is that of "electronic data processing" (EDP) audits, which are more broad in scope than security safeguard evaluations. For example, security safeguard evaluations take place under the control of those responsible for the application of security measures, whereas, the control and results of an EDP audit are under, and forwarded to, an authority that is higher than those implementing particular security measures. While both security safeguard evaluations and EDP audits may both be concerned with anticipated threats, EDP audits are also concerned with the such items as the validation of data reliability (something that may not necessarily have a security application), which makes the EDP audit more broad in scope. (U. S. Dept. of Comm., FIPS PUB 102, Sep. 27, 1983, p. 20-21)

See Figure 3.6 for security stages, evaluations, and applications.

Figure 3.6: Security Implementation Stages, Evaluations, and Applications

Stages	Applications
Initial	Risk Analysis Identify components to be protected Identify specific hazards Identify cost to repair and replace items Identify cost to protect components
Development	Validation, Verification, and Testing Evaluate protective measures Baselines-for measurement of effectiveness: Quantitative (expected loss) Qualitative ("correctness" of system)-as determined by both management and technical experts
Operation and Maintenance	Security Safeguard Evaluation Check-compliance with security policies Divide-security concerns into smaller more specific areas then evaluate each section Piece-sections together, after separate evaluations for overall security picture Electronic Data Processing (EDP) Audits Check-compliance with security policies Check-overall function and performance of EDP system, not just security

Conclusion

The review of literature has shown that computer security is a major concern within both the public and private sectors. It seems that the majority of expert opinions (which all of this information is based on) conclude that management, generally, has a rather nonchalant attitude toward computer security, due to a lack of awareness of the problem, and a naive belief that their organization will not be victimized by a computer crime. These attitudes, along with a lack of funding for preventative measures, are blamed for a lack of sufficient computer security within organizations. (Business Week, Sep. 26, 1983, p. 126; Rice et al., 1982, p. 100)

It can also be said that the problem of securing computer information systems is multifaceted and difficult. This is not only due to the technical complexity of the systems involved, but also, the sheer number of vulnerabilities inherent in the systems. A review of the literature also demonstrates that there has been a wealth of security measures developed to reduce system vulnerabilities. No one or two developments, however, can cover every vulnerability, especially in light of rapid technological developments which allow system penetration. These problems are occurring at a pace equal to, or greater than, security developments. The most reasonable course of action, therefore, is to develop a system of risk analysis and security auditing which assesses and reduces computer system vulnerabilities. By assessing risks and vulnerabilities, managers can learn how to best employ their limited resources in a cost effective manner. (Russell & Gangemi Sr., 1991, p. 24-27)

From the review of the legal and legislative background of computer security and crime, it can be surmised that the laws protecting computer security also have some difficulty in keeping up with technological development. This is evidenced by the constant changing and clarification of laws and sanctions as new developments occur. It is also shown that laws and sanctions dealing with computer security violations are patchwork solutions at best, as evidenced by the differing laws pertaining to federal government, state government, and private sector computer systems. (Russell & Gangemi Sr., 1991, p. 24-32; Vernon's, Texas Penal Code Ann., 1994, Sec. 33)

While the experts, whose opinion forms the basis of this literature review, argue for the implementation of particular computer security measures, these arguments lack any empirical support. All of the measures which are illustrated as offering protection are based on these experts opinions of what constitutes proper safeguards. Unfortunately, there is a lack of empirical evidence to support how well the stated safeguards work. This may be more of a result of the idiosyncrasies of the particular area (ie. the rapid advancement of technology), than any lack of will to perform such empirical evaluations. Finally, this research has shown that most of the writing is concerned with Federal government and private security matters. There is some information concerning Texas state agencies and small local governments (which includes small Texas counties), but even this is scarce. This study, therefore, is performed to try to fill in some of this information gap by focusing on the computer security measures of medium-sized Texas counties.

Texas counties operate in an environment that is quite unique. They are "creatures" of the state, since they derive almost all of their power from either the legislature or the Texas Constitution. Though counties derive most of their power from the state, they are still separate from many state mandates. As mentioned in Chapter 3, state agencies are required to follow the mandates set forth by the state, when it comes to computer security. Counties, however, are exempt from these mandates. The following chapter provides information regarding the unique environment in which Texas counties operate.

CHAPTER 4
TEXAS COUNTIES

Chapter 4 provides the setting for which Texas counties operate. This chapter explains the history of Texas counties, so as, to provide some insight into what particular events influenced the present structure. Further, there is a discussion of what types of functions Texas counties perform. Finally, revenues, expenditures and other miscellaneous data pertaining to Texas counties is also presented. By having an understanding of these basic county functions, some insight can be gained as to the possible use of computer technology within Texas counties.

History of Texas Counties

For as long as government has existed in Texas, counties have also existed. Under Mexican rule, Texas was divided into three "departments." Under each department existed municipalities, some of which were further divided into districts. Both a military and political leader were in charge of each department, whereas, a council consisting of four councilmen were in charge of each municipality. All of the officials of the council were elected. This council was charged with overseeing the political and economic government of the settlement. Further, they were charged with preserving public order, public health, public works (streets, etc.), and taxation. Thus, the primary role of government within each settlement was to provide for law and order, and a means for adjudicating disputes. (Norwood & Strawn, Nov. 1984, p. 1)

After Texas became a Republic in 1836, Texas adopted a county system that was very similar to other county systems of other Southern states, particularly Alabama. This is due in large part to the fact that many Texans at that time hailed from these areas. The Texas Constitution of 1836 required that the new republic be divided into a "convenient" number of counties. Each county was to have a convenient number of justices of the peace, and only one sheriff and coroner. Each county was further subdivided into militia precincts. Taxes were gathered by the tax assessor-collector at militia musters. Finally, county legislative functions were given to a board of commissioners which consisted of a chief justice and justices of the peace. This board was primarily concerned with building roads, levying taxes, and providing for the indigent. (Norwood & Strawn, Nov. 1984, p. 2-3)

After Texas gained statehood in 1845, a new constitution was drafted to comply with those changes which were required for entrance into the Union. During this period, and during the time of Texas' secession from the union, there were relatively minor alterations in the form of county government. After Reconstruction, when primarily military law prevailed, Texas drafted its present Constitution in 1876. This constitution prescribes a form of county government which in organization and concept is very similar to the form of county government adopted in 1845. Under this constitution, county government combines both state and local functions. The officer of the county governing body (county judge) performs both legislative and judicial functions, counties are divided into precincts, and finally, most of the officers which were prescribed

as part of county organization in 1845 are the same as in the constitution of 1876. (Norwood & Strawn, Nov. 1984, p. 4-6)

The Restrictive Nature of Texas County Government

The Texas Constitution of 1876 was drafted after the Reconstruction period. Partly as a response to the abuses of "carpetbag" rule, where elections were basically rigged and the only citizens allowed to vote and hold office were union sympathizers, the Texas Constitution was drafted in very specific terms. This specificity extended to county government. The Texas Constitution of 1876 sets forth a detailed organization of county structure, methods of selecting county officials, and in certain cases, the duties to be performed by particular county officials. (Norwood & Strawn, Nov. 1984, p. 8, 11-12)

The result of this specificity is that county government is very rigid. Courts in Texas have repeatedly affirmed the premise that counties can perform only those functions authorized by law. At the same time, however, Texas Courts have also liberally construed those powers which counties are given. This allows counties more leeway in matters where powers are more implied rather than specified. In some cases, the Texas Constitution specifies the particular function the county may perform. In most cases, however, the constitution gives the Texas Legislature the power to authorize counties to act in specific areas. The result of the Legislature's power to authorize county functions, has been a multitude of laws and legislative acts which provide both general and specific county authority. This legislative detail has further resulted in restrictions on county governmental activity. (Norwood & Strawn, Nov. 1984, p. 11-17)

Dual Nature of Texas County Government

Texas counties, as a governmental body have a dual nature. In one manner they act as an administrative arm of the state, where they carry out the functions of state government on a countywide basis. Such functions include such things as enforcing state health rules and collecting some state taxes. In another manner, counties take on a more local characteristic, due to their responsibilities for such things as administering local public welfare services, building roads and bridges, aiding in fire protection, and serving the needs of citizens living outside of incorporated municipalities. (Norwood & Strawn, Nov. 1984, p. 9)

Those in charge of county government provide another illustration of this dual nature. The offices of those who govern at the county level are established by the Texas Constitution but are locally elected. Each of these elected officials are independent of the other. The governing body of Texas counties (the Commissioners Court) consists of one county judge and four county commissioners. Other constitutionally prescribed offices include constables, justices of the peace, county clerk, county and district attorney, sheriff, tax assessor-collector, and treasurer. The county sheriff is good example of the dual nature of county government. The sheriff is an officer of the state but has the role of administering law enforcement duties at the local level. (Norwood & Strawn, Nov. 1984, p. 21-24)

In addition to those county offices prescribed by the Texas Constitution, the commissioners court of each county is authorized to appoint other officers to head those county departments established by the court (commissioners court). These include such individuals

as welfare directors, librarians, health officers, purchasing agents, and park directors. One very important county officer, the county auditor, is appointed by the district judges of the county. All counties with a population of 10,000 or more, except McColloch and Culberson counties, are required to have a county auditor. In many counties, the auditor is the de facto chief administrator. They are in charge of general oversight of all books and records of all officers of the county who receive county funds. Basically, they are the county budget officer. (Norwood & Strawn, Nov. 1984, p. 26-27)

Texas County Revenues, Expenditures, and Services

The main revenue source of Texas counties, as is in most other states, is that of property tax. As of 1982, 52% of county revenues came from property tax, 32% from charges and other miscellaneous sources, 12% from intergovernmental revenue, and 4% from other taxes. The major expenditures of Texas county governments include in descending categorical order; Other-46%, Health and Hospitals-27%, Highways-15%, Police and Fire Protection-5%, Interest on Debt-3%, Public Welfare-2%, and finally, Education-less than 1%. (Norwood & Strawn, Nov. 1984, p. 44-45)

The main services provided by Texas county governments are those most traditionally associated with county government nationwide. Those services include property tax assessment and collection, maintenance of land records (deeds, etc.), courts, criminal prosecution and maintenance of criminal records, maintenance of jail facilities, police and fire protection, road construction and maintenance, parks and park maintenance, maintenance of vital

statistics, and finally, health related functions such as communicable disease control. (Norwood & Strawn, Nov. 1984, p. 48-49)

Miscellaneous Texas County Data

There are 254 counties in the state of Texas. The total population of Texas as of 1994 is 18, 378, 185. Approximately 75% of that population lives in 31 counties. Approximately 41% of the population lives in the four largest counties, Harris, Dallas, Bexar, and Tarrant counties (populations over 1,000,000 each). Approximately 35% of the population; 6,390, 026 live in the 27 medium-sized counties that are targeted for this study. These counties range in population from 100,000-700,000. This population range (100, 000-700,000) was chosen strictly because it represents the approximate middle range of the population of Texas. In other words, approximately six-million live in the four largest counties, six-million live in the 223 smallest counties, and the last approximate six-million, live in the 27 medium-sized counties that are studied. (Texas Department of State, Dec. 6, 1995, World Wide Web, Internet)

Large counties such as Bexar and Dallas counties (populations over 1,000,000) would have more in common with each other such as budgets, problems, and population. Smaller counties, those less than 100,000, would also be more likely to have similar problems, budgets, etc., peculiar to their population size. In this manner, medium sized counties were chosen for this particular study, because they would be more likely to have similar peculiarities, due to such things as population size.

It is within this context that the computer security of these 27 target counties is studied. As technology and information needs progress, organizations of all sizes and descriptions are forced to keep up with these ever increasing information needs by computerizing all kinds of record keeping and service provision. As the size of Texas counties expands, so too must the use of computer services expand to efficiently administer the records and services provided. With this expansion of computer use comes the associated problems of maintaining the necessary computer security discussed in previous chapters.

To study Texas counties and gather the data needed to perform such studies, certain data gathering techniques must be employed. This study involves fairly detailed information with regards to particular security measures. The following chapter explains how those particular data gathering techniques are employed.

CHAPTER 5

METHODOLOGY

Data Collection

According to Babbie, the most appropriate research technique for use with descriptive categories, and for describing populations which are too large to be observed directly, is that of survey research.[26] Survey research, according to Yin is also the best research method for answering "what" questions. In this case, "what kind of computer security measures are used in medium-sized Texas counties?" The use of a questionnaire to conduct survey research is the most appropriate method to use when time and money constraints, and sensitive subject nature, are a consideration. These types of considerations generally rule out methods such as personal interviews which are more costly, time consuming, and less confidential. (Babbie, 1995, p. 257-264) (Yin, 1994, p. 5-7)

Though this form of research is faster and more cost effective, it does have its weaknesses. Survey research is generally considered to be weak on validity but strong on reliability. This is due to the fact that responses are limited to particular categories which make observations more artificial. However, these same structured response categories which may promote artificiality also promote reliability due to the fact that all subjects (respondents) are provided with a standardized stimulus. Another problem with survey

---

[26]Although the actual population of this particular study is not large, the physical area it occupies is large. It would be a huge undertaking in time and money to travel to the 27 counties involved in this study, due to their dispersed proximities.

research, according to Babbie, is that of response rate. Without someone there physically to prompt potential respondents into participating, there is a lack of impetus to bother with the study at all. (Babbie, 1995, p. 257-264)

To deal with some of these inherent weakness, certain techniques have been employed to collect data, as illustrated by Babbie. First, to encourage a higher response rate, responses have been structured into simple "yes" or "no" categories, since the ultimate aim is to determine whether or not particular security measures are being used. According to Babbie, if a questionnaire is simple it will be more likely to be answered. Second, self addressed, stamped envelopes were sent to all potential respondents. Further, two follow up letters were sent one week after each stated deadline, and a phone call was made to selected non-respondents, again, so as to facilitate a higher response rate. Third, the fact that the survey results would be kept confidential, due to the sensitive nature of the subject, was communicated to all potential respondents. Finally, to deal with some of the concerns of artificiality, a response category called "Additional Comments," was included. No survey can be totally inclusive as to response categories. This is especially true with this particular survey, due to the fact that there are myriads of types of computer system security measures available. With a space which allows for additional comments, some of the artificiality created by limited response categories is negated. (Babbie, 1995, p.257-264)

The questionnaire used in this survey is divided into seven sections, a general introductory section, a short background section,

and five sections related to the descriptive categories as found in Appendix B. Questions concerning the security of computer system components are structured by vulnerabilities and protections available to combat these problems. Questions concerning security evaluation and auditing are structured as to general security evaluation applications most appropriate at particular stages of evaluation implementation.

To reiterate, the population sampled consists of medium-sized counties within the state of Texas, ranging in population from between 100,000 and 700,000. The sampling frame is taken from the *1995 Texas State Directory*. Surveys were sent to the county seat of each county, addressed to the "Data Processing Manager." This survey was pre-tested before being sent out by Dr. George M. Weinberger of Southwest Texas State University. Dr. Weinberger qualifies as a particularly good test due to his credentials in the field of computers and the fact that he has performed similar types of surveys in the past. Finally, results garnered from the survey are tabulated into frequency distributions and simple percentages. Simple percentages are particularly useful in describing and assessing the strengths and weakness in the respondents' computer system security. See Appendix B for survey instrument example, Appendix C for background data profile, and Appendix D for subject area profile.

Respondents

The survey respondents are 27 county Data Processing Managers employed by the target counties. The sampling frame comes from the *1995 Texas State Directory*. These particular 27

counties constitute what are considered to be, by this study, as medium-sized counties within the state of Texas. The population range is from between 100,000 to 700,000 in population. The total population of these 27 counties totals 6,390,026; the approximate middle third of the total population of Texas, which is 18,378,185. See Table 5.1, page 65, for the list of target counties, and Texas Agricultural Extension Service map of counties, Appendix E, for locations.

Operationalization of Conceptual Framework

This survey was mailed to the Data Processing Managers of all 27 medium-sized counties within the state of Texas. The survey consists of 15 background data and 73 subject area questions. This survey takes approximately 15 minutes to complete.

The survey instrument is organized along the lines of the conceptual framework. Questions concerning hardware, software, data, and personnel security, are structured by the vulnerabilities inherit in each area, as well as, security measures available to combat those vulnerabilities. Security evaluation and auditing is organized by distinct stages of evaluation auditing, such as initial stage, development stage, and operation and maintenance stage.

See Table 5.2, page 66, for questionnaire relation to key concepts.

Once it is determined what type of data is to be gathered, that data must be organized. Once data is organized, it is easier to understand the implications of the findings produced by the data. The following chapter organizes and summarizes those findings.

while the last chapter uses those findings to provide conclusions and implications for the results.

Table 5.1: List of Target Counties By Population

	Name	Population	Map Location
1.	El Paso	664,800	Far West
2.	Travis	646,437	South Central
3.	Hidalgo	461,015	South
4.	Collin	326,153	North Central
5.	Denton	320,123	North Central
6.	Nueces	310,881	Coastal Bend
7.	Cameron	299,584	South
8.	Fort Bend	280,026	Upper Coast
9.	Jefferson	242,861	Upper Coast
10.	Galveston	234,690	Upper Coast
11.	Lubbock	230,525	South Plains
12.	Montgomery	222,157	Upper Coast
13.	Bee	215,480	South Central
14.	Brazoria	211,524	Upper Coast
15.	McLennan	197,173	Central
16.	Williamson	172,666	Central
17.	Webb	163,062	South
18.	Smith	159,000	Northeast
19.	Brazos	130,387	Central
20.	Wichita	124,053	Rolling Plains
21.	Ector	123,128	Far West
22.	Taylor	121,902	West Central
23.	Midland	114,165	Far West
24.	Gregg	109,785	Northeast
25.	Johnson	104,278	North Central
26.	Potter	102,928	Plains
27.	Tom Green	101,243	West Central
		TOTAL	6,390,026

See Appendix E for location of target counties.

Table 5.2: Questionnaire Relation To Key Concepts

KEY CONCEPTS	RELATED QUESTIONS (#'s)
Hardware Security	---
Accidental Physical Destruction	1-2
Intentional Physical Destruction	3-9
Environmental Destruction	10-12
Natural Disasters	13-18
Software Security	---
Deletion	19-22
Modification	23-25
Theft	26-28
Data Security	---
Interception	29-34
Modification	35-38
Unauthorized Access	39-44
Personnel Security	---
Improper Training	45-48
Incompetence	49-52
Disgruntled Employee	53-61
Security Evaluation/Audit.	---
Initial Stage	62-65
Development Stage	66-68
Operation / Maintenance Stage	69-72

See Appendix D for more detail.

CHAPTER 6
RESULTS

The purpose of this chapter is to organize the results of the data which were gathered. In the case of this particular study, simple frequency distributions and percentages are used. This technique for presenting data is very useful in describing the strengths and weaknesses in the computer security systems of Texas county governments.

Results are organized using the conceptual framework presented in Chapter 3, and the survey instrument as presented in Appendix B. Major security categories consist of hardware, software, data, personnel, and security evaluation and auditing. Hardware, software, data, and personnel, are further divided by particular vulnerabilities inherit within each area. Security evaluation and auditing data is organized by the particular stages of security measure implementation.

Twenty-seven Texas counties were identified as medium-sized counties, ranging in population from 100,000-700,000. All twenty-seven counties were sent surveys on January 9, 1996, with follow up surveys sent to non-respondents on February the 2nd and 28th, 1996. Further, phone calls were made to select counties prior to the February 28th mail-out. Eight counties returned the surveys, making for a 29% response rate. These eight counties constituted those responding to the initial mail-out on January the 6th. According to Babbie (1995, p. 262), a response rate of at least 50% is "adequate for analysis and reporting." If the response rate is lower

than 50%, there is a possibility of response bias, where samples taken are not representative of the total population. (Babbie, 1995, p. 261) However, a response rate of 29% should still be considered a fairly decent rate of return, especially in light of the sensitive nature of the present subject matter.

Background Data

The counties which responded to this survey fell within the targeted population range of between 100,000-700,000. The particular job titles of those who were in charge of data processing was very diverse. These titles are as follows: System Network Administrator, Management Information Systems (MIS) Director, Director of Computer Services, Director, Director of Information Services, Computer Tech, Computer and Network Services Manager, and finally, Wide Area Network (WAN) Manager.

As expected, counties use their computer systems for all facets of county operation. Some of the major uses of computers include: personnel (including payroll and records), all facets of law enforcement (including warrants, booking, records, drug task forces, etc.), taxes (including assessment, records, and administration), judicial (administration and cases), and others such as health department records, personal computer training, and general county administration.

All eight respondents are linked by a Local Area Networks (LAN's). The type of linkages used within the framework of these LAN's include the three major types including: twisted pair cable, coaxial cable, and fiber optic lines which are more difficult to tap into. (See Chapter 3)

Only 3 of the respondents (38%) either contract out for their data processing needs, or provide services for other organizations. The most common type of services contracted out for were hardware installation, software packages, and other programming needs. The type of services provided for other organizations include such things as tax billing and processing, administration of employment records, and particular information to title companies.

Two of the respondents (25%) claimed that they had experienced security violations. Both of these involved unauthorized data access. One of the respondents had experienced unauthorized data access by a former employee. The response to this violation was to change passwords soon after termination, make monthly user ID and password changes, monitor modem access and print an audit trail of this access, keep an audit trail of file changes and activities, and, finally, not allow access to the computer system by shutting down modems after 5:00 PM.

The other respondent that claimed to have experienced a security violation specified that this was done by remote access. This respondent explained that to remedy their particular security violation, a system of data encrypted modems and triple password protection was instituted. Both respondents claimed to have instituted these measures immediately after the violations were discovered.

See Table 6.1: Summary of Background Information.

Table 6.1: Summary of Background Information

Background Information	Freq.	%
General Information	---	---
Number of Personnel	2-18 Avg. 9	---
Population of County	100,000 - 700,000	---
Computer Related Information	---	---
Linked by Local Area Network (LAN)	8	100
Linked by Wide Area Network (WAN)	4	50
Contract Out for Data Processing	3	38
Provide Services for Other Organ.	3	38
Experienced Security Violations	2	25
Those Violated, Taking Remedial Action	2	100

Hardware Security

Hardware security, as outlined in Chapter 3, can be divided into four major areas of concern or vulnerabilities. Those areas of concern are accidental physical destruction, intentional physical destruction, environmental destruction, and threats from natural disasters. In the area of accidental physical destruction, the respondents show a fair response to such threats. For example, 5 of the respondents (63%) have policies restricting food or drink near computer equipment. Only 1 respondent (13%), however, indicated using protective coverings for computer equipment when it is not in use.

The responding counties show a poor ability to deal with the threat of intentional physical destruction. The major deterrent to intentional physical destruction is that of policies restricting computer use. Seven of the respondents (88%) have policies restricting computer use to authorized personnel only. However, devices such as equipment locks are used by only one respondent, devices which sense hardware tampering are non-existent, and TV monitors which monitor access to computer areas are used by only 3 respondents (38%). Finally, only 1 respondent has a fence which surrounds the building that houses their computer equipment, but 5 respondents (63%) do have bright lighting on this particular building at night.

In the area of environmental destruction, the responding counties scored very high. Seven of the respondents (88%) had inspected their computer room for environmental hazards, such as

water pipes, as well as, ensured that their computers had their own power source. Finally, all respondents indicated that their computer room had its own controlled environment, such as air conditioning, ventilation, and heating.

The responding counties also scored high in the area of natural disaster protection. Seven respondents (88%) had their computer equipment located on or above the first floor (flood protection), and fire detection equipment in the computer room. Six respondents (75%) indicated that the walls of their computer room were made of fire retardent material. All respondents, however, had fire extinguishing equipment located within the computer room, and employed data backup. Finally, seven of the respondents (88%) indicated that their data backup was located off-site, meaning that their backup data would not be destroyed along with their original data when a disaster occurred.

See Table 6.2: Summary of Hardware Security.

Table 6.2: Summary of Hardware Security

Vulnerabilities/Security Measures	Freq.	%
Accidental Physical Destruction	---	---
Policies Restricting Food or Drink	5	63
Protective Coverings Over Equip.	1	13
Intentional Physical Destruction	----	---
Equipment Locks on Hardware	1	13
Devices Which Sense Tampering	0	0
Require I. D. for Access to Equip.	2	25
TV Monitors	3	38
Policies Restricting Computer Use	7	88
Fence Surrounding Building	1	13
Bright Lighting Outside at Night	5	63
Environmental Destruction	---	---
Computer Room Inspect. for Equip. Haz.	7	88
Computer Has Own Power Source	7	88
Computer Has Controlled Environment	8	100
Natural Disasters	---	---
Computer Located On Above 1st Floor	7	88
Fire Detection Equip. in Computer Room	7	88
Fire Ext. Equip. in Computer Room	8	100
Walls of Computer Room Fire Retardent	6	75
Data Backup	8	100
Backup Data Located Off-Site	7	88

Software Security

Software security, as outlined in chapter 3, can be divided into three major areas of concern or vulnerabilities. Those areas of vulnerability include software deletion, modification, and theft. In the area of deletion, the responding counties show a fair ability to deal with the problem. Four of the respondents (50%) have configured their software files so as to avoid accidental deletion. Five of the respondents (63%) periodically check their hardware wiring, so as to prevent software vulnerability. Only one respondent (13%), however, makes use of dongles or other key-like devices to prevent unauthorized access to software files. Finally, only two respondents (25%) have encrypted access to their software files.

The responding counties score well in the area of software modification. Five of the respondents (63%) have "vaccinated" their programs against computer viruses. Seven respondents (88%) use only licensed software, and six respondents (75%) do not allow the use of shareware or other programs brought from home. Both of these measures help to prevent the incursion of a computer viruses into their system.

In the area of software theft, the responding counties score rather poorly. Only 2 respondents (25%) possess software that can be read only by their organization's equipment. Further, only 2 respondents (25%) indicated that they apply for copyright or patent protection of software that is developed by their organization. Finally, only 3 respondents (38%) indicated that they require employees to wave their rights to software developed by them on organization time. See Table 6.3: Summary of Software Security.

Table 6.3: Summary of Software Security

Vulnerabilities/Security Measures	Freq.	%
Deletion	---	---
Software Files Config. to Avoid Acc. Delet	4	50
Hardware Wiring Checked Periodically	5	63
Dongles	1	13
Access to Software Files Encrypted	2	25
Modification	---	---
Programs "Vaccinated"	5	63
Use Only Licensed Software	7	88
Do Not Allow Use of Shareware	6	75
Theft	---	---
Software Read Only by Organ. Equip.	2	25
Apply for Copyright or Patent Protect.	2	25
Require Employ. to Wave Rights to Soft.	3	38

Data Security

Data security, as outlined in Chapter 3, is divided into three major areas of vulnerability. Those areas of vulnerability include data interception, modification, and deletion. In the area of data interception, the respondents show a fair response to such threats. Four of the respondents (50%) indicate that they shield their computer equipment to guard against electro-magnetic radiation emanation, which, with the proper equipment, can be read. Further, 50% of the respondents run their communication lines through electrical pipe, which also has the effect of reducing the vulnerability to message interception. Only 2 respondents (25%) indicate that they shield their communication lines in such a manner as to reduce the emanation of readable electro-magnetic radiation.

None of the respondents run their communication lines through gas filled pipes hooked to alarms. Six of the respondents (75%) indicate that they use fiber optic cable for communication lines. Fiber optic lines, as discussed in chapter 3, are much more difficult to tap into. These same respondents, however, as was indicated in their background data, also use twisted pair and coaxial cable, which are easier to tap into. Finally, only two respondents (25%) indicate that they use data encryption to protect against message interception.

In the area of data modification, the responding counties score rather poorly. Only four respondents (50%) employ the use of backup services to guard against communication disruptions. Only one respondent (13%) makes use of authentication services to verify the ID of a message origin, or time stamps to verify contacts made.

Finally, no respondent made use of digital signatures for verifying the ID of message origins.

In the area of unauthorized data access, the respondents show a fair response to such threats. All eight respondents (100%) indicate that they restrict data access according to sensitivity level, and require passwords for data access. Only one respondent (13%), however, indicated that they use access control software to control data access. One respondent (13%) indicates that they use "firewalls" (dedicated access control computers) to control access to their organization's data. Half of the respondents (50%) indicate that they make use of "filters" to keep data that is unauthorized to leave the organization, from leaving. Finally, only 1 respondent (13%) indicates that their organization makes use of security test software such as Tripwire or SATAN.

See Table 6.4: Summary of Data Security.

Table 6.4: Summary of Data Security

Vulnerabilities Security Measures	Freq.	%
Interception	---	---
Comp. Equip. Shielded to Reduce EM Rad.	4	50
Commo. Lines Shielded to Reduce EM Rad	2	25
Commo. Lines laid in Gas Filled Pipes	0	0
Commo. Lines Run Through Elec. Pipe	4	50
Fiber-Optic Cable for Commo. Lines	6	75
Encrypt Data	2	25
Modification	---	---
Authent. Services for Message Origin ID	1	13
Digital Signatures for Mess. Origin ID	0	0
Time Stamps to Verify Contacts	1	13
Backup Services for Commo. Disruption	4	50
Unauthorized Access	---	---
Use Access Control Software	4	50
Data Access Restricted by Sensitiv. Lev.	8	100
Passwords Required for Data Access	8	100
"Firewalls" to Control Data Access	1	13
Filters to Prevent Unauth. Data Leaving	4	50
Security Test Software-Tripwire, SATAN	1	13

Personnel Security

Personnel security, as outlined in Chapter 3, can be divided into three areas of concern, or types of vulnerabilities. Those vulnerabilities consist of improper training, incompetence, and disgruntled employees. In the area of "improper training," the responding counties scored fairly well when it comes to providing their personnel equipment training. Seven respondents (88%) gave new employees equipment training at the time they were hired. Five of the respondents (63%) based that training on the new employee's current level of expertise. When it comes to security training at the time of orientation, however, only 4 respondents (50%) indicated that they did so. These same respondents continue this security training after the initial orientation training.

To deal with the problem of employee incompetence, only 4 respondents (50%) indicated that they had hiring policies which were specific to computer personnel. Seven of the respondents (88%), however, indicated that they had specific job descriptions for each position and screened the background of computer personnel. Finally, none of the respondents indicated that they employed the use of polygraph examinations for more sensitive positions.

The responding counties show a mixed ability to deal with disgruntled employees. Seven of the respondents (88%) base data access on a "need to know" basis. All respondents (100%) said that they have their former employees turn in badges and keys upon termination. Six of the respondents (75%) claim that terminated employees are denied access to data and equipment, and passwords

are changed immediately upon their termination. Only four of the respondents (50%), however, log the use of their computer equipment and data access. Finally, five of the respondents (63%) indicated that they assign the responsibility of computer security to all personnel, while only 2 respondents (25%) assign one individual overall computer security responsibility.

See Table 6.5: Summary of Personnel Security.

Table 6.5: Summary of Personnel Security

Vulnerabilities Security Measures	Freq.	%
Improper Training	---	---
Personnel Given Equip. Training	7	88
Training Based on Current Expertise	5	63
Computer Secur. Training at Orientation	4	50
Comp. Security Training Continued	4	50
Incompetence	---	---
Hiring Policies Specific to Comp. Person.	4	50
Specific Job Descriptions Each Position	7	88
Background of Comp. Person. Screened	7	88
Polygraph Exams for Sensitive Positions	0	0
Disgruntled Employee	---	---
Data Access by "Need to Know"	7	88
Log Use of Computer Equipment	4	50
Data Access Logged	4	50
Individuals Assign. Comp. Sec. Respon.	5	63
One Person Respons. Overall Comp. Sec.	2	25
Terminated Employees Denied Access	6	75
Former Employees Turn in Badges, Keys	8	100
Passwords Changed Upon Termination	6	75
Locks Changed Upon Termination	2	25

Security Evaluation and Auditing

Security evaluation and auditing, as discussed in Chapter 3, consists of three stages of development. Those stages consist of the initial stage where computer security evaluation is first implemented, the development stage where these measures are evaluated and changed as necessary, and the operation and maintenance stage where computer security is further checked for overall results. In the "initial stage," five of the responding counties (63%) indicate that they have identified the computer components that need to be protected, and the specific hazards to those particular components. Three of the five respondents who have indicated that they identified such components and hazards, indicate that they have identified the cost to replace any losses that might occur. Finally, four of this same group of five, indicated that they have compared the cost to protect computer components, to the possible losses identified.

Within the "development stage" of security evaluation and auditing, 4 of the respondents (50%) indicate that their current security measures are evaluated for their "correctness." In other words, security measures are evaluated to see if they are the proper remedy for the perceived security problem. These same four respondents indicate that they also use qualitative analysis, instead of just quantitative, to determine the "correctness" of security measures. As mentioned in Chapter 3, not all security hazards and measures can be easily quantified, especially in terms of dollars. All 4 respondents who indicated that they also use quantitative analysis for the determination of "correctness" of security measures, indicate

that they rely on input from both technical experts and management for the determination of those qualitative measures.

In the operation and maintenance stage of security evaluation and auditing, 3 of the respondents indicated that they check the overall compliance with computer security policies determined by their organization. Four respondents (50%) indicate that security areas are divided into smaller units for more detailed evaluation. Of those 4 respondents who performed such detailed evaluations, three reassembled those smaller units to provide one large overall picture of their organization's computer security. Finally, four respondents (50%) indicated that they check the overall performance of their electronic data processing (EDP) system. As mentioned in Chapter 3, this last check is a determination of how well the entire EDP system is working, not just security measures. A badly performing system can wreak as much havoc as a insufficient security.

See Table 6.6: Summary of Security Evaluation and Auditing.

Table 6.6: Summary of Security Evaluation and Auditing

Evaluation Stages/Measures	Freq.	%
Initial Stage	---	--
Computer Components to Protect IDed	5	63
Specific Hazards IDed	5	63
Cost to Replace Losses IDed	3	38
Cost to Protect Compared to Losses IDed	4	50
Development Stage	---	---
Current Sec. Meas. Evaluated for Correct.	4	50
Qualitative Anal. of "Correct." of Sec. Mea	4	50
Qualitative Measures Determined By:	---	---
Technical Experts	---	---
Management	---	---
Both	4	50
Operation and Maintenance Stage	---	---
Overall Compliance With Security Check	3	38
Security Areas Divided for Detail. Eval.	4	50
Div. Units Reassembled for Overall Pict.	3	38
Overall Perform. of EDP System Checked	4	50

Additional Comments

Additional comments were provided by 3 of the respondents. The first respondent said, "Most data is public record, so anyone can request the public information. Passwords and menus restrict users from the operating system. The data is protected by the department head."

The second respondent said, "[We] use the IBM AS/40 and the HP-3000 minisystem. Mainly PC-LAN's are limited to Juvenile Probation, Drug Task Force, Health Department, and computer PC training."

The third respondent said, "The computer department is only about one year old. Security has only been implemented on several key systems. Security is a high priority that continues to grow as our department is able to add required staff."

CHAPTER 7
CONCLUSION

Hardware Security

Overall, it can be said that the computer security of medium-sized Texas counties is fair. When it comes to hardware security, the responding counties do well when protecting against natural disasters and environmental destruction. The fact that these counties have taken the time to inspect computer rooms for hazards, ensure that computers have their own power source, backup their data and store it off-site, indicates that they are well prepared for environmental destruction and natural disasters.

When it comes to accidental and intentional physical destruction, however, these same counties are lacking. The major deterrence to both of these calamities is policy restriction, such as policies restricting food or drink near equipment, or policies restricting computer use. To reiterate, only 1 respondent (13%) indicated that they use protective coverings over equipment to deter accidental physical destruction. Further, very few respondents employed such measures as equipment locks on hardware not in use, required ID for access to computer equipment, or used TV monitors to guard access. These deficiencies show a lack of ability to deal with these calamities.

Software Security

The responding counties show a fair ability overall to deal with software security issues. The responding counties are strongest when it comes to protecting themselves from modification of their software programs. The majority of responding counties "vaccinate" their programs against computer viruses, use only licensed software, and restrict the use of shareware or other programs brought from home.

The responding counties show a fair ability to deal with the problem of software deletion. Only half of the respondents have configured their software files in such a manner as to avoid accidental deletion. The majority have their hardware wiring checked periodically, so as to prevent software files from being vulnerable to deletion. Only one respondent (13%) uses dongles or other key-like devices to restrict access to software files. Finally, only 2 respondents (25%) have taken the extra precaution of encrypting the access to their software files.

When it comes to software theft, the responding counties show a poor ability to deal with such problems. Very few of the respondents (25%) indicated that they had software programs that could only be read by their organization's equipment. Further, very few of the respondents have applied for copyright or patent protection of software developed by their organization. Finally, only 3 respondents (38%) required employees to wave their rights to software developed by them for the organization's use.

In all fairness, it must be said that the perceived weakness in the area of software theft (waving rights to software developed) may be due to a design flaw in the survey. It was never ascertained as to how many of the respondents actually developed their own software programs. If very few counties develop their own software, then the amount of protection against this type of theft indicated by the survey, may actually indicate a high rate of protection in this particular area.

Data Security

The responding counties also show only a fair ability to deal with the problem of data security. The respondents have a fair capability of handling data interception by the fact that 50% have computer equipment which is shielded from producing electro-magnetic radiation that can be read, and run communication lines through electrical pipe to protect against tapping. While 75% of the respondents use fiber optic cable, all of the respondents indicate that they also use coaxial, and twisted pair cable which are more easily tapped into. Finally, the fact that only 25% of respondents use data encryption shows that the majority of respondents lack protection for data that is intercepted.

With regard to data modification, the responding counties show a poor ability to protect themselves. Only half of the respondents employ the use of backup services in case of communication disruption. This makes half of the respondents vulnerable to attacks that are aimed at service disruption. Only 1 respondent (13%) indicated using authentication services to verify message origins, and time stamps to verify contacts, while no respondents used digital

signatures to verify the ID of message origins. This leaves respondents open to attacks through masquerade, and repudiation of services (discussed in chapter 3).

To deal with unauthorized data access, the responding counties have done well in the areas of restricting data access by sensitivity level and requiring passwords. In other areas of unauthorized access control, however, the respondents do not perform so well. Only half of the respondents use access control software and "filters" which prevent unauthorized data from leaving. Only one respondent uses "firewalls" (dedicated access control computers) and security test software, such as Tripwire or SATAN, which test for weaknesses in data security. All of these weaknesses point to the fact that data access security is weak. There is not much real protection from unauthorized access, and once data security is breached it, there is not much protection in place to prevent that data from being stolen.

It must further be mentioned that both respondents who had experienced computer security violations, experienced those violations in the area of unauthorized data access. Nothing was mentioned as to whether data had just been read, or whether there had been some form of data modification or destruction. If security measures such as "filters" and "firewalls" had been in place, or if security test software had been used to probe for, and correct, weaknesses, these violations may have been avoided. The fact that this was the only type of security violation experienced (unauthorized data access) by 25% of the respondents shows this to be a weak area that needs to be addressed.

Personnel Security

In the area of personnel security, the responding counties perform fairly well. To deal with the problem of improper training, the majority of counties indicate that they give new personnel equipment training and base this training on the employee's current level of expertise. Only half, however, provide computer security training at the time of orientation, or continue that training once given. This indicates that computer security training is not as important as technical expertise. This may send an unintended message that computer security is not that important.

The responding counties perform fairly well when it comes to guarding against incompetent personnel, by the fact that the majority have specific job descriptions for each position and screen the background of computer personnel. It is interesting to note, however, that none of the respondents make use of such things as polygraph examinations for more sensitive positions. This may indicate either a distaste for using such screening methods, or confidence that any irregularities will be discovered during the screening process.

The responding counties also perform fairly well when dealing with the problem of disgruntled employees. The fact that the majority of respondents assign data access on a "need to know" basis, deny data access to terminated employees, change passwords upon their termination, and have them turn in badges and keys (all immediately), shows that the respondents are dedicated to protecting themselves from this problem. The main criticisms that can be

mentioned are that only half of the respondents log data access or computer use. Without these events being logged, it may be more difficult to ascertain who committed a security violation. Finally, though most respondents assign individual computer users responsibility for security, very few (25%) assign one person overall responsibility for computer security. This may have the effect of making it difficult to hold any one person accountable for a security violation, due to the fact that everyone is responsible.

Security Evaluation and Auditing

Security evaluation and auditing is another area that the responding counties performed fairly. Five of the respondents (63%) have identified the computer components to be protected and their specific hazards. Three of those five respondents indicated that they had identified the cost to replace possible losses, and four of those same five compared the cost of protection to the cost of replacement. All of this indicates, however, that half of the responding counties have not completed the first, or initial stage, of security evaluation and auditing. Without the proper evaluation of items to be protected and cost to protect them, counties will have difficulty ascertaining the proper security measures needed to protect their computer systems.

It is good to note, however, that those responding counties who did indicate that they performed the initial stage of security evaluation and auditing, went further by going into the second stage of evaluation and auditing (development stage). This was indicated by the fact that half of the respondents evaluated their security measures for "correctness," and also performed qualitative checks of

those measures. This shows that the respondents are concerned with ensuring they have the proper security measures in place to deal with any perceived security problems.

Finally, the results of the survey suggest that the majority of those respondents who performed the first two stages of security evaluation and auditing, also went on to the third stage (operation and maintenance stage). The majority of those who completed the first two stages, checked overall compliance with stated security policies and the overall performance of their electronic data processing (EDP) systems. Further, most of this same majority divided computer security areas for more detailed evaluation and reassembled those divided security areas, for an overall picture of their computer security situation. All of this indicates that the majority of those who take the time to initiate security evaluation and auditing, perform all three stages. On the other hand, it must be mentioned that only roughly half bother to do so. As was mentioned earlier, especially in chapter 3, proper computer security begins with a proper security evaluation and audit. Without one, it is difficult to ascertain the proper protection needed for a computer system.

Possible Further Studies

This concludes this research project. A further study of the security measures of medium-sized Texas counties should be made, especially in light of 29% response rate in this present research. In the future, other studies could be made comparing the computer security of medium-sized counties to other counties, both small and large, or even all three. Another angle of research might be to study the computer security measures of counties and compare those to the security measures found in municipalities or state agencies.

One of the main contributions of this particular research is the questionnaire that was devised to gather the data. Due to its comprehensive nature, counties, or other organizations, could use this questionnaire as an computer security assessment tool. No matter what assessment tools are used, however, further investigation into the effectiveness of security measures is an imperative undertaking. This is especially true in light of the rampant and potentially destructive nature of computer crime.

APPENDIX A

LIST OF ACRONYMS

COMSEC-Communication Security

DES-Data Encryption Standards

DIR-Department of Information Resources

FIPS PUBS-Federal Information Processing Standards Publications

NBS-National Bureau of Standards

NIST-National Institute for Standards and Technology

OMB-Office of Management and Budget

TAC-Texas Administrative Code

APPENDIX B

SURVEY INSTRUMENT

COMPUTER SYSTEM SECURITY SURVEY OF MEDIUM-SIZED TEXAS COUNTIES

Part 1: Introduction

The intent of this survey is to assess the type of security measures that are currently in use within medium-sized counties within the state of Texas. Due to the sensitive nature of the material, all responses and information provided will be kept strictly confidential. Thank you very much for your time and cooperation.

Part 2: Background Information

A. What is your job title?_____

B. How many personnel are directly involved in computer operations? (e.g. programmers, systems analysts, etc.)_____

C. What is the current approximate population of your county?_____

D. In what ways are computers used by your county? (e.g. courts, personnel, payroll, etc.)

_____

E. Are your computers linked by a Local Area Network (LAN) Yes____No____

F. If linked, how so? (e.g. twisted pair, coaxial cable)_____

G. Are you linked by a Wide Area Network (WAN)? Yes____No____

H. Do you contract out for any of your data processing? (e.g. from other governments, vendors, etc.) Yes____No____

I. If you do contract for services, which services do you contract for?

_____

J. Do you provide data processing services for other organizations? Yes____No____

K. If you do provide services for other organizations, which services do you provide?

_____

L. Has your computer system experienced any security violations? Yes____No____

M. If so, what type of violations have you experienced? (e.g. unauthorized access, software theft, etc.)_____

N. Have you initiated procedures to remedy the problem? Yes____No____

O. If remedial measures have been taken, please describe those measures. (Remember, all information provided is strictly confidential.)

_____

Part 3: Hardware Security	Yes	N
1. Do you have policies restricting food or drink near computer equip.	____	____
2. Do you use protective coverings over computer equipment?	____	____
3. Do you use equipment locks on hardware when not in use?	____	____
4. Do you use sensing devices which detect equipment tampering?	____	____
5. Do you require badges or other forms of ID before access to computer areas is allowed?	____	____
6. Do you use TV monitors to guard access to sensitive areas?	____	____
7. Do you have policies which restrict computer use to authorized personnel?	____	____
8. Do you have a fence which surrounds the computer equip. building?	____	____
9. Is bright lighting used on the outside of the building (at night) which houses your computer equipment?	____	____
10. Have you inspected your computer equipment room for hazards to your system? (e.g. electric motors, water pipes, etc.)	____	____
11. Does your computer have its own power source?	____	____
12. Does your computer room have a controlled environment? (e.g. air conditioning, ventilation, etc.)	____	____
13. Is your computer system located on or above the first floor?	____	____
14. Do you have fire detection equipment in your computer room?	____	____
15. Do you have fire extinguishing equipment in your computer room?	____	____
16. Is the wall of your computer room made of fire retardent material?	____	____
17. Do you back-up your data?	____	____
18. Is this data back-up located off-site?	____	____

Part 4: Software Security		
19. Are files which store software programs configured to avoid accidental deletion?	____	____
20. Do you periodically check hardware to ensure that protections provided for software are still operable?	____	____
21. Do you use "Dongles" or other key like devices to prevent unauthorized use of software?	____	____
22. Is access to your software files encrypted?	____	____
23. Do you "vaccinate" programs to prevent computer viruses?	____	____
24. Do you use only licensed software?	____	____
25. Do you allow the use of "shareware" or programs brought from home?	____	____
26. Can your software only be read by your organization's equipment?	____	____
IF APPLICABLE:		
27. Do you apply for copy-write or patent protection of software developed within the organization?	____	____
28. Does your organization require employees who develop software to sign an agreement forfeiting their rights to that software?	____	____

Part 5: Data Security	Yes	No
29. Do you use computer equipment which is shielded to reduce the emanation of electro-magnetic (EM) radiation?	____	____
IF APPLICABLE: COMPUTERS ARE LINKED		
30. Do you shield communication lines between computers to reduce the emanation of EM radiation?	____	____
31. Do you run communication lines through pipes filled with gas which are connected to alarms?	____	____
32. Are your computer lines run through electrical pipe?	____	____
33. Do you use fiber-optic cable for communication lines?	____	____
34. Do you encrypt data?	____	____
35. Do you use authentication services to verify the origins of messages sent to your computer?	____	____
36. Do you use "digital signatures" to verify message origins?	____	____
37. Do you use "time stamps" to verify contacts between communicating parties?	____	____
38. Do you employ back-up services in case communications are disrupted?	____	____
39. Do you use access control software?	____	____
40. Do you restrict data access based on levels of sensitivity?	____	____
41. Do you require passwords to gain access to data?	____	____
42. Do you use "firewalls," computers totally dedicated to controlling access?	____	____
43. Do you use "filters" which prevent accessed data from leaving the organization unless authorized?	____	____
44. Do you use security test software such as Tripwire or SATAN?	____	____

Part 6: Personnel Security		
45. Are personnel given training on the computer equipment they are to use?	____	____
46. Is training based on current level of expertise?	____	____
47. Are personnel given computer security training at the time of orientation?	____	____
48. Does security training continue after orientation?	____	____
49. Are there hiring policies which are specific to computer personnel?	____	____
50. Are there specific job descriptions for each position?	____	____
51. Do you screen the background of computer personnel?	____	____
52. Do you employ measures such as polygraph examinations for the most sensitive positions?	____	____
53. Is data access limited by a "need to know" criteria?	____	____
54. Do you log the use of computer equipment?	____	____
55. Is data access logged?	____	____
56. Are individual personnel assigned particular responsibilities for computer security?	____	____
57. Is one person assigned overall responsibility for computer security?	____	____
58. Are terminated employees immediately denied access to equipment and data?	____	____
59. Upon termination, are former employees required to turn in security badges, keys, etc.?	____	____
60. Are passwords which former employees had access to changed immediately after their termination?	____	____
61. Are locks these employees had access to changed immediately?	____	____

Part 7: Security Evaluation and Auditing	Yes	No
IF APPLICABLE: COMPUTER SYSTEM SECURITY HAS BEEN EVALUATED		
62. Have you identified the components of your system to be protected?	____	____
63. Have you identified the specific hazards to your computer system?	____	____
64. Have you identified the cost to replace losses?	____	____
65. Have you identified the cost to protect your computer system from these losses?	____	____
66. Were current security measures evaluated to determine if they were the correct measures?	____	____
67. Do you also use "qualitative" measures to determine the "correctness" of security measures. (Not all security measures can be easily quantified, evaluation is more subjective.)	____	____
68. Are these qualitative measurements determined by:		
A. Technical experts?	____	____
B. Management?	____	____
C. Both?	____	____
69. Do you check overall compliance with security measures?	____	____
70. Do you divide areas of security concern (e.g. data, personnel, etc.) into smaller units for more detailed evaluation?	____	____
71. Do you reassemble these smaller units, so as, to gain an overall picture of your computer security?	____	____
72. Do you check the overall performance of your electronic data processing system (e.g. accuracy and timeliness of data).	____	____

73. **ADDITIONAL COMMENTS:** If you have any additional comments regarding your organization's computer security, feel free to comment in this section.

APPENDIX C

BACKGROUND DATA PROFILE

Part 2: Background Data

A. This information is used to determine the exact job title of the person in charge of data processing, due to the lack of standardized data processing titles within Texas counties.

B. This question is used simply to determine how many personnel are actually involved in computer operations.

C. This information is used to determine the most up to date population information.

D. This question is used to assess the particular types of services respondents use their computer systems for.

E. This information is used to determine whether or not respondents have inter-linked systems.

F. This information is used to determine the most common types of communication mediums used by respondents for local linkage.

G. This information is used the same as in question E, but has the emphasis on a wider area of distribution.

Note for questions E and G: According to the literature, when computers are linked, they become more vulnerable due to remote access possibilities.

H. This question is used to determine how many respondents contract for their data processing needs.

I. This information is used to determine the types of services respondents contract for.

J. This information is used to determine whether or not respondents provide computer services for other organizations.

K. This question is used to determine the particular types of computer services respondents provide for other organizations.

L. This question is used to determine how many respondents have experienced violations in the security of their computer systems.

M. This information is used to determine the particular types of computer security violations respondents have experienced.

N. This information is used to determine whether or not respondents who did experience violations took remedial action.

O. This question is used to determine the types of remedies taken.

APPENDIX D
SUBJECT AREA PROFILE

Note: All questions in Subject Area Profile are used to determine if certain computer security measures (protections) are in place to guard against particular vulnerabilities.

Part 3: Hardware Security

Questions 1 and 2 are used to determine whether or not respondents have protection against the accidental physical destruction of hardware.

Questions 3, 4, 5, 6, 7, 8, and 9, are used to determine whether or not respondents have protection against the intentional physical destruction of hardware.

Questions 10, 11, and 12, are used to determine whether or not respondents have hardware protected against environmental destruction.

Questions 13, 14, 15, 16, 17, and 18, are used to determine whether or not respondents have hardware protected against natural disasters.

Part 4: Software Security

Questions 19, 20, 21, and 22, are used to determine whether or not respondents have protection against software deletion.

Questions 23, 24, and 25, are used to determine whether or not respondents have protection against software modification.

Questions 26, 27, and 28, are used to determine whether or not respondents have protection against software theft.

Part 5: Data Security

Questions 29, 30, 31, 32, 33, and 34, are used to determine whether or not respondents have protection against data interception.

Questions 35, 36, 37, and 38, are used to determine whether or not respondents have protection against data modification.

Questions 39, 40, 41, 42, 43, and 44, are used to determine whether or not respondents have protection against the unauthorized access of data.

Part 6: Personnel Security

Questions 45, 46, 47, and 48, are used to determine whether or not respondents have protection against improperly trained personnel.

Questions 49, 50, 51, and 52, are used to determine whether or not respondents have protection against incompetent personnel.

Questions 53, 54, 55, 56, 57, 58, 59, 60, and 61, are used to determine whether or not respondents have protection against disgruntled employees.

Part 7: Security Evaluation and Auditing

Questions 62, 63, 64, and 65, are used to determine whether or not respondents have performed the initial stage of security evaluation, which involves "risk analysis."

Questions 66, 67, and 68, are used determine whether or not respondents have advanced to the next highest level of security evaluation. This "development stage" basically involves verifying that security measures in place are the correct ones.

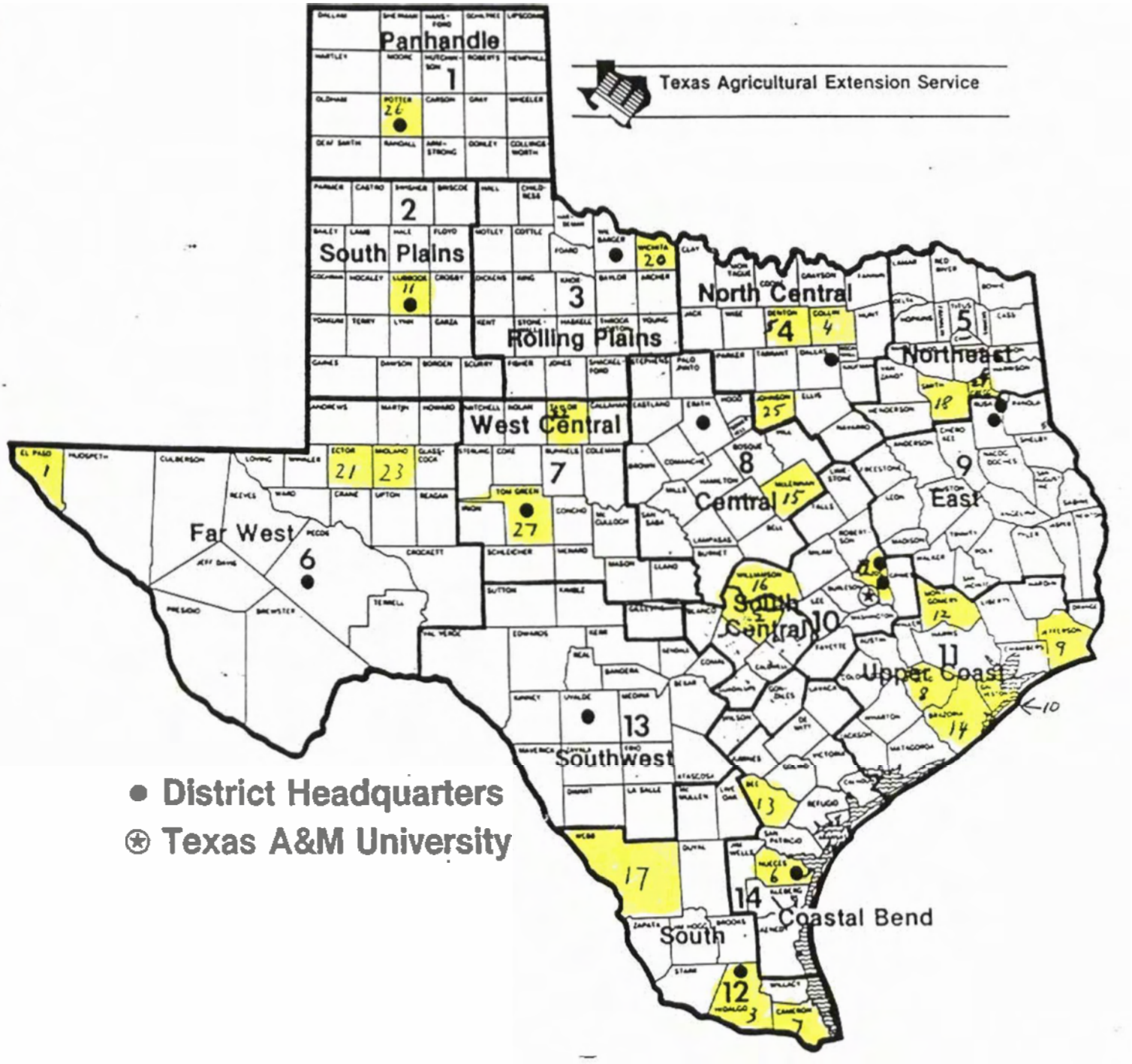
Questions 69, 70, 71, and 72, are used to determine whether or not respondents have advanced to the highest level of computer security evaluation. The main emphasis of this "operation and maintenance stage" is compliance with security policies and the overall performance of both computer security measures and basic data processing services.

Additional Comments:

Question 73 is used to gather information and insights from respondents that can not be gathered in the form of predetermined response categories.

APPENDIX E

MAP OF TEXAS COUNTIES



REFERENCES

Babbie, Earl R., (1995). The practice of social research, 7th ed. Belmont, CA: Wadsworth Publishing Company.

Bradbard, D. A., Norris, D. R., & Kahai, P. H., (Jan. 1990). Computer security in small business. Journal of Small Business Management, 28, 9-19.

Business Week. (Sep. 26, 1983). Computer security: What can be done. Business Week, pp. 126-130.

Buss, M. D., & Salerno, L. M., (Mar./Apr. 1984). Common sense and computer security. Harvard Business Review, 62, 112-121.

Cortese, Amy. (Mar. 13, 1995). Warding off the cyberspace invaders. Business Week, pp. 92-93.

Daly, J., & Anthes, G. H., (Feb. 14, 1994). Internet users go on the alert. Computerworld, 28, 14.

Department of Information Resources (DIR). (Feb. 1, 1990). Instructions for the agency plans for information resources management: Fiscal years 1991-1995. Austin, Texas: DIR.

Department of Information Resources (DIR). (Nov. 1990). State strategic plan: For information resources management. Austin, Texas: DIR.

Department of Information Resources (DIR). (Mar. 1993). Information resources security and risk management: Policy, standards, and guidelines. Austin, Texas: DIR

Forester, Tom. (Mar. 1990). (Mar. 1990). Software theft and the problem of intellectual property rights. Computers & Society, 20, 12-25.

Grover, Derrick. (Ed.). (1989). The protection of computer software-its technology and applications. Cambridge, Great Britain: University Press.

Guynes, C. S., & Vanecek, M. T., (Apr. 1981). Computer security: The human element. Personnel Administrator, 26, 71-77.

Lobel, Jerome. (1986). Foiling the system breakers: Computer security and access control. New York, New York: McGraw-Hill Book Company.

Mandell, Steven L., (1992). Computers and information processing: Concepts and applications. (6th ed.). St. Paul, MN: West Publishing Company.

Miller, Frederick W., (Aug. 1978). A 'common sense' approach pays off. Infosystems, 25, 39-42, 46.

Muir, James A., (April 1994). Browsing the Internet. San Marcos, TX: Southwest Texas State University.

Norwood, Robert E. & Strawn, Sabrina. (Nov. 1984). Texas county government: Let the people choose, 2nd ed. Texas Research League.

Neumann, Peter G., (Apr. 1994). Risks of passwords. Communications of the ACM, 37, 126.

Neumann, Peter G., (Jun. 1995). Computer vulnerabilities: Exploitation or avoidance. Communications of the ACM, 38, 138.

Pfleeger, Charles, P., (1989). Security in computing. Englewood Cliffs, New Jersey: Prentice-Hall.

Purser, Michael. (1993). Secure data networking. Boston, MA: Artech House.

Rice, Mitchell F., Alsobrook, R. A., & Weinberger, G. M., (Mar. Apr. 1982). Computer security in small local governments in Texas. Texas Business Review, 100-104.

Rotenberg, Marc. (Mar. 1990). Prepared testimony and statement for the record on computer virus legislation. Computers & Society, 20, 12-25.

Russell, D., & Gangemi Sr., G. T., (1991). Computer security basics. Sebastopol, CA: O'Reilly & Associates, Inc..

Srinivasan, C. A., & Dascher, P. E., (Aug. 1986). Access control assures network security. The Internal Auditor, 44, 40-45.

Stallings, William, Ph.D., (1995). Network and internetwork security principles and practice. Englewood Cliffs, New Jersey: Prentice-Hall.

Texas Agricultural Extension Service Map of Texas Counties.

Texas Department of State, County Population Statistics. (Dec. 6, 1995). World Wide Web (WWW), Internet.

U. S. Congress, Office of Technology Assessment (OTA). (Sep. 1994). Information security and privacy in network environments. Washington, D. C.: U. S. Government Printing Office.

U. S. Congress, Office of Technology Assessment (OTA). (Jun. 1995). Issue update on information security and privacy in network environments. Washington, D. C.: U. S. Government Printing Office.

U. S. Department of Commerce/National Bureau of Standards. (Sep. 27, 1983). Guideline for computer security certification and accreditation. (FIPS PUB 102). Washington, D. C.: U. S. Government Printing Office.

U. S. Department of Justice, Justice Management Division. (Nov. 1988) Basic considerations in investigating and proving computer-related crimes. Washington, D. C.: U. S. Government Printing Office.

Vernon's. (1994). Texas penal codes annotated, Section 33. St. Paul MN.: West Publishing Company.

Watson, Katrina. (Jan. 1985). The very soul of honesty. Business Atlanta, 14, 68-73.

Yin, Robert K. (1994). Case study research: Design and methods, 2nd ed. Thousand Oaks, CA: Sage Publications, Inc.