1990

Data Security: The Securing of Computer Installations and Data Sets

Willy B. Kuehnle

1990

DATA SECURITY: THE SECURING OF COMPUTER INSTALLATIONS AND DATA ASSETS

Willy B. Kuehnle, B.A.

An Abstract Presented to the Faculty of the Graduate
School of Lindenwood College in Partial
Fulfillment of the Requirements for the
Degree of Master of Business Communications

1990

ABSTRACT

This thesis will focus on the study of data and its value to the organization, and ways to protect data from harm. Threats to data integrity take two main forms: human intervention and acts of nature. Also discussed in detail are countermeasures to make data secure from these threats.

The decentralization of computing power has vastly increased the threats to the database. For most organizations, this base of information is the single most valuable asset they own. Yet many data processing administrators do not protect this wealth of data from harm as they should.

It is hard to "sell" security planning and procedures to upper management for two significant reasons.

The first concerns the notion many managers have that the data is secure just because it is stored in a digital format. Others do not understand data's value and blindly leave security to data administrators.

The second reason managers balk at expenditures for data and computer security is that it is hard to see the true value of the database.

Security costs money, and managers do not see a direct correlation between expenses for security and the profitability of the organization. This is sometimes hard to understand since no manager is likely to leave cash laying around, yet store data assets --printed reports, floppy disks-- in an unprotected manner.

The purpose of the present study is to investigate the true value of data and suggest a common sense approach to protect the asset from all threats.

Most of the library research is from a variety of periodicals, together with stories from newspapers, books directly related to the subject, and interviews.

The consensus of opinion suggests that few organizations value data as they should, and many lack sufficient security procedures to keep data from alteration, damage, or destruction.

DATA SECURITY:
THE SECURING OF COMPUTER INSTALLATIONS AND DATA ASSETS

Willy B. Kuehnle, B.A.

A Culminating Project Presented to the Faculty of the
Graduate School of Lindenwood College in Partial
Fulfillment of the Requirements for the
Degree of Master of Business Communications

1990

COMMITTEE IN CHARGE OF CANDIDACY:

Associate Professor Michael Castro, Chairperson and Advisor

Adjunct Assistant Professor Robert Sullentrup

Adjunct Assistant Professor Scott Intagliata

For my mother, Minnie Kuehnle, who early in my life taught me the value of education.

I gratefully acknowledge the valuable support,
and considerable time of the committee: Michael Castro,
Bob Sullentrup, and Scott Intagliata.

Also, special thanks to the light of my life, Kathy.

TABLE OF CONTENTS

List of Tables

Illustration

Preface

Everywhere we turn, magazine articles and television reports tell us that computers are used by more Americans than ever before. Some workers routinely juggle computers, programs, and networks every workday. We are also bombarded by the media's coverage of computer crime and espionage.

In the past, vast data processing centers maintained a strangle hold on the use of computer hardware and software, and practiced strict security procedures to protect the common database of information.

Today, computer systems are decentralized. Many local area networks offer the same computing power as mainframes once did. As an example, the first television computer automation system went on line at KMOX-TV, the CBS owned and operated station in St. Louis, in 1966. That first Digital Equipment PDP-8 computer contained 8 kilobytes (8k --thousands of bytes) of system memory with no provision for storage of any kind. Today's automation systems require megabytes (millions of bytes) of storage and system memory. Many vendors now speak of accessing gigabytes (billions of bytes) of storage space for today's complex computer databases.

Information, the lifeblood of today's computerized organizations, provides the grist for the day-to-day operations of many businesses today. These records may contain personnel files, accounts receivable and payable, mailing lists, and customer orders.

There is a very real need to protect this wealth of information from outside computer intruders, disgruntled employees intent on harming the organization's ability to do business, and natural disasters. With decentralized systems, computers become much harder to protect. There are considerably more entry points for invaders to penetrate.

The organization first needs to ascertain the value of its data assets in order to provide sufficient security for the resource.

Next, upper management must decide where the database is vulnerable to invasion, and develop a plan to protect their data investment.

This paper concerns itself with the value of the database, and presents appropriate actions to prevent data loss or damage.

Chapter I

INTRODUCTION

Computer security covers a lot of territory. Access controls, passwords, power conditioning, and backup and recovery plans all fall under the security administrator's control because all of these techniques affect the integrity of the computer database. Three examples help to illustrate the scope of the computer manager's responsibility for data security.

On September 21, 1985, the USPA & IRA, a Texas insurance agency and registered securities broker, discovered that 168,000 detailed records of monthly commission payroll reports were deleted from their computer system. The computer, an IBM System/38, was able to print a transaction or history log showing that someone had signed on early on the 21st and ran three unscheduled jobs. The account name used was previously unknown to the accountants and operators.

A senior systems analyst was notified, and all programs and data were backed up to 12 magnetic tapes to preserve the state of the system at the time of the erasures.

An audit trail, provided in part by the computer's history log, listed eight unsanctioned transactions. Between 3:04 a.m. and 3:47 a.m. someone logged onto the system with a clandestine account name unknown to the staff. This bogus account appeared to be a legitimate IBM maintenance account number. An individual logged

on from the same terminal as the company's computer security officer. Next came a series of log-ons and log-offs from various terminals using different account names each time. One of the accounts used was that of a recently hired programmer. Finally, three unauthorized jobs ran on the system. In the subsequent investigation, all personnel stated they knew nothing of these mysterious jobs. Several communications lines were turned off and their descriptions changed. Finally, the programmer's account was logged off the System/38.

In the following days, the computer suffered an unexplained power-down. Other problems concerning loss of communications lines popped up unexpectedly.

After a thorough analysis of history logs, and an exhaustive search through myriad directories on the System/38, three Control Language programs were discovered with the same names as the three unknown jobs that ran on the 21st.

Code changes in existing programs were discovered that called the three unauthorized programs. These unauthorized programs were the ones that caused all the problems for USPA & IRA. The illegal code was designed to delete files every month, hide the bandit programs from casual viewers, and replicate the three programs. Many man-hours later, the system was restored to its former condition with the help of journal files, backups, and manual re-entry of data.

Donald Gene Burleson was found guilty of "Harmful Access to a Computer-with loss over $2,500," in Tarrant County, Texas. On October 1, 1988, he was

sentenced to seven years probation and ordered to pay restitution to USPA & IRA of $11,800.

Burleson was the company's systems analyst and computer operations manager for a little over two years before his dismissal on September 18, 1985. Ironically, Burleson was also the company's security officer (McCown 3).

The second recent example involves Cornell University graduate student Robert Tappan Morris, the son of a National Security Agency programmer. The younger Morris was indicted July 26, 1989 for paralyzing as many as 6,200 computers when he unleashed a virus that caused an estimated $96 million worth of damage on the ARPANET computer network. Robert Tappan Morris became the first person prosecuted under a provision of the Computer Fraud and Abuse Act of 1986.

The indictment charged that Morris intentionally and without authorization accessed computers at the University of California at Berkeley, the National Aeronautics and Space Administration (NASA), Purdue University, the United States Air Force Logistics Command and other installations not specified (James Rowley AP).

Still a third recent security breakdown involved a benign computer virus, known as the Aldus Virus. The virus was written by a Canadian journalist associated with MacMag magazine. The virus broadcast a "Peace Message" on March 2, 1988,

and then deleted itself from Macintosh computers running Aldus Freehand software. This is thought to be the first time that off-the-shelf software was infected with a virus program. Up until this point, most computer users believed that "shrink-wrapped" programs from reputable software publishers were immune to this form of computer manipulation (Computer Virus Handbook AI 12).

These illustrations point out the need for better computer security. The Burleson case addresses the need for stricter system controls and cross checks in business computers. In the Morris trial, we find that thousands of expensive computers used in education and scientific endeavors were not able to function --some not for days-- until the virus could be eradicated. The Aldus Virus teaches us a lesson concerning the vulnerability of computer systems. It is estimated that the "Peace Message" alone was seen on 350,000 Macintosh screens (Fites, Johnson, Kratz 20).

This staggering estimate clearly shows the magnitude of interconnection between computers today. Through computer bulletin boards, information utilities and networks this kind of interconnectivity became possible during the decade of the 1980's.

What if the Aldus Virus did more than deliver a message of good will? What if it deleted files on thousands of hard disks? What if Burleson's antics had not been caught before irreparable harm was done? What if Morris' virus couldn't be contained? The cost to reprogram the thousands of computers linked by ARPANET and associated sub-networks could easily have reached the billions of dollars.

Thankfully, the ARPANET virus did not destroy data in the scores of Digital Equipment VAX computers it invaded. It only filled up available memory bogging the systems down to a fraction of their normal computing power.

In the early days of computing, giant machines demanded staggering amounts of man-hours and money to perform a single calculation. These machines resembled later mainframe computers, but were actually electronic or electro-mechanical calculators. The first true computer capable of storing a program within its own memory was the EDVAC (Electronic Discrete Variable Computer) introduced to America in 1952 (Augarten 141).

The men and women who programmed these room-filling behemoths of computation became the "czars" of their era. The bureaucracy of fledgling data processing departments with layers of insulation between end users and data processing (DP) managers meant long delays between request and job completion (Baker 6).

The first true computers of the 1940's and 1950's, with internal memory, used thousands of vacuum tubes as electronic switches. In the late 40's a turning point came in the development of computer components. Solid state components called transistors were perfected and proved much more reliable, consumed far less electricity, and made computers much smaller (Augarten 297). The electronic revolution didn't stop with solid state components, though. Next came the integration

of large numbers of components into small silicon chips called integrated circuits (ICs). The Fairchild Camera & Instrument Corporation announced the development of their first integrated logic circuits in 1961 (Augarten 225).

Developments throughout the 1960's led to two important conclusions. First, large computers could be used to great advantage where the task was repeatable, computing the same equations over and over again. Setting up separate tasks was another matter. Each new application meant delays while the machine was re-programmed for the new job.

The computer industry's response to this problem was timesharing. Many users were then able to use the computer's costly resources a few moments at a time. With time-sharing perfected, end users could run different computer applications concurrently.

With the notion of timesharing came the second conclusion. Workers didn't need to visit the computer room itself to perform their tasks. Employees could sit at their desks and input data --for instance insurance claim information-- from dedicated workstations consisting of a keyboard and monitor. These work stations were often referred to as "dumb" terminals because they had no computing power of their own. They were simply input devices.

Microprocessors, along with ICs were necessary before computing could move out of the vast computer center and onto the desktop. Microprocessors are chips that act as traffic cops, controlling the input and output functions of the computer, as

well as managing the memory of the system. With the miniaturization of components, a new form of computer became available. Personal computers (PCs) began to replace lowly terminals on business desktops across the country. This trend spawned a new form of departmental anarchy that did not want to wait months for the data processing department to change programming or make updates to their systems. They wanted to buy off-the-shelf programming and run it themselves. This became possible because PCs, unlike terminals, are capable of independent computation.

Mainframes are inherently easier to secure than desktop computers. Most mainframes operate in a data center that offers limited access to the outside world. With wired terminals, office workers communicated with the mainframe, but few had physical access to the computer itself. For the most part data center personnel were the only people authorized to work inside the computer room. Access from the terminals was controlled by passwords, and access to the DP area usually meant guards, badges, keycards, or all three.

The office worker with his own computer meant security was much harder to maintain. Small floppy diskettes could easily be transported from office to home. Sensitive hard copy printouts once stored in the secure DP center could be left laying on desks or in trash cans for prying eyes to find. With the PC revolution, it became much harder to keep track of who was running a particular application since computing power was built right into the workstation itself.

As if this wasn't bad enough for DP professionals and security administrators to swallow, as PCs began to populate work areas, it became evident that these smart terminals needed to share common databases with each other. They also needed to share expensive printers and other peripherals. It became clear that these individual computing workstations needed to be linked or "networked" together. Local area networks (LANs) were born to provide the interconnection between computers departmental users demanded.

As more departments wired together their own networks, it became evident that additional benefits could be gleaned by linking these networks together from building to building or city to city. Short distances could be physically wired together easily, but longer distances required modems and telephone lines. Modem is an acronym for modulator/demodualtor. A modem is a device that converts a computer's digital data to an analog format for transmission over telephone lines. At the receiving end, the analog signal is converted back to the digital data a computer understands by a second modem (Sippl 302). This is the kind of interconnect scheme that caused ARPANET so many problems when a virus invaded their computers.

Dennis W. Fife, W. Terry Hardgrave and Donald R. Deutsch, writing in their textbook *Database Concepts*, establish the fact that the data collected and stored on computers has great value: "The cost of capturing and maintaining computer data dictates that data must be preserved carefully over time and made readily accessible for many purposes" (1). Although it can be argued that data *per se* has no value of

its own, it represents great worth because of the information that can be derived from it. Also, replacing lost data may drain a vast amount of company assets.

The integrity of the data must be preserved beyond question if the database is to have lasting value. This means that it must be protected from all threats: man made as well as "acts of God."

Many organizations make a conscious decision to hush up any unauthorized penetration of their computer systems. Only 10 to 15 percent of computer crimes are ever reported to authorities, according to Hossein Bidgoli and Reza Azarmsa, reporting in the *Journal of Systems Management* (21). Managers are afraid of adverse publicity and a tarnished image. They are concerned about further intrusion attempts if their plight is made public.

In a survey conducted by Ernst and Whinney, the results indicate an increasing concern for security among computer professionals:

- 87% recognize security's importance
- 75% are implementing security policies
- 62% see security risks rising
- 42% have security orientation for new hires
- Only 6% say security safeguards are adequate (Fish 23)

Computer disaster recovery and security expert Norman L. Harris states that: "lax security is the rule rather than the exception. Organizations start out with good intentions in designing security systems, but because of pressures from budget considerations, budget cuts, or even familiarity with fellow employees, they let it [security] slip." Harris concludes that the only thing that has saved many organizations from ruin by computer security violations are honest employees. "All that is needed is a dishonest employee and their security system can be bypassed." Harris writes that lax computer security "is a time bomb just waiting to go off" (13).

Thomas J. Knapp, senior manager, Management Advisory Services at Price Waterhouse in Milwaukee, Wisconsin, states: "Managers assigned the responsibility for data security often cite problems in obtaining funding because upper-level management has not fully recognized the importance of data security project requests" (22). This is due in part to the fact that security expenditures do not make money for the organization. They are a constant drain on resources without apparent benefit. Norman Harris agrees it is hard to convince senior management of the need for strict computer security procedures. Harris writes that "they'll [management] argue security systems don't make profits. But it can be argued just as loudly that security systems can prevent devastating losses" (13).

With the explosion of PCs and networks in the workplace, the job of securing sensitive data gets harder all the time. It is clear that DP managers need to aggressively strive to protect the data entrusted to their care. It is also clear

that data integrity is the job of every member of the organization from the chief operating officer to the newest data entry clerk.

Data is the single largest asset many organizations own. Computer security, therefore, must entail more than just access control. It must be an integrated master plan for the protection and preservation of the database over time. The plan must encompass all natural disasters and unauthorized human intervention.

The following sections consider the available literature and research methods employed to collect it.

The bulk of the paper discusses the value of the data asset, presents threats to the data, and proposes countermeasures to protect the organization's computer assets.

Chapter II

REVIEW OF THE LITERATURE

My initial interest in computer security came about by accident in 1984. At the time, a friend and I were running a computer bulletin board system (BBS) open to the public. The BBS became so popular that we received over 13,000 calls before shutting the system down after two years of operation. Many innovations used on that system were the work of my friend and co-system operator Ron Francois. Ron at the time was a high school junior who lived 24 hours a day with computers. Elements like our random one-liner sign-on greetings called from a data base of over 300 user-written lines are still found on systems running today.

During the operation of the bulletin board, we were invaded on several occasions by unscrupulous hackers. For the most part, intrusions were a nuisance but did little damage to the system's ability to function. On one occasion, however, a hacker penetrated the rudimentary password security and became a super user on the bulletin board. With the attributes of super user he had the privileges of the system operator (sysop). The intruder had complete access to all the system files as well as those that were updated by users themselves. He completely erased the hard disk and effectively put the

BBS out of commission for a number of days. When the programming was restored to its operating status at the time of the last backup, many mailbox messages and files posted to the public since the backup were lost forever.

I began reading books about telecommunications in general, looking for ways to make our system more secure. Mike Cane's *The Computer Phone Book* was a starting point. The beginning chapters of Cane's book are a primer for telecommunicators. The listings of working bulletin board systems are extensive and as up-to-date as possible. Since BBS's change phone numbers and operating parameters frequently, this book is invaluable to new users because Cane provides updated lists periodically. Cane will not list a bulletin board that he has not personally logged onto at least once. The book has listings for several hundred BBS's as well as the major networks and tips for accessing on-line services like The Source and CompuServe (138).

Other books that piqued my interest were *The Joy of Computer Communications* by William J. Cook, and *Connections: Telecommunicating on a Budget* by Robert Chapman Wood. Cook's work is another good text on beginning computer communications. Wood discusses electronic mail, on-line research and offers a dictionary of communications terms.

Increasing Your Business Effectiveness Through Computer Communications was the first text I read that was directly related to business computing. This was my introduction to security and local area networks (LANs). Author

Phillip I. Good provides a good general text for business groups not familiar with computers and communications. He takes the reader from communications essentials through linking PC's into networks and on to communicating with mainframes.

With this general background information, the subject of computer security became an unconscious part of my life. Although I use computers every working day, and many hours at home, the need for increased security did not begin to take hold until I began thinking about a thesis topic. I realized I needed to know more about computer security and recovery.

In 1984, Carl Nicholai, the inventor of non-deterministic cryptography, wrote: "it is estimated that by 1992 there will be 24.4 million personal computers used in business in this country. Many engineering firms already have two computers or computer terminals per user" (64). This trend toward two or more computers on a desktop is more prevalent today than it was in 1984.

The proliferation of hardware multiplies the risk of security breaches many times over. Each computer represents a potential threat to the security of the system. Personal computers are linked together by networks. Networks are linked together to form wide area networks with thousands of terminals. Gateways allow communication between dissimilar networks or mainframe computers. Each connection is another door for intruders to check, looking

for a weak link. Because networks can make telecomputing nearly anonymous, computer intrusions are much harder to track.

Ten years ago, an article in *Industry Week* sounded one of the earliest warnings about lax computer security. Louis Scoma Jr., president of a Fort Worth computer security company, estimated that 95 per cent of all U.S. companies were ill-prepared to recover from the loss of their computers. Scoma maintained that "Many managers believe their computers and data centers are adequately protected, when actually they're not" (Much 79).

Evidently, American business leaders did not heed the warnings of Scoma and others. In April of 1989, A roundtable discussion of top computer security experts sponsored by *Network World Magazine* found a surprising number of *Fortune 1000* companies did little to protect their systems from intruders (Bolt AP).

As bad as threats may be from outsiders, threats from workers inside the company are even greater. Computer-related white collar crime in the United States is estimated at $70 billion dollars every year, according to the Research Institute of America. The Institute claims that 75 percent of that total "take" is caused by insiders (Baker 23).

Marvin M. Wofsey, president and co-founder of HSH Inc., a Columbus, Ohio consulting firm specializing in computer security, concludes: "Current employees have a prime opportunity to observe the computer system and its

controls. They can locate the weak spots, the telephone access number of the computer and passwords of other employees. If there is no audit trail, the insider can accomplish his or her desired goals from almost any terminal" (15).

In a 1983, Bill Zalud's article, *Computer Criminals Will be Prosecuted: Adopting a Prevention First Attitude*, provides an uncannily accurate picture of the potential inside computer criminal:

> He's usually 18 to 30 years old. Highly intelligent, he (usually male) is a model employee, willing to work late, eager to learn new things, to explore other company areas, involve himself in other departments to 'fight' those occasional fires where an extra set of hands is needed. He's quick to learn the computer system, to bypass the program menus, to make the system work harder and faster for the company. Potentially, he's the perfect computer criminal (30).

In the past few years, a new threat, computer viruses, became an additional dilemma for system managers. Computer viruses are executable programs like any other program except there is an added twist. Like viruses that attack the human body, computer viruses invade the host system and may lay dormant for some time before exploding into action. Also like viruses that invade humans, they are able to replicate themselves, and may eventually destroy the host system (Fites, Johnson, Kratz 23). This is the kind of program that Cornell University graduate student Robert Tappan Morris used to invade the ARPANET network.

There are many variations on the virus theme. Some appear to be benign, that is, they perform some task like writing a message on the computer screen, and then delete themselves from the system. The Aldus virus discussed earlier is such a program. Other viruses are not so easily removed from the system. In the Burleson case, investigators found that a group of programs were deployed to destroy financial records every month, remain hidden, and cause other problems like unscheduled system power downs. Since Burleson had the top clearance as the security officer for the company, he could have just as easily erased *ALL* records at one time. The fact that the system was quickly cleansed of these programs is little comfort to the USPA & IRA board of directors and chief operating officer. The nagging doubt remains that some destructive program element wasn't found. A very sobering thought to say the least.

John McAfee, president of the Computer Virus Industry Association, paints very grim pictures when speaking about the harm viruses can do to the country's main computer systems. He discusses threats to our freedom in very convincing terms. Elections can be manipulated, missile guidance systems reprogrammed and air traffic control systems sabotaged because of the intentional infiltration of viruses (McAfee, Haynes 186).

The staggering results of the *Fortune 1000* survey demonstrate that many corporate managers are still unclear about the potential risk to their

own organizations. Who is responsible for security? Is it the chief operating officer, the data processing manager or the end user? The answer is all three. They must share responsibility for the integrity of the system. Sanford Sherizen, adjunct associate professor at Northeastern University, who wrote, *Successful Security Relies on Corporate Awareness Training*, states emphatically: "Corporate security awareness must be directed to both top management and lower level user populations. The most important security official in any organization is the employee -at any level-who understands the security requirements of the *Information Age*" (10).

Noted author and professor of accounting in the College of Business and Economics at the University of Wisconsin-Whitewater, Dr. Robert Bloom writes about the problems of management computer centers:

> For executives to begin to unveil the mystery surrounding computer crime, they must be aware that knowledge of hardware isn't necessary to commit computer crime-though such knowledge may facilitate the fraud. Moreover, they must be aware that DP personnel are not control-oriented, they are typically independent-minded, identifying more with their profession than the organization they work for. Accordingly, turnover among DP personnel is high and their allegiance to particular firms limited (14).

One of the best tools for assessing the need for tighter security is risk analysis. Risk analysis provides a way to determine the actual risks to the data

and computer system, and the impact on these elements in financial terms if the system is penetrated (Knapp 22). Table 1 displays risk analysis procedure.

Once the risks are identified, the next step is to estimate the probabilities of each risk actually happening, and provide the most effective countermeasure to the threat. These measures may include loss-of-business insurance, disaster recovery plans, or additional security procedures. By 1995, Michael R. Gauthier estimates that the disaster recovery business and contingency planning industry will reach the $1 billion mark in the United States (49).

If you lock up a computer, and remove all communications lines to the system, the computer is reasonably secure. But computers were not intended to work in a vacuum. Computers are made to communicate and share information. John Ratliff writes concerning the selling of security in his article: *To Sell Disaster Recovery, Think in terms of Corporate Insurance*. Ratliff says, "without the free exchange of information via computers through all departments of an organization, a company simply cannot operate in an efficient, profitable manner. Keep in mind that the data processing function is the one system that permeates virtually all boundaries within the corporate structure" (17). If that statement is true, then it behooves every business, large and small, to have a comprehensive security and disaster recovery plan that is continually monitored for effectiveness.

Besides the references already mentioned, my library research led me to a considerable number of books, periodicals, newspaper accounts pertaining to computer security, backup and recovery procedures, and computer center management in general.

A collection of newspaper articles and wire service stories were retrieved from Vu-Text, a database service to which my employer KMOV-TV subscribes. Notable in this selection of stories were the following:

✓ A series of *Associated Press* articles by John A. Bolt on protecting computers from hackers. Bolt interviewed several experts at a roundtable discussion in Dallas, Texas.

✓ Kathleen Day of the *Washington Post* discussed corporate computer sleuthing with Michael Hershman, a former government investigator who now heads the Fairfax Group, a computer security consulting firm.

✓ A *St. Louis Post Dispatch* article concerning the lack of viruses in St. Louis corporate computers. *Post Dispatch* writer Bill Smith interviews several St. Louis big business computer users.

✓ Another *Associated Press* story by Kevin Costelloe concerned the charging of three West German hackers for selling information to the Soviet Union. The information came from military base computers and industrial computer databases in the United States.

✓ A series of articles from the *Reuters News Service* about Robert Tappan Morris, the Cornell University graduate student who planted a virus in the InterNet (formerly ARPANET) computer network. Tappan brought an estimated 6,200 computers to their knees with his virus.

✓ A series of *Associated Press* articles about the Tampa, Florida television news executives that stole computer news files from a rival TV station.

These and 39 other articles about computer crime and espionage were gleaned from the Vu-Text service thanks to KMOV. Other stories from prominent papers like *The Baltimore Evening Sun* and *The Los Angeles Times* round out my base of newspaper material.

Through the Info Trak periodical database, a total of 78 articles on various facets of computer management and security were retrieved. Some of the most useful information came from the following:

✓ An October, 1989, article by Hossein Bidgoli and Reza Azarmsa in the *Journal of Systems Management*. Mssrs. Bidgoli and Azarmsa discuss the concern of management with computer security in the 1990's. Both men are on the faculty of California State University in Bakersfield.

✓ A *Modern Office Technology* article concerning the integrity of data, and management controls to protect computer assets. Writer Marge Yonda is president of the Computer Solutions consulting firm in Rochester, New York.

✓ Thomas Knapp's July, 1983 *Data Management* article concerning the selling of security to upper management. Knapp is senior manager, Management Advisory Services at Price Waterhouse in Milwaukee, Wisconsin.

✓ From *Best's Review*, An article by system analyst Monte Garretson entitled *Think Like a Crook*. Garretson discusses record keeping and secure check writing procedures, audit trails and reports.

✓ A December, 1984 *Data Management* article by Norman L. Harris on: *Rigid Administrative Procedures Prevent Computer Security Failure*. Mr. Harris is co-founder of an Ohio disaster recovery consulting firm.

✓ Robert Bloom's *Data Management* July, 1983, article concerning the role of internal auditors, security administrators and personnel controls.

These and 72 additional articles in my possession concern every aspect of data protection including articles on fire prevention, Halon fire suppression systems, electric power conditioning for data centers, environmental concerns of computer centers and much more. Other articles of interest represent a wide variety of publications including: *Canadian Business*, *Forbes*, *Cost and Management*, *Electric Light and Power*, *Computers and Electronics*, *Dun's Business Month*, *Business Insurance* and many more.

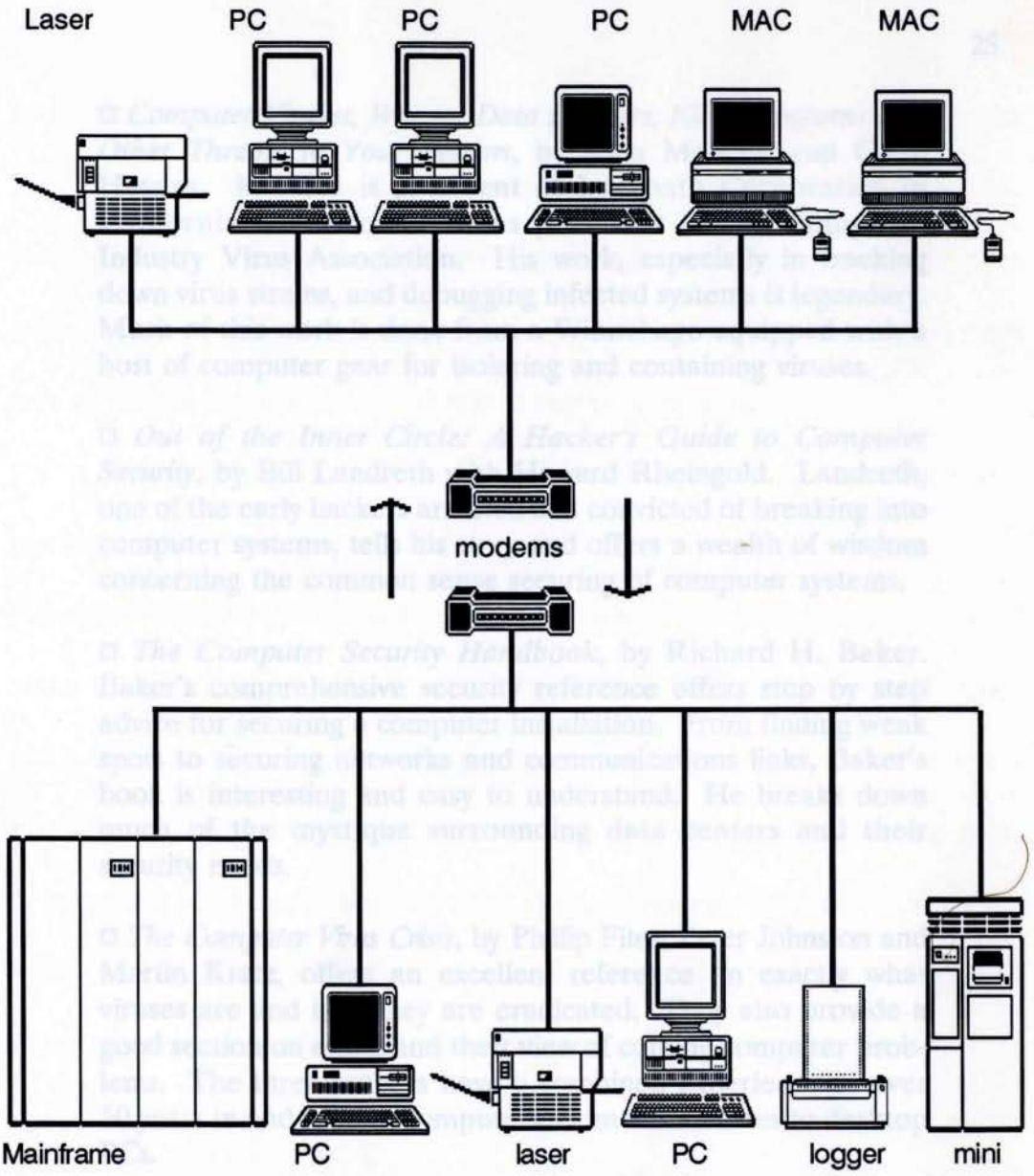
Today there is a wide variety of books relating to every facet of computer security. In the Last two years, several books concerning the plague of computer viruses have been published. Below is a listing of some of the most useful texts about computers and how to secure them:

- *The Computer Security Handbook* by Richard H. Baker
- *People and Computers* by James N. Danziger and Kenneth L. Kraemer
- *The AMA Management Handbook*, Second Edition, William K. Fallon, Editor

- *Out of the Inner Circle*, by Bill Landreth with Howard Rheingold
- *Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System* by John McAfee and Colin Haynes
- *The Cuckoo's Egg*, by Clifford Stoll
- *Crime Prevention Manual for Business Owners and Managers*, by Margaret Kenda
- *The Computer Virus Crisis*, by Phillip Fites, Peter Johnson and Martin Kratz
- *Compute!'s Computer Security*, by Ralph Roberts and Pamela Kane
- *The Small Business Security Handbook*, by James Edward Keogh

Below is the synopsis of several of the books mentioned above. It should be noted here that I own many of these texts, though not all. These references make a sound basis for computer security research. The issues presented by these authors, when added to the information obtained from interviews, periodicals and newspaper stories, provide a solid foundation concerning computer security matters.

- *The Cuckoo's Egg*, by Clifford Stoll, is the personal story of Stoll's attempts to track down a computer spy that invaded the Berkeley Livermore computer facility. Little did he realize that it would take over a year to finally catch the West German computer spy. His bouts with federal agencies including the CIA, FBI, NSA and the military are revealing. An interesting sidelight is Stoll's participation in tracking down the author of the ARPANET virus, graduate student Robert Tappan Morris.



Above are two small networks like the ones discussed earlier. The upper network consists of various IBM and Macintosh computers plus a laser printer. The lower network includes mainframe, mini (department size) computer, plus laser printer, system logger, and two workstations. The networks are joined by modem to each other. Any PC in the upper network can access any device in the bottom network if they have access priviledge (authorized account name and valid password). The two lower workstations can access all devices on the lower network they are authorized to use. They can also access the upper network devices via modem. To the end user, all the devices appear as if they are hard wired together.

Figure 1.

- *Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System*, by John McAfee and Colin Haynes. McAfee is president of Interpath Corporation in California and also serves as president of the Computer Industry Virus Association. His work, especially in tracking down virus strains, and debugging infected systems is legendary. Much of this work is done from a Winnebago equipped with a host of computer gear for isolating and containing viruses.

- *Out of the Inner Circle: A Hacker's Guide to Computer Security*, by Bill Landreth with Howard Rheingold. Landreth, one of the early hackers arrested and convicted of breaking into computer systems, tells his story and offers a wealth of wisdom concerning the common sense securing of computer systems.

- *The Computer Security Handbook*, by Richard H. Baker. Baker's comprehensive security reference offers step by step advice for securing a computer installation. From finding weak spots to securing networks and communications links, Baker's book is interesting and easy to understand. He breaks down much of the mystique surrounding data centers and their security needs.

- *The Computer Virus Crisis*, by Phillip Fites, Peter Johnston and Martin Kratz, offers an excellent reference on exactly what viruses are and how they are eradicated. They also provide a good section on ethics and their view of coming computer problems. The three authors have a combined experience of over 50 years in and around computers, from mainframes to desktop PCs.

These and other references cited throughout this paper clearly show the amount of research undertaken to acquaint myself with the topic. All of the articles mentioned would be useful for anyone researching the topic of data security.

Since my beginning premise was that *any* threat to the integrity of data is a potential problem for security administrators, it is difficult to narrow down the topic to one particular problem. Although the body of the work may seem to be a "scattershot" approach to the subject, I believe this is the only way to handle an issue as broad and complex as data security.

In concluding the review of the literature, I would like to point out a glaring discrepancy in a well-known guidebook found on many business manager's desks in the United States. The American Managers Associations' *AMA Management Handbook*, edited by William K. Fallon, is a 1,455 page tome on every aspect of building and managing a company. There are chapters on nearly every aspect of corporate life. When it comes to the topic of computer information systems, and especially security for these systems, the editor and the association decided that less than one page could adequately cover the entire subject of data integrity and computer security (8-40).

It is just such attitudes, found in upper management circles, that makes the topic of computer security so important. I believe the glossing over of a topic as important as data security is exactly why many companies today are ripe for the picking.

Table 1

A Simple Risk Survey

- What can happen?
- How likely is it to happen?
- How can it happen?
- If it happens, how much will it cost?
- What is my acceptable Risk?
- What is being done now?
- What should be done to reach the right security level?

SOURCE: *Dun's Business Month*, December 1982, Page 92.

Table 2

Risk Vs. Cost

- **Risk:** Data replacements as a result of unauthorized introduction of data or unauthorized program modification.
  - **Cost:** Cost to reconstruct data or program and ill will.

- **Risk:** Fraud losses as a result of the unauthorized introduction of data or the unauthorized program modification in order to perpetrate fraud.
  - **Cost:** Cost incurred by unauthorized transactions and fraudulent activity.

- **Risk:** Loss of business income as a result of unauthorized disclosure of business records or the inability to process data.
  - **Cost:** Lost opportunities and the inability to make decisions.

- **Risk:** Legal liability resulting from the introduction of unauthorized data or the inability to process data.
  - **Cost:** Cost of lawsuits and fines.

SOURCE: Thomas J. Knapp, *Data Management*, July 1983

Chapter III

RESEARCH METHODS

My library research was conducted in the manner described below. Through the Info Trak periodical database, a considerable collection of articles relating to management and data security in all its forms was retrieved. Articles written between 1980 and 1990 are included in this base of information. This offers a tremendous opportunity to follow trends in the computer industry through a decade of rapid change. Notable contributions came from *Data Management, Journal of Systems Management, Industry Week, Datamation, GPN, Cost and Management, Records Management* magazines, and other periodicals. All periodicals were copied from microfilm for a permanent record.

Additionally, articles from the newspaper and wire service information utility Vu-Text were retrieved. These articles included stories on computer espionage, computer viruses, security, international computer spy rings and new advances in computer protection.

The full text of the articles along with source, author, and date were printed on the newsroom printer at KMOV. It should be noted that many of the wire service stories from the Associated Press (AP) and the Business Wire were written by a pool of reporters and not a single author. In this case, the wire

services very often do not indicate who the writer is. There are several places in the paper where the source is listed as "AP," or "Business Wire." All articles are properly documented in the works cited section.

In addition, I contacted the Computer Industry Virus Association, and received four lengthy reports that include excellent illustrations. The Computer Security Institute sent a number of *Computer Security* newsletters. The newsletters were particularly helpful with information concerning the Burleson trial, computer networks and viruses.

The accounting firm of Price Waterhouse provided me with *The Computer Virus Handbook* and *Computer Viruses: A Management Perspective*, both excellent booklets geared to managers.

Ross M. Greenberg, president of Software Concepts Design, is a noted virus fighter and authority on anti-virus software. He is quoted in several books and articles concerning viruses and their detection and removal. Mr. Greenberg provided informative comments in the manual that accompanies his program *FLU_SHOT+*. Mr. Rosenberg was the victim of a virus attack himself. A hacker took a copy of his shareware program and added a virus to it. The infected software was dubbed *FLU_SHOT4* by the hacker. The virus invaded many systems since the users thought they were adding anti-viral protection to their hard disk drives. Shareware is a system whereby small computer publishers can

distribute their products at little cost to end users. Shareware is often distributed through bulletin board systems. If users like the product and plan to use it, they are asked to send a small registration fee to the publisher.

Interviews were conducted with the following: Dean Hoven, Citicorp's Mortgage Banking Treasury department computer Security Administrator, Certified Public Accountant John Deal, a partner in the accounting firm of Botz, Deal and Company, who sets up and audits computer accounting systems for small and medium size firms. The third interviewee is James Bush, an employee of Honeywell Federal Systems assigned to Scott Air Force Base in Illinois. All these men are experts in hardware, software, security, and disaster recovery.

Mr. Hoven provided insights into the problems of disaster recovery. Hoven has worked as system administrator at Citicorp for three years. Prior to his employment with Citicorp, Hoven held a similar position with Boise Cascade, now Sonoco.

Mr. Deal is a graduate of the University of Missouri at St. Louis, and is a Certified Public Accountant. Deal offered an interesting perspective to the research since some small business computer practices work well for small organizations, but fail to work for large companies. Notable is the use of "handshake" agreements for system backup. This is discussed in the recovery section of the paper.

Mr. Bush has worked with Honeywell Federal Systems in many capacities during a long tenure with the firm. He now handles hardware installation for Honeywell Federal at Scott Air Force Base. In addition, Mr. Bush will offer comments after reading the finished paper. His remarks are found in chapter V.

All the information gleaned from periodical articles, newspaper reports, reports from the industry organizations and personal interviews was transferred to a database for quick retrieval during the writing phase of the paper.

Chapter IV

DATA SECURITY: THE SECURING OF COMPUTER INSTALLATIONS AND DATA ASSETS

THE VALUE OF DATA

Although corporations possess physical assets such as manufacturing plants, office buildings, vehicles and real estate, for most organizations the data in the computer based information system (CBIS) comprises the bulk of the company's wealth. This data is essential for the day-to-day operation of the organization. It provides the base of data used by management to assess the present health of the organization. It maintains valuable records required by government and other agencies. The data is used to plot trends and forecast new avenues of expansion for the company. Without this abundance of information, the organization would soon come to a grinding halt.

The interesting point about data is that unlike computer hardware, it continues to increase in value. This happens because the amount of information contained in each record often increases over time. As time progresses, more information is added to individual records, and this data can be used to provide various forms of information for the organization's use.

There are diverse ways to use data derived from a database. For instance, transaction processing systems serve a dual role for the organization. First, transaction processing systems (TPS) provide basic record-keeping services. They provide the secondary function of furnishing processed data (information) to other computer systems in the organization (Kroeber, Watson 184).

One system that uses TPS output to analyze and generate predetermined or ad hoc reports is the management information system or MIS. The MIS system may be used to analyze sales trends, provide summary reports or schedule the sequence of print jobs (Kroeber, Watson 228).

In this case, a commonality of the database between TPS and MIS means that the same data may be used in different forms to provide specific reports for end users. This adds additional value to the data owned by the organization.

A common complaint is the amount of "junk" mail delivered each day by the U.S. Postal Service. Advertisers are eager to buy lists of names of people who fit their target audience. For instance, civil engineers in New York state making $50,000 or more a year can easily be targeted by professional societies and others interested in getting their message to this group. Where do these lists come from? Many come from computerized

magazine subscription lists, voter rolls, new auto license registrations and other lists available to advertisers for a price.

Mailing lists may result from either TPS or MIS. A general mailing list of all people in St. Charles could be the result of TPS reporting. On the other hand, doctors of dentistry living in St. Charles with incomes over $75,000 may very well be the result of MIS reporting. The management information system has the ability to take TPS data and analyze it to provide the specific output required by the organization.

The staggering amount of information and the speed and accuracy of sorting through large quantities of data make computer databases the logical choice for those wishing to sell a product to a particular socio-economic or special interest group. This is only one example of how data increases in value over time. It is possible to sell information derived from the database, and still retain the data itself.

Author Richard Baker discusses the possibility of one day finding *information* listed as a company asset in an organization's annual report. This may very well be the case. Nearly 25 percent of a financial institution's payroll is devoted to creating and maintaining the information needed for routine business operations (22). The 25 percent figure would not be far off for many organizations that utilize computerized information.

This figure does not represent the money needed to own and run the information system itself.

In 1984, Jerry Buckley, president of California Interactive Computing, Inc., a company that provides computer systems for insurance claims administration, stressed the value of data at the Self Insurance Institute of America's Fourth National Educational Conference. Mr. Buckley contends that the value of data is equal to the sum total of the organization's labor. "The loss of data translates into a corresponding loss of labor hours if you have to go back and recover it," said Buckley (Bradford 88). He maintains that the loss of data can severely affect the ability of an organization to stay current, and perform its basic business functions.

Donald W. Kroeber and Hugh J. Watson discuss the vulnerability of data in their book *Computer-Based Information Systems: A Management Approach:*

> Even if natural disasters, malfunctions, and criminal acts were not threats to CBIS, systems managers would still need to take precautions to safeguard data. The very nature of processing -- changing, adding, and deleting data-- raises the possibility of error. Changes may not be posted properly, incorrect data may be added, or data that should have been saved may be deleted (472).

An insurance company survey found that computer facilities and the data they contain have become so important to the health of the organization that 90 percent of companies that manufacture and/or rely heavily on electronic data systems would not survive a serious injury to their data processing centers. The Chubb Group of Insurance Companies survey, reported in *Datamation* magazine, goes on to say that those that do survive the disaster can expect a drastic drop in earnings both during and after the actual loss period (Tangorra 70).

Managers must endeavor to protect the organization from loss-of-business due to computer failure or data disaster. The organization must recognize its obligation to assess the value of the data held in its computers and plan accordingly to protect it.

Perhaps the closest thing to a security golden rule is the simple admonition of James Edward Keogh, a security consultant, and author of two books about security for home and office. Keogh says: "The computer files of a business should be treated with the same care that the manager uses when dealing with money" (180). What he is saying is so simple, it often slips by without making the impact that it should. If a computer tape contains records worth $50,000 to the organization, for instance, then the computer tape deserves the same security as $50,000 in cash. Since no one is likely to leave that much cash unattended, tapes, disks, printed reports, and computers

that store valuable information should not be left unattended either. Data is an asset. The care needed to protect this valuable resource can affect the organization's ability to conduct business.

The Ability to Conduct Business

In May of 1988, the Penn Mutual Life Insurance Company's downtown Philadelphia office complex suffered a catastrophe. A fire broke out two floors above Penn's data center. Although the fire did not reach the center's level, the tons of water used to combat the fire destroyed the center and threatened the company with a shutdown of operations.

Luckily, Penn Mutual was ready for such an emergency. While the eight-alarm fire was still raging, the company began moving dozens of trusted employees and thousands of backup records to a nearby emergency computer facility known as a "hot site." A hot site is a completely equipped stand-by computer center that is ready to go on line at a moment's notice.

Because of a thorough disaster recovery plan, Penn Mutual was up and running 24 hours after the first alarm was turned in. Most system users and customers did not realize there had been an interruption of service.

Michael R. Gauthier and Julie K. Buchanan, writing in *Across The Board* concluded:

> Penn Mutual's experience is a potent example of why companies can no longer afford to ignore the threat of computer disaster. Although nearly everyone in business has suffered the annoyance of temporary downtime resulting from faulty hardware or software, few have considered the disorder that would follow a paralysis of their main computer operation. For an unprepared company, the consequences of such a disaster --disrupted operations, lost orders and revenues, dissatisfied customers-- could be devastating.

In a 1987 University of Texas study, researchers found that by the seventh day following a computer disaster, a service company would be losing a fifth of its daily revenue. For the average bank suffering from a seven day outage, 40 percent of daily revenues would be lost (47).

John Ratliff, of Sungard Services Company, corroborates the University of Texas study. Speaking of banking, Ratliff observes: "A large portion of a bank's assets are electronic. If it lost the ability to electronically manipulate money (e.g., transfer funds), it ceases to be a viable business. Quickly" (18). Ratliff's analysis makes obvious the need for disaster prevention and planning: "A comprehensive disaster recovery capability is, first and foremost, an insurance policy. It's a vital step in assuring the continuity of the single most important function a company has: The ability to run a business in a profitable manner using the data processing function" (17).

In order to sustain the existence of the company through a computer disaster, management must insist on a thorough survey of risks and assess

probable losses. They must take proper precautions to protect the organization's computer assets. In the next section, legal implications of safeguarding data are discussed.

Legal Implications of Data Loss

Management is responsible for protecting the assets of the organization. When those assets are sensitive data files, extra steps must be taken to ensure the integrity of the data. "Data integrity is defined as procedures to protect data and ensure that data is accurately and consistently maintained in the computer system" (Knapp 22).

It is the obligation of corporate managers to safeguard data assets. Larry Deitz, writing in *Computers & Electronics*, explains why corporate executives must be prepared to combat computer intrusions:

> Corporate management must use reasonable means to safeguard its assets, and information is one such asset. Consequently, managers will have to devote more effort to protecting information. Potential litigation concerning such things as loss of data, illegal copying, inaccurate figures and privileged information that shows up where it is not supposed to will force managers to institute safeguarding measures (68).

Deitz maintains that confidential or proprietary information is confidential no matter where that data may be stored. If sensitive files are stored as part of a word processing document on the office PC, then care must be taken to make that data safe from inquisitive eyes.

Below are examples of sensitive items that deserve special security consideration:

- ✓ Employee records including applications for employment
- ✓ Corporate and individual tax information
- ✓ Company and employee insurance records
- ✓ Government regulatory reports (Internal Revenue Service, Federal Trade Commission, Securities and Exchange Commission)
- ✓ Credit reports and financial records

Margaret Kenda, a recognized expert on crime, suggests that the theft of sensitive information is much harder to monitor than theft of physical assets like office furniture or a system component:

> You may not know about the loss for years. You may never be sure any theft took place. The loss may be just barely discernible in the attitudes of opponents engaging in complex business one-upmanship. It could appear in the form of a competing product or a patent problem. It could mean a loss of the competitive edge. It could mean years of research thrown away (261).

There now exists legislation, both federal and state, that protects data owners against computer related crimes. Another group of laws deals with the related area of privacy. Although many of these laws were written in general terms, new legislative efforts are describing intrusion and theft in more detail. Sentences are also getting more severe. Tables 3 and 4 list legislation about computers and their use.

Forty-eight states have some form of statute on the books relating to computer security, computer fraud or computer crime. California sets the standard with tight criminal statutes covering invasion of privacy, even if no damage was done. (Computer Virus Handbook 24).

Massachusetts state senator William Keating is at the vanguard of state legislators proposing bills against the invasion of computers. Under Keating's bill, penalties would increase depending upon the degree of invasion. In the worst case, any person found knowingly releasing a computer virus would get a maximum of ten years in prison, or a fine of $25,000. Keating said he wanted the record to clearly show that unauthorized computer invasion is a criminal activity and should be punished as such (AP).

In 1989, three revised Missouri Statutes describe the crimes of (1) tampering with computer data, (2) tampering with computer equipment, and,

(3) tampering with computer users. The statutes provide penalties for those convicted of computer invasion. Penalties range from a class A misdemeanor (imprisonment is six months or greater), to class D felony (prison term is less than 10 years), depending on the severity of the damage done to the system (Missouri Revised Statutes 1503).

As with most states, Missouri allows for civil suits against computer invaders. Typically, civil suits allow the victim to sue for damages caused to the data, equipment or users of the system as well as the cost incurred to trace the source of the damage. They also allow for the reimbursement of legal fees.

Prestin K. Covey, chairman of the American Philosophical Association's Committee on Computer Use in Philosophy and director of the Center for Design of Educational Computing at Carnegie Mellon University, said in an Associated Press interview that up until the present, he believes there existed "real timidity about bringing the hammer of justice down on hackers who abuse the system." Covey, planning for a 1991 computer ethics conference, says:

> I think that when damage is caused --in terms of person-hours lost, property lost, work lost-- it ought to be treated just like the case of arson or breaking and entering, where there are actual and measurable harms. It's perfectly analogous to if somebody broke into your office and destroyed or stole paper files (Reppert AP).

Table 3

Federal Computer Legislation

Computer Fraud and Abuse Act of 1986:
The law covers computer crimes as they relate to federal computer systems. It is a felony for an individual to obtain intentional unauthorized access that "alters, damages or destroys information...or prevents authorized use."

Electronic Communications Privacy Act of 1988:
The law prohibits unauthorized access to electronic mail systems.

Wire Fraud Statute:
This law, not originally intended to cover computer crime, may be used to protect against viruses when the crime makes use of network communications.

The Computer Security Act of 1987:
This law provides for technical protection measures and training to improve security of government computers. Authorizes the National Bureau of Standards to set policy for nonmilitary computer security. Also, authorizes the National Security Administration to set standards for military computers.

SOURCE: *The Computer Virus Handbook*, Price Waterhouse, 1988

Table 4

Major Federal Privacy Laws

Privacy Act (1974):
Federal agencies are forbidden from letting information they collect for one purpose be used for a different purpose. Loopholes allow agencies to exchange information anyway.

Right to Financial Privacy Act (1978):
Sets strict guidelines for federal agencies who want to rummage through a bank's customer records.

Video Privacy Protection Act (1988):
Prevents video retailers from disclosing video rental information without a court order or customer's consent. Privacy advocates want same regulations for medical and insurance files.

Computer Matching and Privacy Protection Act (1988):
Regulates computer matching of federal benefits or for recouping delinquent debts. Individuals are given a chance to respond before adverse action takes place.

SOURCE: *Business Week* "Cover Story: Is Nothing Private?" September 4, 1989

More and more citizens are voicing their concerns, and federal and state legislators are listening. Because laws are fluid and change nearly every year to accommodate new situations, expect to see new legislation as new problems in computer security come to light. Robert Morris is the first person sentenced under the Computer Fraud and Abuse Act of 1986. Others will follow as police and government agencies learn more about computer intrusion, and how to prosecute these crimes effectively.

The Maytag Syndrome

Nearly everyone has enjoyed Jesse White's portrayal of the lonely Maytag repairman in television commercials. He patiently waits day in and day out for someone to call. Maytags are just too dependable. People *perceive* Maytag as a company with a dependable reputation. It's an advertising manager's dream come true because to many people, Maytag is the last word in appliances that require little maintenance.

Unfortunately, corporate managers suffer from a similar syndrome. Corporate managers often *perceive* security where little or none exists. Because they don't hear of security violations, they believe none take place. Sanford Sherizen, a security consultant who testified before the United States Senate on security matters declares, "Nontechnical users and management

may well assume that security is built-in or somehow automated so they don't need any responsibility" (11). Users feel no responsibility for security. Many managers don't either. There is little accountability for computer or data tampering. Sherizen states that the awareness training needed to combat this lax attitude must flow from corporate policy and procedures. This can only happen if managers are aware of intrusion dangers and make training a requisite for anyone handling computer data.

Dr. Deborah Downs, a computer software expert at Aerospace Corporation in Los Angeles feels that the increase in computer incidents is not due to system design, but rather bad system administration (*Research and Development* 66).

For system administration to improve, every organization needs:

1. Education and motivation
2. A strong prevention program
3. A thorough disaster recovery plan (McAfee 136)

The following pages describe the various threats to the organization's valuable data assets, both man-made and acts of nature. The countermeasures section deals with positive steps management can take to safeguard data from loss or harm.

PHYSICAL THREATS TO DATA INTEGRITY

The physical well-being of computer hardware, the integrity of the operating system and applications software, and the safety of stored data depend on the security provided for their protection. Data center managers tend to think first of the obvious threats to the installation such as physical intrusion and electronic theft. But some of the worst damage may be caused by *Mother Nature* on the rampage. Acts of God most likely to concern data professionals are water damage due to flooding, fires and earthquakes.

Floods/Water Damage

In the Penn Mutual disaster, tons of water from sprinkler systems and fire hoses cascaded down from the floors above to inundate the data center. There are more reports of computer center flooding from fire control than flooding caused by heavy rains. The Federal Emergency Management Agency has targeted many areas in the United States as "hundred year" flood zones. Because these areas are well documented, nearly all major computer centers are kept far from them. According to structural engineers Charles Scawthorn and William E. Gates writing in *Data Management*, "it is relatively rare for hurricanes, for instance, to cause major structural damage to data processing centers" (30).

Preservation Officer Toby Murray, of the University of Tulsa Libraries, says that 95 percent of all disasters will result in water-damaged material (13). Besides the water itself, high levels of humidity with ambient temperatures above 75 degrees make a likely spawning ground for mold. Mold spores are always present in the air and can be dormant for many years before the right conditions cause rapid growth. Although Murray was referring particularly to books and other library materials, her cautions against mold are equally valid for computer centers loaded with disk and tape media, paper support documents and operating manuals for the computers themselves.

Water is the arch enemy of electronics, and can also damage disk and tape data beyond recovery. To provide adequate fire protection without water damage, the wise DP manager considers the purchase of Halon fire suppression equipment. Halon smothers a fire without water and does no damage to delicate computer components. However, the price tag for such a system can be several hundred thousand dollars.

When fire struck the Illinois Bell Telephone Company switching center in Hinsdale, 500,000 business and residential customers in the Chicago area experienced disrupted telephone service. Some Bell customers lost millions of dollars in revenue because phone service was not restored for as long as three or four weeks. Over 118,000 fiber optic lines melted during the intense fire. Fire protection experts claim that a $350,000 Halon fire extinguishing system could

have extinguished the fire, and saved millions of dollars. The fire-damaged computer in the Hinsdale site may cost as much as $16 million to replace (Gauthier, Buchanan 50). In comparison to the huge amount of revenue lost by Illinois Bell and its subscribers, and the dollars needed to rebuild the computer switching center, the third of a million dollar price tag for the Halon system would have been a small price to pay.

Fires

The second major threat to computer centers and data bases is fire itself. Related smoke and water damage are considered part of the fire threat.

December 20, 1987, was a black Sunday for the employees of the National Rural Electric Cooperative Association in Washington, D.C. The first alarm sounded at 3:13 a.m., and firemen arrived moments later. The blaze was already so intense that much of the third floor had literally evaporated. The 2,000 degree heat softened steel support beams in the 10-year old building (80). Because sprinklers and smoke detectors were not required when construction began on the NRECA structure, they were not installed. Although the NRECA data center was protected by a Halon system, the suppression equipment could do little to protect the facility against the hazards of heat, soot and water damage because the fire began on the floor below and the heat rose to the data center. The total replacement cost caused by the fire reached $3.3 million.

Within a week of the disaster, NRECA was operating at 80 percent capacity, estimates Robert Nelson, director of public and association affairs for the cooperative (Carter 79). This would have been a remarkable recovery under any circumstances, but is especially impressive when you take into consideration that December is normally the busiest time of year for NRECA. December is traditionally the month when applications for the annual meeting are processed by the data center. Also, all the data for year-end reports gathered for the co-op's annual meeting are processed during the last month of the year. The recovery was made possible because of the farsightedness of the computer division's management team. Religious use of tape backups and off-site storage allowed the co-op to resume business operations in another computer center within days.

Smoke and heat detectors, fire alarms, conventional sprinkler systems in non-technical areas, and adequate fire extinguishers are sound fire prevention practices. Many of these are dictated by state and local building codes. The National Electrical Manufacturers Association (NEMA) recommends that all commercial buildings follow Group B (business) guidelines for early fire detection and human safety. Computer centers are included under these guidelines. The association's regulations are stringent and require much more than many building owners realize. NEMA recommendations follow on the next page:

- Install smoke detection systems in boiler and furnace rooms, return-air plenums, corridors, elevator lobbies and elevator penthouses.

- Install fire alarms, emergency communications panels and voice alarms. Voice alarms play pre-recorded messages to the affected fire zone over the building public address system.

- Provide electrical fault detection systems.

- Install two-way fire department communications for fire department use.

- Install and maintain a central fire systems control panel for use by the fire department. This centralized control system includes: voice alarm panel, fire department communications panel, fire detection and annunciator panels, status indicators for elevators, status indicators for air-handling systems, stairwell unlocking devices, sprinkler and waterflow detector displays, emergency power for lighting and panels, telephone for exclusive fire department use (97).

Robert Bloom, who, besides his duties as professor of accounting at the University of Wisconsin, is affiliated with the American Accounting Association and the National Association of Accountants, urges the installation of adequate drains under computer flooring. These drains help remove water entering from overhead sprinklers and fire equipment (17).

For documents and files that must be kept on the premises, fire-proof file cabinets and vaults can supply protection within certain tolerances. These are especially needed where negotiable securities could be damaged or destroyed during a fire.

Regular fire drills and a well documented escape plan can provide peace of mind and quick response in the event of a real fire situation. Each department needs to practice leaving the building expeditiously in order to save human life. Alternate escape routes should be clearly marked and included in any practice fire drill.

Earthquakes

Graphic television news pictures from earthquake sites portray the violence and destruction possible from even mild seismic disturbances. These seismic disturbances are generally thought of as western occurrences. However, the 1811-1812 earthquakes midway between St. Louis and Memphis were larger than the 1906 San Francisco quake. Other large earthquakes include those in Boston and Charleston, South Carolina. Indeed, many areas of the country face some degree of seismic hazard.

Data centers are particularly at risk from the upheaval caused by a major earthquake. Structural engineers Scawthorn and Gates discuss the effects of earthquakes on computer operations:

> While building damage is a serious concern in itself, the more likely threat facing DP managers is interruption of operations, with subsequent business interruption loss to the center itself or its corporate or outside clients. Following even a moderate earthquake, this interruption of operations can be quite serious.

> Business interruption to computer facilities in small to moderate California earthquakes, such as the Livermore earthquake of 1980, ranged from six to 12 hours. In a moderate to large event, such as the 1971 San Fernando, California, earthquake, the interruption experienced by the area's computer centers ranged up to weeks (31).

From direct observation, engineers Scawthorn and Gates list the most prevalent computer center problems they have encountered following an earthquake as:

> 1. Cabinets become warped and cooling and electrical lines are stretched or broken by violent upheaval. In some instances, cabinets broke loose and rolled into open spaces in the computer floor. If computer floor penetrations are covered with grills, the cabinets are not likely to pitch into an opening. The installation should provide for some movement of equipment without breakage.
>
> 2. Raised access floors, popular in computer installations, are likely to collapse without adequate cross-bracing. Many of these systems use pedestals bonded to the concrete floor below with mastic. The mastic deteriorates with age and provides little strength during an earthquake. Cross-bracing provides the strength floor systems need to endure the stress caused by movement of large pieces of computer equipment.
>
> 3. The jarring of perimeter walls causes the collapse of suspended ceilings. The gridwork for suspended ceilings contains sprinkler heads, overhead lighting and heating/cooling ducts. All these components can fall on the computer center below.
>
> Also, as dust accumulates on top of the ceiling over time, a disruption of any magnitude can dislodge large quantities of dust and introduce it into the computer room. The solution to suspended ceiling collapse is an earthquake-proof grid system that can support the movement of perimeter walls without failing.

4. The tipping of tape storage cabinets can cause considerable damage when the cabinets fall over onto mainframe cabinets. Open shelving holding heavy tape reels can collapse under their own weight. Cage-like reel holders of extra strength are recommended to ensure that plastic tape reels are not broken when falling from open shelving.

5. Support equipment such as power distribution, chillers and cooling towers can be damaged with movement. Many generators are spring mounted and tend to bounce up and down during an earthquake. The bouncing causes ruptures in cooling and electrical lines. Special earthquake anchors for heavy equipment can minimize risk.

6. Fire suppression and power systems consisting of racks of batteries should be strengthened against building movement. "Anchorage, bracing and strengthening of emergency systems is highly cost effective and should be a number one priority in reducing earthquake risks to a data processing center" (33).

The risk to the data processing facility is a combination of the existing earthquake hazard, which can be ascertained from geological surveys and state and local planning authorities, and the importance of the facility to the organization's continuing operation. If the risk is great enough, then consultation with a reputable structural engineer is recommended by Scawthorn and Gates. Structural consultants can quickly identify areas of vulnerability and plan a program to adequately strengthen the facility.

Although floods, fires, and earthquakes are the most spectacular threats to computers and peripherals, environmental factors and power glitches can not be overlooked as real threats to the smooth running of a computer facility.

Environmental factors

Temperature and humidity can affect the productivity of the data center. Extreme heat can harm delicate computer components. Improper levels of humidity can adversely affect magnetic media. James E. Hassett, author of *Process Cooling for the Data Center Environment*, maintains that the term air conditioning connotes people comfort. "Process cooling," on the other hand indicates specific cooling considerations for data centers (176).

Hassett confirms that each system manufacturer has a recommended temperature and humidity level for optimum operation. These recommendations are used when planning a data facility. A consultant can quickly compute the amount of heating, cooling, humidification or dehumidification needed by completing a heating/cooling load form for the data center. The heating/cooling consultant takes into consideration the heat generating equipment along with the volume of air in the computer center. The manufacturer's recommendations for ambient conditions help him compute the cooling load correctly.

According to Hassett, the minimum capacity of the system should allow for a 30 per cent growth of computer (heat generating) hardware (176).

Consideration should be given to whether excess heat given off by the data center can be used elsewhere in the building to provide heat for offices and common spaces.

Redundancy of conditioning equipment must be built into the system since at some point a cooling/heating component will fail. This redundancy assures that the data center will receive adequate amounts of conditioned air even though one system is off-line for service.

The elimination of contaminants and dust in the air is necessary to ensure proper operation of tape and disk drives. Dust can adversely affect the drive's ability to read or write on magnetic media. Filtration and positive air flow allow computer systems to work effectively.

Positive air flow provides air pressure greater inside the data center than that outside the room. When doors are opened, clean air flows out in an attempt to keep dust from entering the computer center.

Hassett says that there are many sources of information available to DP professionals faced with designing or adding to an existing data facility:

> When analyzing a data center's environmental requirements, a manager should consult these sources of free, competent advice: the professional designer retained for the project; the site preparation specialists representing the hardware manufacturer; the building's plant engineering and maintenance department (which can often help avoid unnecessary equipment duplication and mistakes); the local utility; user groups, many of which have published information on aspects of data center design and maintenance" (176).

Although flooding, fires and earthquakes can cause staggering losses on a grand scale, they are not likely to occur on a daily basis. That is not the case with electrical power fluctuations. Electrical power provides a continuing source of trouble for computer data centers managers.

Electrical Power

Since computers demand steady, conditioned electrical power, the DP manager needs to know what problems electrical power can cause, and take steps to safeguard the system's delicate components. Frank Stifter, president of Electronic Specialists, Inc., an electrical interference control company, says that "some of the most insidious 'culprits' responsible for the loss or damage of data, which wreaks havoc in DP departments, aren't people at all. Power surges, electrical noise, brownouts and power failure adversely affect computer equipment" (26). He adds that nearly all shortcomings associated with electrical power can be controlled or eliminated. Stifter cites typical computer problems that often baffle office employees and data center personnel. Graphics displays may exhibit stray lines or snow on the screen. Data received by modem is not the same as the original. Word processors display garbled text. Reliable copy machines run amuck changing settings for contrast, paper size, and number of copies. All of these manifestations may be the work of electrical power that is not adequately conditioned.

Although awareness has increased in recent years concerning electric utility problems, "there is still a fairly low awareness level of the problems utility power creates for a computer system," says Jerry Hanwacher, market planning and operations manager at A T & T Technology Systems. "Garbled data and misfiled data may not ever be picked up as arising from power problems, or not until long after the power problem has occurred," says Hanwacher.

Stifter, who holds a Master of Science-Electronics degree from Northeastern University, points to four main electrical problems and their cure. The first of these is electrical noise.

Electrical Interference

Radio frequency interference (RFI) is caused by broadcast stations, police and taxi two-way communications equipment, and other radio frequency devices that include computers themselves, especially computers operating at very high processing speeds. Electrical interference is often caused by atmospheric conditions and lightning. The noise caused by these sources is generally induced on the power line electromagnetically. Electromagnetic interference (EMI) is easily detected on a standard radio. It is what we normally think of as noise.

Power lines act as antennae picking up noise from all these sources. In addition, other sources of electromagnetic interference are: electric motors, welders, faulty light sockets, and light dimmers. The interference can be coupled magnetically directly to computer equipment, but more likely, it is introduced to the data center through power lines.

Properly shielded "clean" power lines were once thought to be the salvation for electrical interference. Low noise electric lines are shielded from the substation to the customer's electric panel. These lines are so expensive, however, that few are ever installed. Other solutions were found instead.

These solutions include: filters, line conditioners, and isolation transformers. Since it may take one or more of these products to adequately condition incoming power to the data center, Stifter recommends asking manufacturers for trial units. If they do not adequately fill the need, no out-of-pocket expense is incurred, except for shipping.

High Voltage Spikes

The second power problem concerns high-voltage spikes. Many of the devices mentioned earlier are sold with built-in surge suppression. It is a good practice to purchase surge suppressors if the installed filters and transformers do not already include them in their design.

A lightning bolt can instantaneously unleash 75 million horsepower (Stifter 27). The awesome discharge of raw power can induce 7,500 volt spikes on electrical and telephone lines. Air conditioners, huge industrial motors, and transformers are other sources of spikes, although they are relegated to lower levels. Spikes from these sources can sometimes reach 2,500 volt levels. Manufacturers offer spike suppressors suitable for computer center power line protection. Many of these devices are actually combinations of two or more units designed for various purposes, such as the ability to withstand high peak voltages, fast detection and line clamping capability.

Low Voltage

The third power consideration, low voltage, can just as effectively interfere with correct computer operation. Motors under heavy loads tend to draw more current to compensate for low voltage situations. When this happens, increased noise is generated. For chronic low voltage situations, regulators can maintain a steady output voltage even though the input voltage may vary from 90 to 140 volts (Stifter 27).

Total Loss of Power

The fourth power worry stems from total loss of power. The national average for blackouts in the United States is seven times per year.

An uninterruptable power supply (UPS) can save data and keep disk heads from crashing by providing the computer system with emergency stand-by battery power. The cost of rebuilding files and recovering lost data --if it can be recovered-- quickly overrides the argument against uninterruptable power supplies: that of cost. Local area networks are especially vulnerable to outages. Patrick Kareiva, president of Electronic Protection Devices Inc., says, "It is one thing to lose one terminal. It is quite another to lose six or 10 terminals and take out a whole department. If you lose one hour of keystroking, it is not a big deal. It you lose a thousand hours, your whole business may depend on it" (Victor 94).

In recent years the cost of a high quality UPS has decreased dramatically and there are systems for every power requirement and cost range. Many also provide the added benefit of power conditioning by combining voltage regulation and spike protection.

Many UPS models provide only enough power to allow for the saving of data and the safe powering down of the system. Others provide longer use times to allow the system to continue functioning in a normal manner. The longer the system is required to run on battery power, the larger the price tag. But no matter what the cost, as with Halon extinguishers, one disaster prevented could very easily pay for the entire system many times over.

Floods, fire, earthquake and power outages are all areas that need attention by data center professionals. As James Hassett points out in

Datamation, "like it or not, the DP manager is responsible for the entire operation of the data center. Unfortunately, responsibility for performance includes many specialized fields such as air conditioning, fire protection, and security" (176). The data center manager may need to rely on outside advice plus help from others in similar circumstances. Although no one person can be an expert at every area, the DP professional must remain aware of all dangers to the computers and data entrusted to his care. He must be aware of new products and techniques for providing protection and security, and he must be aware of the other major area of concern to data integrity, the threat of data damage from humans. This danger can come from four distinct possibilities: inept data center personnel, disgruntled employees, hackers, and viruses.

HUMAN THREATS TO DATA INTEGRITY

No matter how powerful the computer, it still takes human personnel to enter data, order reports, support, and maintain the system. Marge Yonda, president and principal consultant of Computer Solutions in Rochester, New York, makes the case for logical controls in data processing centers:

> There are many ways --accidental or intentional-- that data can be compromised. Human error or carelessness is the main reason logical controls are needed. Data errors are most often directly

> traceable to the human factor: crime will never surpass incompetency (or anything else) as a source of trouble (128).

Human Error or Carelessness

Many data entry problems can be overcome by providing proper controls over computer data entry personnel. Table five lists some of the best software controls for securing data from accidental manipulation or erasure.

Some researchers estimate that between 50 and 85 percent of all data losses are due to errors and omissions. There need to be sufficient safeguards built into the system so that someone hitting a wrong button will not crash a program and cause data or monetary loss to the organization (Harris 13).

John Deal, a Certified Public Accountant and partner in the accounting firm of Botz, Deal, P.C., believes that one of management's worst failings lies in the hiring of unqualified people for data entry. Deal, who works with small and medium size firms and advises clients on how best to computerize their accounting procedures, says that the same manager who doesn't blink an eye at spending large sums for hardware and software, hires five or six dollar an hour employees, figuring "that the computer does all the work anyway" (Interview).

Deal notes that for many customers of his firm, the hiring of computer room employees does not get the attention it deserves. "I would be surprised if most business owners I deal with check any further than the last employer, if that," said Deal.

Margaret Kenda, author and authority on crime prevention, says that not many small businesses are inclined to take the necessary time and trouble to conduct a thorough background search on prospective employees. Kenda lists sources that often reveal information about applicant's when their statements are incomplete or evasive:

- Records of local police and sheriff (not available in all states)
- Public proceedings of criminal and civil courts
- State Motor Vehicle Bureau records for license restrictions
- State Bureau of Vital Statistics provide information on births, marriages, divorce
- Armed Forces records
- Immigration and Naturalization Service data
- School transcripts
- Credit ratings
- City Hall records of mortgages, real estate loan transactions
- Files of National Crime Information Center (115)

Kenda says that for companies not willing to take the effort or time in-house, private agencies can provide background information on prospects. She contends that although there is cost involved in hiring others to conduct

investigations, the actual outlay of cash is probably about equal to having a company employee gather the information.

The second half of the equation concerns the training for those who are involved in day-to-day computer operation, either as entry clerks, or those concerned with the operation and programming of computers. Table six lists personnel controls that help ensure the integrity of system data by compartmentalizing the functions of the computer room. No one except the system administrator should have free access to all areas of the system. Even then, activity logs and other safeguards make sure no illegal processing takes place.

When it comes to training personnel on security issues, Sanford Sherizen suggests that corporate policy dictate how business is to be conducted. Sherizen believes that employees must be aware that they are accountable for the security of the company's assets. He feels that managers need to indicate to computer users why they need to be security conscious:

> It is quite easy to assume that everyone understands the security implications of the computerized office. Yet, this is an uncertain assumption. DP managers must inform employees about their stake in security. Explain how it will affect their jobs, the privacy of their own records, the usefulness of their work data, the profits affecting their salaries and other matters of vital importance.

> End users should be given a set of rules for proper and accepted behavior. Employees should be evaluated on how well they observe these rules. Some corporations have made this one aspect of the employee performance evaluation. An employee who mis-handles paper files or leaves copies of important documents [computer tapes or disks] out in the open should certainly be questioned (11).

Sherizen, president of a consulting firm specializing in computer crime prevention, believes strongly in making sure employees know that prevention and detection mechanisms are in place, and that they are there to thwart unauthorized computer use or abuse.

With proper hiring practices, including checking prospective employees' background information, and a commitment by management to raise the security consciousness of all employees, many problems can be stopped before they reach catastrophic proportions.

One area where DP managers have serious problems concerns the human computer user and abuser. He may be a disgruntled employee because of lack of advancement, mistreatment by management, or a lack of interest in the tasks he is assigned. The disenchanted employee may seek to harm the company from within, or plan an attack after leaving the firm. In this case, he will often use his knowledge of his former employer's structure to benefit his new employer.

Hackers on the other hand seek out computer targets with great finesse. They research the company and the system they are about to penetrate. The next section deals with the disgruntled worker.

Table 5

Software Controls For Human Error

Error Trap Entry:
Error trapping is an essential part of good application software. For example, a general ledger program should not allow an operator to input alphabetic characters into a number field where only numeric data is acceptable. Transactions should be rejected by the system if they do not balance.

Verification of Data:
The system should be able to verify that customer number, employee number and so on, when entered by the operator, are valid numbers. The description of the data associated with the number displayed along with the number is an excellent visual check that the right customer number, etc., was entered.

Read / Write Protection:
It is essential in a multi-processing environment where more than one terminal may input data, that the terminal performing an update to a particular file locks out all other terminals until the update is complete.

Control Totals -- Dollar Values:
Daily totals of all transactions at day's end should be mandatory. Yesterday's balance forward, the addition or subtraction of today's totals provide end of day figures. This becomes the balance forward for tomorrow's calculations. Also end of month, quarter and year are required.

Procedural Controls:
A good system will control the processing steps so procedures occur in a logical order. No "leapfrogging" in the order of steps can be allowed. All preceding steps in the order must be complete before allowing the next step to process.

Table 5 Continued

Audit Trails:
Every transaction that took place during the year should be documented to allow for error investigation and auditing purposes. The audit trail shows the step by step transactions of the system.

Forced File Backup:
The system should force a backup of records into a temporary storage area before transactions proceed. For example, payroll records should be backed up before the processing of payroll checks can proceed in case a rerun is needed.

Identification of Reports:
All printed reports should contain the system date, time of printing, operator's initials, and title of the report.

Exception Reporting:
The system should "flag" any items that do not conform to pre-defined norms. For example, the payroll program should print an exception report when a check is processed above a certain dollar amount.

SOURCE: Marge Yonda, *Modern Office Technology*, September 1985

Disgruntled Employees

The gaining of a competitive edge in television news ratings led two 33 year old news executives into a life of computer crime. It was a way for both men to prove their worth both to their former employer and their new company. It was a way to right past wrongs. Unfortunately after four months the hacker's snooping was discovered. An assignment editor at the target news organization realized some of his files were missing. Computer experts agreed that the newsroom computer system of WTVT-TV news in Tampa, Florida, had been electronically burglarized.

The two news executives were charged in May of 1989 with 17 counts of computer hacking and conspiracy in the theft of information through the use of computers and telephone lines.

Terry Cole, former news director for WTVT-TV in Tampa, and former WTVT assignment editor Michael Shapiro told Judge Edward Ward that they were sorry for the theft of story ideas and news follow-up files. They claimed their computer attacks had destroyed their families and their careers. Judge Ward sentenced both men to five years probation and 250 hours of community service, which were to include at least three talks each year to journalism students.

Both Cole and Shapiro had used knowledge of their former station's news operation to steal exclusive stories and series ideas which gave their new

employer, station WTSP-TV, a competitive edge in the Tampa television market.

Shapiro knew WTVT's security system thoroughly, including passwords and identification numbers, because he had helped to set up the computerized newsroom while working for the station (AP).

In the case of Donald Gene Burleson mentioned in the introduction, it is clear that he had planned his attack on the USPA & IRA computer database some weeks before he was relieved of his duties. Perhaps Burleson saw the writing on the wall, and knew he had a limited time to plan his revenge before leaving the firm.

Greed, reversal of investments, revenge for slights either real or imagined, passed over promotions, addiction, and family problems are ample reason for many disenchanted employees to steal from their employers. The organization must guard against such attitudes, and seek ways to neutralize attacks on the company's computer assets.

Both the USPA & IRA and station WTVT-TV share some of the blame in the attacks by former employees. First, neither organization followed the good administration practice of changing all passwords when employees intimate with the computer system leave the company.

Second, in the case of the Texas Insurance firm, USPA & IRA, Burleson was allowed on the premises when he had no business to be there, yet no one

Table 6

Personnel Controls

- Provide clearcut job specifications
- Separate duties of systems analysts from those of computer operators and entry clerks*
- Enforce vacations*
- Consider bonding employees
- Rotate personnel to different shifts and duties
- Keep logs of those using the library
- Prohibit programmers and analysts access without suitable authorization
- Permit only those with current authority to log on the computer
- Immediately collect all keys, badges and keycards when someone leaves the company (Some experts say this should be done when notice is given)
- Emphasize computer controls and offer adequate training to all personnel
- Provide an internal audit group independent of DP personnel

---

SOURCE: Robert Bloom, Data Management, July 1983

*NOTE: The rotation of duties and the forcing of vacations helps prevent one person having the ability to defraud the company. A telltale sign of attempted fraud usually is detected when an employee will not take a vacation, or complains about a shift to new duties. Very often the employee needs to physically remain at work because the scam takes daily maintenance. bk.

questioned his operation of various company terminals, even after his dismissal from the company.

In the next section, the motivation of hackers is presented. Very often those who launch computer attacks against business computers are hackers. The discussion concerns hackers and their psychological profile.

Hackers

Computer hackers have been around for many years, but only in the last decade has the stigma of vandals, thieves and terrorists been part of their mystique. In the early days, "hacker" was a term of respect for one's abilities as a programmer and debugger of computer software. It was a badge of honor. The tradition began with young computer wizards employed by the artificial-intelligence and computer systems research laboratories at the Massachusetts Institute of Technology (MIT). In the early 1960's, MIT created state-of-the-art hardware for the Defense Department.

The early hackers, many school dropouts with high IQs, worked on the development of the high level programming language known as LISP. They also developed the first computer chess game, a by-product of their artificial intelligence research.

These hackers, often wearing grubby clothes and existing on chocolate bars and soft drinks, helped create the first time-sharing programs for comput-

ers. These early time-sharing programs were the forerunners of today's advanced operating systems. Operating systems keep tabs on all the computer's resources and they control the input and output to and from the computer. They are the backbone which applications software programmers use to make the computer productive.

Programmers at MIT took turns developing time-sharing software. These programs were designed to solve the particular problem of multiple users. The software was meant to be as foolproof as possible. Other hackers were duty bound to break the computer code and crash the system. They delighted in confounding their fellow programmers with traps of their own. It was in this kind of high-tech intellectual environment, rife with an indulgent anarchy, that hacking was born.

Bill Landreth, a super-hacker of the early 80's known as *The Cracker*, describes these pioneers of computing in his book *Out of the Inner Circle*:

> The hackers who created and crashed those early time-sharing operating systems delighted in getting around any attempt to keep them away from the computer's resources. As far as they were concerned, any hacker who could find a way to circumvent or even destroy a barrier set up by the system operator wasn't at all obligated to keep from using his discovery -- it was up to the system programmers and operators to patch up any holes in their software (28).

By the early 1970's, before personal computers became available to everyone, hackers built their own rudimentary *black boxes*. Most of these early attempts at computing required programming in machine language since no operating system existed for computers of such limited capacity. In fact, controls for these early PC prototypes had banks of switches since no keyboards, printers or disk drives worked with the fledgling computers.

Other early hackers got their start by phone *phreaking*. Phone phreaking is the illegal use of the long distance phone system for personal calling without payment. Phreakers do this by using a series of tones to bypass normal telephone channels, and route long distance calls all over the world for free. Many of today's giants in microcomputers got their start phreaking. Notable among them are Steve Wozniak who co-founded Apple Computer, and John Draper, developer of a word processing program for Apple computers called EasyWriter (Landreth 32).

During the late 70's and early 80's phreaking overlapped with true personal computers as they became widely available. Modems, once used only by mainframes, became faster, cheaper and more reliable for use with PCs. Hackers used modems to link their computers with other hackers who shared the same view of computing.

The hacker mentality is both interesting and frightening. Most are male. Many are backward in terms of social skills. Hackers live through their

computers and communicate by keyboard. They are often extremely literate on computer subjects and think nothing of spending 24 or 48 hours straight trying to break into a system they wish to study. They are students of operating systems, and like the early hackers of MIT, expect software publishers to write competent programs to keep them out. When they find a programming weakness, they exploit it for all it's worth.

Hackers are addicted to computing. These reclusive, obsessive computerists experience highs similar to race drivers and test pilots when they break into a secure system, or unravel an extremely complicated piece of computer coding. The early MIT hackers engaged in what they called "sport death". In today's parlance, it might be described as "pushing the envelope;" that is, pushing one's resources beyond what seems possible (McAfee 41).

As the 80's progressed, hackers became more brazen. Newspaper and magazine accounts of their exploits abound.

Brian Murphy, writing in the January, 1984, issue of *Creative Computing* describes one group of hackers that got out of control:

> The 414s were a very small group of high school age kids from Milwaukee who had met at an explorer post and found they had a similar interest, telecomputing. Until the Spring of '83, they had done nothing to merit national headlines or a Newsweek cover, but with a few log-ons all that changed (266).

What the 414s (taken from the Milwaukee area code) did was destroy vital cancer research records at New York's Memorial Sloan-Kettering Cancer Center. The group, through the Telenet computer network, gained access to the computer system used by radiologists across the country. This system had been intentionally designed for easy access by busy radiologists who needed to check on the levels of radiation administered during cancer therapy (268). The case of the 414s is one nearly all authors of computer security books include. The publicity from the Sloan-Kettering episode, and the controversy surrounding the movie *War Games* contributed to the public's perception of how hackers work to penetrate and sometimes destroy valuable computer assets.

Celebrated computer programmer Leo Schwab takes exception to the way the term hacker is used to paint all computer hackers with the same brush. There are good hackers, essentially programmers trying for that big hit game or program, and there are bad hackers trying to destroy what others build. Schwab admits however that hackers like to play God. They enjoy the power trip of absolutely controlling a computer --theirs or someone else's (AP).

The true addicted hacker will go to great lengths to gain access to a computer system. Some are known to systematically sift through a target company's trash looking for documents that offer clues to passwords and log-on sequences. Others have posed as building maintenance workers in order to gain physical access to computer terminals on Friday nights knowing few people

would work over the week-end. Still others have passed out innocent looking surveys asking for complaints about computers used by the target company. All these ways and many more are employed to gain the keys to the system, a user identification and password.

It takes diligence by system administrators to keep these highly intelligent and dedicated hackers off a system if they become interested. It is far better to keep them out entirely, rather than try to remove them once they have penetrated the system because hackers have a multitude of offensive and destructive weapons at their disposal. Table 7 lists these weapons in the hacker arsenal. One of the worst weapons employed by hackers is the computer virus. It is the next topic discussed under the umbrella of human threats.

Computer Viruses

Computer viruses are rogue computer programs that attach themselves to legitimate computer files. They may lay dormant for a long time in order to duplicate themselves into as many files as possible without detection. Once enough files (computer disks, backup tapes) are infected, they may enter the active phase of their life cycle, destroying priceless computer data and programming. But this is not the end, because they leave behind other clones of their computer code so that they may attack other systems in a similar manner.

Although mainframe computers could be attacked by viruses, they are considerably more immune to this type of threat since greater system and programming controls are built into mainframe operating systems. They can however help to spread personal computer viruses. In this case, the mainframe computer becomes a "carrier" of the virus, transmitting the virus to personal computers attached to the network. Although the main information utilities like CompuServe and The Source take great care in screening programs uploaded to their systems, this was not always the case. Several viruses were initially spread through such utilities. Table 8 lists the most wide spread personal computer viruses for several mini and personal computer operating systems. Table 9 describes how viruses infect and alter IBM compatible systems.

John McAfee, president of the Computer Industry Virus Association, and president of Interpath Corporation, a computer security and anti-virus consulting company, describes his *10 Anti-Viral Commandments*:

1. Limit the exchange of diskettes containing executable code between systems.
2. Reduce the use of public domain and shareware programs.
3. Do not insert system diskettes into another's computer.
4. Add write protect tabs to all system and program diskettes.
5. If running on a floppy only system, boot from only one, clearly labeled, write-protected floppy.

6. Never boot hard disk systems from a floppy, unless it is the original, write protected system master.

7. Never execute programs of unknown origin.

8. Limit the transmission of executable code over networks and other communications links.

9. Do not use network file servers as workstations.

10. Never add data or programs to system master [DOS] diskettes (21).

Certified Public Accountant John Deal says that any new program intended for use on a system or network should be isolated and run on a stand alone floppy-only system. In this manner, any virus can be spotted immediately with commercial anti-virus programs (Interview).

Additionally, backing up all data and keeping backups in a safe place is cheap insurance indeed if a virus strikes despite following the *10 Commandments*. For important data, two different backups are recommended. After backup, these copies should be write-protected.

For the safest possible protection, only shrink-wrapped, off the shelf programs are recommended (Fites 87). Programs from bulletin boards and shareware sources should be treated with extreme caution.

Although many computer programs are only available in the shareware arena, and many serve very real needs not addressed by commercial software publishers, downloaded programs from reliable information utilities or bulletin

Table 7

Hacker's Arsenal

Logic Bombs:
Logic bombs are programs secretly installed in a computer system. They are intended to perform a particular function such as erasing all data on a hard disk or subtlety altering data. Logic bombs are normally triggered on a specified date, or after a certain amount of time has elapsed.

Salami Techniques:
These routines are written into existing programs that take a very small "slice" of assets from a large base of accounts. This type of fraud existed long before computers, but computers allow for greater flexibility in its execution. The slices, perhaps only a cent or two, are deposited in another account controlled by the hacker / embezzler.

Superzapping:
This program is a utility employed during program development. It bypasses all security and other controls so that a programmer can fix bugs in new computer coding. It is analogous to having the master key to a hotel. It allows the hacker unlimited access, not only to program files, but data as well.

Trap Doors:
Holes intentionally written into computer code allow programmers to make changes in a computer program. It is an easy entry point into a program for unauthorized users if they are not removed after final system testing.

Trojan Horse:
Like the fabled horse of ancient Troy, a trojan horse is a program concealed inside another tried and tested program. The concealed program executes a "bonus" routine not intended by the original programmer. This Trojan Horse program might copy the users identification number and password to a file accessible by the hacker. Viruses and computer-based fraud usually include the use of a Trojan Horse.

Table 7 Continued

Viruses:
Viruses are much like a logic bomb except that viruses have the added ability of duplicating and attaching themselves to other executable programs. They can spread from one system to another by the use of disks or tapes. Authors love the phrase "safe hex" when discussing ways of eliminating the chance of infection. Good rule to follow: do not use software of questionable parentage.

Worms:
Worms are similar to viruses except that worms do not move from system to system. They duplicate as many copies of themselves as system memory will allow. In this manner they slow the computer to a halt since no memory is available to install new programs or data files.

SOURCE: Compute!'s Computer Security, Ralph Roberts and Pamela Kane

Table 8

Wide Spread Computer Viruses

Internet Virus:

Infects minicomputers running Berkeley Unix Version 4.3. The Internet Virus attacked the ARPANET (Internet's former name) network. Both Sun Microsystems and Digital Equipment computers were infected. The virus attacked the system in four ways: 1. It obtained the names and account numbers of all system users; 2. It "guessed" passwords from a database of commonly used words; 3. It attempted to decipher encrypted password files; 4. The virus infected other nodes of the system using valid passwords and account names derived from previous attempts.

Aldus or Peace Virus:

Infected Apple Macintosh computers. Displayed a "peace" message on infected systems and then deleted itself. Supposedly used to demonstrate how easily a virus can be spread. First virus known to infect shrink-wrapped commercial software.

The Brain:

Infects IBM PCs running PC or MS DOS. The virus copies the boot (startup) sector of a hard disk to another location on the disk and installs itself in the boot sector's place. Every time the computer is booted, the virus is loaded first, and then passes control of the system to the normal boot program. Some versions created hidden files on the infected system making it harder to detect their presence.

Table 9

Types of IBM PC Viruses

Boot Infectors:

1. Move or rewrite original boot sector
2. Replace boot sector with virus
3. Create "bad" sectors containing the remainder of the virus
4. Infect through <Ctrl>, <Alt>, <Del> or other functions

System Infectors:

1. Infect IBMBIOS, COMMAND or other system files
2. System infectors are memory resident (TSR) programs

General .COM or .EXE Infectors:

1. Infect the .COM or .EXE files
2. Can be memory resident
3. If TSR, virus infects all executed programs
4. If not TSR, contains an infection selection algorithm

SOURCE: Computer Viruses: Background, Detection and Recovery, Computer Virus Industry Association

board systems are recommended by the experts.

Even shareware products specifically developed to guard against virus infection can be altered to introduce a virus to unsuspecting users. Ross M. Greenberg is a knowledgeable computer programmer based in New York. His anti-virus software *FLU_SHOT* is a shareware program designed to alert users to the threat of infection by detecting several common virus symptoms.

Someone obtained a copy of *FLU_SHOT* from a bulletin board and altered the program to introduce a virus to all unsuspecting users. This virus laden program is known as *FLU_SHOT4*, and has caused considerable harm to Greenberg's efforts to eradicate the threat of computer viruses on IBM PCs (10).

Negligence by careless employees, harm from dissatisfied workers, intrusion by hackers, and infection by virus programs are all threats that the DP professional must guard against. Since access is the key to controlling all of these threats, various environmental, software and hardware controls will be discussed in the next section.

COUNTERMEASURES TO HUMAN THREATS

The first line of defense against computer attack is an aggressive program of countermeasures. Passwords, surveillance, encryption, security modems, audit trails, and access cards all fall into this classification.

Certified systems professional Felix Pomeranz discusses the levels of security he believes best describe what the DP professional should look for in total data security. Writing in *The Annals of the American Academy of Political and Social Science*, Pomeranz, a Certified Public Accountant, lecturer and author, considers level one as physical countermeasures. Levels two, three and four are administrative countermeasures, personnel countermeasures and computer-technology countermeasures respectively (73). Levels three and four, personnel countermeasures and computer-technology countermeasures have already been covered in some detail earlier. The next discussion considers levels one and two, physical and administrative controls. Although Pomeranz provides the basic outline, other experts expand on his concepts.

Physical Countermeasures:

Level one includes surveillance, passwords, access codes, access cards, badges, biometric security methods, communications security, and encryption. Several of these methods may be necessary in order to assure management that all possible precautions within reason are implemented.

Surveillance

Surveillance assures that those monitored by the system are aware of the surveillance, but cameras do not interfere with normal operations such as

records retrieval, filing, or the loading of tape and disk drives. Two psychological conditions are instituted with the installation of surveillance cameras. The first puts pressure on dishonest employees. In effect, management is saying "if you want to steal from this company, you have to do it in front of me." The second psychological condition involves the risk of the employee actually being caught in the act (Keogh 62). Although the chance of actually determining wrongdoing by watching surveillance cameras is slight, the pressure of not knowing if someone is watching helps to keep employees honest. It is not surprising then that studies tend to indicate that those under surveillance actually become an active part of their own monitoring (Pomeranz 73). Employees who see others performing questionable work, or see employees in areas they know are off-limits, come to the aid of the "eye" of the TV camera by becoming the surveillance system's partner. Often they will aid monitoring by tipping guards to watch for questionable behavior.

Passwords

Passwords should be assigned to individual users, not whole departments or divisions. Individual passwords ensure accountability. Lydia Dotto writing in *Information Technology*, believes that passwords prove to be a very weak security measure.

> If people are allowed to choose their own passwords, they usually choose words that are easy for them to remember, and just as easy for others to guess. If they're assigned a word that's hard to remember, they'll write it down and put it in their desk --or even tape it to the computer terminal (72).

Worse than this is the system administrator who does not change passwords used in setting up a computer system. Clifford Stoll who wrote the bestseller *Cuckoo's Egg*, tells of Digital Equipment VAX computers on the Internet system with the original passwords still on file years after installation. A West German computer spy was able to penetrate several computers on the Internet system --some military computers as well-- simply because the initial passwords used in installing the system were not removed before operations began.

Computer makers routinely send operating systems with passwords in place to aid DP personnel in installing software on mini and mainframe computers. After installation, administrators are warned to install their own passwords and delete the generic versions since these passwords are known throughout the industry. Despite repeated warnings by the manufacturer, DP administrators neglected to protect the system from the very day the VAX went on-line (24). Table 10 offers suggestions for good password security.

The use of names, birthdays, pet's names and automobile models are popular with many users, but easy to guess. The trick is to choose passwords that are easy to remember, yet difficult for others to guess. A grandmother's name and birthdate are much more secure than the name of a pet. Grandmother's name is farther removed from those who are familiar with individual users' lives.

The changing of passwords should be forced by the system. Dean Hoven, System Administrator for Citicorp Mortgage's Treasury division, explains that good password administration demands changing passwords every 30 days. In his system, Hoven says that several days before the password is set to expire, a message at log-on alerts the user that the password will no longer be valid after a certain date. The user has the choice of changing the password that very minute, or continuing with the old one for another session. If the expiration date passes, the user is denied access until he contacts the administrator for activation of a new password (Interview).

Access Cards / Badges

Access to most government installations is dependent on five variables: value, portability, vulnerability to damage, ease of replacement, and replacement cost (Drahos 14). Plastic cards with variations are used to limit control. Where risk is considered high, access is granted only after the individual is recognized

and proves need to enter the facility. These same methods are employed effectively to guard many business computer installations.

The photo badge is a plastic card that carries a picture of the person seeking admittance. The picture is compared by a guard to the user to make sure they match. Often a sign-in log is used in conjunction with this approach. About 31 percent of government facilities use this method of security (Drahos 14).

Machine readable cards are the second approach for limiting access to computer rooms. The plastic cards have an electronic circuit imbedded in them. The cards are inserted in a reader that matches the card to a list of authorized users.

A variation on the card theme is the magnetic stripe cards similar to those used in bank automatic teller machines. Since magnetic cards can easily be altered, admittance is normally not granted until a personal identification number (PIN) is entered on a keypad. If PIN number and card information match the information in the entry database, the user is granted admittance.

The magnetic sandwich is similar to the magnetic stripe except that a pre-programmed dot pattern is embedded in the card. If the pattern matches the code on file, the user is allowed to enter.

The versatility of card systems lies in the fact that the database can be programmed to allow entrance only on a certain shift, within certain time

Table 10

Password Security

---

1. Each user should have his or her own password. A global password for everyone is just a hair better than no password.

2. Administrators need the ability to assign specific privileges to each individual on the system. One employee may need security rights to read payroll data, while others are denied all access to payroll records.

3. Provisions should be in place for password lockout. After three attempts to gain access without correctly entering a valid password, that user should be locked out of the system to guard against repeated guessing by unauthorized personnel.

4. When assigning passwords, longer passwords are harder to guess than short ones. A combination of letters and numbers is better. Try not to use common names like "guest," "password," or "security." A minimum of five characters is preferred, eight offers good protection, 10 characters is better still.

5. The system should provide for automatic password expiration. The more frequently you change passwords, the less chance a given password will be known by other users.

SOURCE: *Compute!'s COMPUTER SECURITY*, Ralph Roberts and Pamela Kane.

parameters, admit users to certain areas, or a combination of all of the above. The card system also keeps a log of card activity denoting when an individual left and returned to the computer facility. This audit trail is useful if security is breached.

Biometric Countermeasures

Biometric measures to counter unauthorized access resemble the high tech gimmicks of *Star Trek* movies. The state-of-the-art techniques listed here make use of the computer's computational powers to aid system security. These effective but high priced access control methods include: hand geometry recognition, fingerprint analysis, retina scans, signature dynamics, keystroke analysis and voice verification (Business Wire 10/3/89).

Hand geometry recognition involves the analysis of the user's hand print, skin transparency, palm thickness and shape. The hand is one of the human characteristics that is hard to duplicate. Once a user's handprint is on file, the computer matches the applicant's scanned hand print with the one on file to determine when admittance should be granted.

Fingerprint analysis is similar to hand geometry recognition, except that the analysis detects variances in the unique ridges and loops associated with human fingerprints.

Retina scans read the size, location and pattern of blood vessels within the eye. Human eyes are like fingerprints in that they each possess a unique signature.

Signature dynamics compares not only the applicant's signature, but also the velocity and pressure with which he signs his name. This is much more accurate than a simple hand written signature match.

Keystroke analysis compares the individual patterns humans use when entering digits into a keypad. No two people have the exact same patterns and rhythms when entering data on a keypad.

Voice recognition maps the actual physiology that produces speech, not merely the sound or pronunciation. Advances in technology have made this a dependable form of computer protection.

All of these methods are reliable and extremely accurate. In each case the computer compares data on file with data detected from the applicant to determine if access can be granted. The cost involved is directly tied to the amount of risk to the data in question.

Most of the high tech approaches are costly options, but their accuracy may be worth the cost if the data is of a sensitive or negotiable nature. American Airlines felt the threat to their "Sabre" reservation system great enough that they employ many of these techniques in an underground ultra secure facility worth millions of dollars (Gauthier, Buchanan 48).

Communications

Most hackers and computer spies work at a distance. There is no need to take a physical risk breaking into a system. Their entrance to the target's computer most often is through the door marked *communications*. Their toolkit contains a personal computer, a modem and a communications program.

Today, modems are cheap and fast. The ease of use has increased dramatically from the early days of computing. Bulletin boards across the country list valid passwords and account names picked up by hackers. But even if bulletin boards did not exist, hackers have other ways of zeroing in on a system they wish to crack.

One of the easiest ways to gain access is through a computer network. This is how a West German spy entered the Berkeley Livermore computers in California.

Clifford Stoll, astronomer turned computer sleuth, spent over a year tracking the unknown hacker through various network gateways until the identity of the hacker was discovered months later in Hanover, Germany.

Along the way he discovered that the hacker phreaked across the Atlantic, entered a defense contractor's computer, dialed out using the contractor's facilities, and eventually made contact with the Livermore computers in California --an eight thousand mile telephone journey.

It's been pointed out that hackers are painstakingly diligent in cracking a computer system once they make contact. In this case, the spy used a hole in the Berkeley Unix operating system to make himself a super user. With super user status, he was free to look through any files on the system, download encrypted tables of user passwords and use the Livermore computer to launch attacks on other systems.

The best defense against intrusion is an aggressive offensive posture. Tools the system administrator uses are passwords, special modems and encryption to lessen the risk of illegal entry.

Hackers rely on sloppy operating procedures and inefficient administrative practices to ply their craft. Sometimes it is as simple as *tailgating* on another user's session. This is accomplished by taking advantage of a user's inattention to proper log-off procedures. If a user hangs up without logging off, a hacker calling immediately afterward can connect and continue the modem session using the user's password and clearance. Since this practice is well known, most newer communications programs check for inactivity on the line and disconnect after a certain time interval.

Another known technique hackers employ is the use of a trojan horse. If he has gained a sufficient level of privilege on the target system, a wily hacker can plant a trojan horse. Usually these are programs listed with an interesting title.

And, there actually is a program associated with the listing, often a game. What the unsuspecting user does not realize, however, is that the program's trojan horse routine saves his account name and password to a file accessible by the hacker. In just such a manner, many hackers have been able to pick and choose between high level clearance accounts on target systems.

The methods are endless, but the fact is, the hacker must first get on the system before he can start testing to see if he can gain admittance to secure areas. This can be likened to walking down a long hallway twisting each door knob to see if any are unlocked.

Passwords are discussed elsewhere, but the point to keep in mind is that common words like: sex, secret, test, visitor, games, guest, password, work, okay, and God should be avoided at all costs. They are some of the most often used passwords, and are easy to guess by hackers (Landreth 83). Often the hacker builds a database of common words and tries each one in succession until one of them unlocks the door.

Such a database of passwords was one of the offensive weapons used by Cornell University graduate student John Tappan Morris to spread the InterNet virus. John McAfee describes how this was accomplished:

> Imbedded within the InterNet (ARPANET) virus was a list of commonly used passwords. The passwords enabled the virus to open user files on infected systems and find out the addresses for news hosts to infect (89).

McAfee points out that statistical analysis of password usage shows over 90 percent of large computer systems have at least one user with a password in Morris' list of 365 words (91). McAfee likens the list to a skeleton key opening myriad electronic locks.

The password dilemma can be controlled by educating users to the need for system security. End users need to understand how important their choice of passwords is to the security of the system. In general, the longer the password character string, the better the security. Numbers and letters combined are harder to crack, and the further the password reference is from the user, the better.

Besides passwords, there are several additional safeguards to communications security in the administrator's arsenal. First, there are specialty modems which make communications over telephone lines much more secure.

The first such modem is the answerback modem. Unlike passwords that allow access by users with specific *knowledge* like the password, answerback modems allow access to the host system because of specific *equipment* at both ends of the telephone connection. Howard Marks, a New Jersey based networking consultant, describes what takes place when one answerback modem calls another answerback modem:

> When the host system answers the call, it sends a code to the caller called WRU for Who aRe yoU. When the caller's system receives the WRU, it sends back a short message called its answerback.

> The caller can access the system only if its answerback is acceptable. Answerback has been used for many years by the Telex network and is well proven in the field (242).

While answerback verifies specific equipment, callback modems pinpoint a specific *location*, in this case a phone number. As soon as connection is made with a callback modem, the computer asks for a specific password. Once the password is exchanged, the host disconnects from the caller and calls back the caller at the telephone number registered in its database. Obviously, mobile computer users cannot use such an instrument since the host system will call only one number.

It is a good idea to have the host system call back on a separate telephone line, rather than the one used by the caller. This ensures that tailgating cannot take place on the call-in telephone line. Tailgating can occur when the caller sends a dial tone down the telephone line tricking the host modem into thinking it is safe to dial out. With two separate lines, this is not a problem. Dean Hoven of Citicorp says that in conjunction with callback modems, he monitors activity on each of his call-in lines. If a number of attempts are made to access the host system without the right password, he will change phone numbers assigned to the modem. Citicorp has several additional lines normally not in use so that computer communications can be established from a pool of numbers.

Hoven also recommends that telephone numbers be from different exchanges so that a hacker has a much harder time reconnecting with the system. Although Citicorp does not go to the expense, those living in cities that straddle state lines like St. Louis and Kansas City could actually draw from numbers in different area codes as well as exchanges, making the guessing game even harder.

Encryption

Encryption is a method of securing corporate data by scrambling the letters in a file or message in such a way that the outcome looks like "garbage" to anyone intercepting the message. At the receiving end, the process is reversed transforming the message back into a useable form. This method of security is used for both voice and data transmissions, especially on satellites where interception of the transmission is relatively easy. This same method can be used to secure computer data of a sensitive nature. The files are encrypted when they are stored, and can only be decrypted by someone with a matching "key."

Jim Bienkowski, president of BM&T Consultants, a planning service for financial institutions, says that "the security of the data encryption depends on the secrecy and protection given to encryption keys" (9). Key management entails the generation, storage, distribution, and disposal of electronic keys by the organization.

There are several schemes used to scramble the letters in a message into its coded form. Among the most common are simple transposition codes, scrambling, couple codes, and data packing.

Transposition is by far the easiest of the encryption techniques to use, but also the easiest to crack. Transposition replaces one letter for another. With a little patience and a table of the most commonly used English letters, an experienced code breaker would have little trouble in decrypting files.

Scrambling is somewhat more sophisticated in its approach. The scrambling technique uses information fields, like name and address, and views them as a field where individual letters are shuffled to predetermined locations. They are decrypted by reversing the process.

Couple codes employ the use of sets of letters that are replaced with other sets. This technique works well with text as well as numbers and can be made considerably harder to break by replacing certain couples with two or more replacement values. A frequency of use table is then used in conjunction with the key to decrypt the data.

Data compression recognizes that in most fields, there are bits on each byte that can be used in two distinct ways. It is possible to pack characters closer together, for instance, four letters into three data bytes, or the overhead bits can be used to create an additional character.

These four techniques can be used in various combinations as long as care is taken in the original setup of the encryption system. Louis Mills, president of Henge Corporation in Petalmua, California, warns that simple techniques are not enough to keep data secure:

> None of the four techniques described are sufficient for good security. They are only alternatives in a scheme of protection that starts with a security plan and includes the vigilant efforts of everyone on staff, a physically secure site, restricted access and a host of other considerations.
>
> Don't depend on one simple code to protect your data. However, you can combine all these techniques to ensure top management that their information is secure (23).

The second level of countermeasures, administrative, helps to determine the risk to the computer and the data it holds. A discussion of administrative countermeasures follows.

Administrative Countermeasures

Felix Pomeranz, author of four books and an advocate of advance auditing technology suggests that level two countermeasures include risk management, tape backup and storage policies, disaster recovery plans, and auditing procedures (72).

Risk Management

Risk management touched on earlier, and amplified here, deals with the system administrator's use of "what if" techniques to try and assess the vulnerability of the system, and addresses measures to combat those risks. Thomas J. Knapp describes data security analysis as a program designed to assist management in "identifying data security weaknesses, the probability of the risk occurring, and the cost associated with the security penetration" (23).

Knapp uses the example of a weakness in password security to illustrate his point. If password protection fails, then unauthorized data could be introduced into the database, unauthorized program modifications could be inserted in program code, and unauthorized disclosures from the data could be made. Knapp maintains that "the potential cost of a security penetration constitutes a significant element in the development of a data security program" (24). For every risk, there is an associated cost to repair or replace hardware, programming, and the database that is destroyed or stolen. Knapp concludes that "the probability of the risk occurring estimate, multiplied by the asset value assessment for each potential loss considered in the data security profile, indicates the dollar amount that could be spent to protect the information asset." Sometimes it is difficult to determine exact costs for replacement or repair. In this case, management must use good judgement in determining the true cost. Knapp concludes:

> The risk analysis technique requires significant subjective interpretation and weighing in the process of attributing value to data, assessing the cost of business interruption or loss of assets, and defining the probability of a security penetration.
>
> It is imperative that the organization's management be involved in preparing the risk analysis and determining the evaluations (25).

Data Backup and Storage

Under law, a company is required to keep vital records from harm. Some of these records include: permanent financial records, personnel records, settled court cases involving the organization, bylaws, minutes books, accounts payable files, patents, database and backup systems software. Companies are also obligated to protect their charters, stock certificates and other information relating to shareholders.

Of special interest to the DP manager is a set of contingency files needed to restart a company following disaster. Vital items include: the database and systems software, system manuals and other documents such as blueprints, a list of all key people with addresses and up to date phone numbers. The list should also contain vendor phone numbers and contacts. Other items needed are: blank payroll checks, extra stationery and forms.

Dean Hoven of Citicorp's Treasury division adds to this list of "must have" documents. "I keep a map to the recovery site in my brief case. It goes home with

me every night. I also keep extra credit cards for emergency use as well as the account book for a petty cash account in case we need to rent equipment or hire temporary workers," says Hoven. Hoven, a stickler for strict backup and recovery procedures, maintains that he is confident that "the guts of my organization can be up and running in a short span of time. Perhaps one percent of information is stored on floppies in desk drawers in the affected plant" (Interview). He adds that usually these unprotected floppies are used by system users to make work easier. One such utility might be a communications program log-on sequence saved to disk. These files are important, especially at restart because they enhance the worker's ability to increase his productivity.

Experts agree that backup copies of systems and application software need to be kept in a secure off-site facility. In addition, periodic backups of the database need to be rotated to off-site storage. Depending on the amount of information that changes each day, a backup system can be implemented on a daily or weekly basis.

Jean Hiltenbrand of Archives Inc., a commercial records storage facility in Memphis, says that "auditors and insurers are beginning to play a definite role in rotation decisions by requiring records be updated more often, and that security copies be stored off-site" (19). Table 11 lists Hiltenbrand's recommendations for assessing off-site storage for computer records.

Table 11

Off Site Storage Recommendations

- The building should be secure in a safe location, at least four miles away from the shop if possible.
- An off-site monitoring system for fire, smoke, temperature fluctuation and illegal entry should be installed.
- A special room for tapes should have temperature and humidity control.
- Two-hour turnaround in event of emergency should be required --preferably one hour.
- Check for good housekeeping. Is the facility relatively dust free?
- Delivery service should be available.
- Twenty-four hour emergency delivery is a must.
- Check security procedures used when entering the facility. Is it adequate?
- Observe as many employees as possible. Are they bonded?
- Are fire extinguishers available?

SOURCE: Jean Hiltenbrand, *Data Management*, July 1983

Disaster Recovery

Every organization dependent on computers, and that includes virtually all but the smallest shops today, should have a well documented and tested disaster recovery plan. The disaster plan should include the items listed under important records in the backup section above, plus complete plans for use of an alternate computer site. This site may be a duplicate computing center owned by the organization in another location, a hot site consisting of duplicate equipment usually owned by a group of firms with similar computing needs, a shell that provides electric and space for a fee, or a handshake agreement with another organization nearby.

The most expensive, but most reliable situation is a duplicate computing center owned by the organization. Benefits of the duplicate center are:

1. The firm does not pay monthly fees for holding space.
2. It is the company's own equipment, therefore an asset.
3. The duplicate equipment can be used during overflow periods or routine downtime of the main system.
4. The facility can be used as a company service center (Hiltenbrand 20).

The second best approach is to join a consortium of organizations using a jointly owned fully equipped "hot site." A hot site provides almost immediate restart since all that is needed to begin operations is time to mount system and database software and begin computing. The site can also be used for overflow work and as an alternate site during routine downtime. The disadvantage is that each organization has an equal stake in the facility, and must share the center with others. This is a distinct disadvantage if the disaster is of a general nature, and affects several of the member organizations.

The third alternative is the "shell" approach to recovery. In this system, the organization pays monthly fees for warehouse space that can provide adequate power, heating and cooling, and communications if it must be used as an alternate site. In this mode, organizations sign agreements with vendors that guarantee delivery of replacement computer systems within a matter of days. Of course this equipment still must be installed, tested and prepared for the organization's use, but vendors often can provide additional personnel to assist the quick installation and utilization of the equipment.

The fourth and least desirable method of alternate computing facilities concerns the "handshake" agreement. Essentially, the handshake agreement is a gentlemen's agreement between two organizations that pledge mutual support in case of emergency. The problem arises when the host company is already

running at near capacity and there is no time for the sharing of facilities. This is often the case in middle to large organizations.

John Deal, of Botz, Deal & Co., P.C., believes that the handshake agreement is a viable method for small firms that do not run at capacity. He says that he routinely pairs companies with like equipment and software and works out agreements between the two. This implies that small firms can be best served by gentlemen's agreements while larger installations need to choose between duplicate facilities, joint hot sites, or shells.

No disaster plan is valid if it has not been tested. Citicorp's Dean Hoven believes in surprise drills designed to measure the true worth of the plan should a disaster strike. He describes the drill as follows:

> On a given day picked at random by management, key operating personnel get a call at six in the morning saying a disaster struck the data center and it has been wiped out. These key players have secretly been relieved of normal duties for two or three days so that they can participate full time in the drill.
>
> Others reporting for work are told to report to their pre-assigned disaster meeting point, usually a hotel ballroom or warehouse nearby. At the first meeting, the players are given an assessment of the damage and told what systems are out of commission.
>
> The participants are each given assignments and problems to solve. As an example, payroll is told there are no facilities for cutting payroll checks this week. Until backup payroll tapes can be mounted in a duplicate facility, they are to decide how the checks can be issued since the recovery center only has enough checks for half the personnel.

> Real life problems like this must be solved on your feet. Do we hire temporary help to manually compute checks and type them by hand? If so, where do we get the temps and typewriters? Where do we get space and desks? Where do we get blank company checks?
>
> These kinds of exercises painfully point out problems in the disaster plan, and revisions are made so that duplicate payroll records are kept at our New York alternate site, and adequate supplies of blank payroll and accounts payable checks are kept on hand in off site storage (Interview).

Hoven believes that only with periodic drills and reviews can a disaster plan stay current. Only at the point where the plan is a viable backup to the main facility has the job been accomplished. Hoven believes that the recovery plan is only good until new equipment and software are installed. Then the review process must begin all over again.

Security Administrator Hoven concluded the interview by saying "planned disaster drills, for instance, on the 15th of next month, serve no purpose because the participants are aware of the upcoming trial and work through problems ahead of time" (Interview).

Auditing Procedures

Correct accounting procedures are necessary to ensure the integrity of the system and the data contained in the system. Several well known procedures help to safeguard against fraud or carelessness. They are: segregation of duties, periodic checkups, analysis, and audits.

Table 12

Audit Functions

---

1. Evaluate customer credit-worthiness by reviewing the adequacy of allowance for doubtful accounts against norms in the industry.
2. Review the nature of items in inventory in light of market forecasts and economic conditions. Assess carrying values for slow moving goods.
3. Concerning physical property: Compare the client's policies with others in the industry with respect to depreciation, amortization, carrying values and write-offs.
4. Develop data for the appropriate valuation of nonmarketable or restricted securities. Check the treatment of the partner's books in joint ventures.
5. Identify dispositions of major parts of the business concerning possible declines in value.
6. Develop estimates in light of economic conditions, unsettled court cases, actions, fines or assessments.

SOURCE: *Annals of the American Academy of Politics and Social Science*, Felix Pomeranz, July, 1988

There are several steps necessary for an employee to conduct a fraud. First, there must be an asset to either steal, modify or destroy. Second, the perpetrator must be inclined to participate in fraud. Finally, the perpetrator must have the knowledge and the opportunity to access the asset.

Controls make sure that the perpetrator and the asset do not come in contact. Separation is one of the best methods of securing data. Fortunately the system itself can contribute to the segregation of assets from those seeking to damage or steal them.

Felix Pomeranz says that "studies have shown the need for foreclosing access opportunities by separation of custody of assets --or other items subject to conversion --from record keeping, or authorization of transactions from execution, and of planning from operations" (77).

Pomeranz, who is a Certified Public Accountant in four states, contends that the objective of separation of duties is to have different people responsible for record keeping, custody of assets, general supervision and, authorization of transactions.

Since no one person is a power unto himself, the system is secure from the threat of a lone perpetrator authorizing the use of data assets, manipulating those assets, and then changing reports to cover the abuse.

Periodic checkups by responsible consultants aid the DP manager in making sure the once secure system stays that way. Consultants and auditors

inspect the system for separation of duties, and can confirm that loss prevention controls are still working as they were intended.

A consultant's review should contain contingency plans for fire prevention and detection, disaster planning, heating / cooling plant failure, protection from hostile attacks, and backup practices.

Computer cross checks can help verify that the work reported done was in fact accomplished. Pomeranz relates the story of a steam ship line that, in collusion with stevedores, conspired to unload fake cargos from ocean-going vessels. This was accomplished in part by reporting loads in American short tons while in fact unloading enough cargo to fill English long tons. The difference is 240 pounds per ton of cargo unloaded (78). Cross checks make sure that the same units of measure or the same rate of exchange is globally used for all computations.

Auditors, in the words of the National Commission on Fraudulent Financial Reporting, should reaffirm "generally accepted auditing standards." They were admonished to "take affirmative steps to assess the potential for fraudulent financial reporting and to design tests to provide reasonable assurance against detection" (8).

Internal as well as external auditors can use the system itself to check for the integrity of data entry, the administration of security and for detection of

abnormal situations in the system. Table 12 describes functions auditors can perform for the organization.

Speaking of management controls, Data Security Systems Incorporated president Sanford Sherizen believes that many techniques such as the "need to know" theory and the separation of duties have been severely undercut by computer advancements:

> Managers need to be advised of this situation and informed that this requires other forms of control and supervision. Managers may not be held responsible for supervising employee activities that cannot be controlled with existing corporate procedures. Procedural and operational changes may be required in order to provide managers with the capability to act in proper control fashion and to assist users with proper security work habits (12).

Auditors and consultants alike provide a necessary service to the organization. They keep a watchful eye on day to day operations to ensure data integrity and security, and they are watchful for anomalies in the system that need immediate attention by management.

CONCLUSION

It is obvious that threats to the data center itself, and the organization's main asset, the database, leave top management and computer system admin-

istrators with little choice but to provide countermeasures for any likely breach in security. The tool used to ascertain the amount of risk to the computer center and its assets is the risk management survey.

The survey includes a listing of problems that can develop, the likelihood of the problem happening, and the cost to the organization if it does happen. With this assessment in hand, management can determine what steps are necessary to guard assets.

For management that is not aware of the severity of risk to the organization's ability to survive an emergency situation, the data center administrator must "sell" security and recovery plans to top managers. Price Waterhouse's Thomas Knapp suggests the following steps to ensure management awareness of security issues and their impact on the organization:

- ✓ Keep management informed of the data security impact of current hardware and software developments.
- ✓ Use terminology associated with other business risks such as: interruption of business operations due to data loss, unauthorized access of data by competitors, violation of legal require ments in record keeping and reporting.
- ✓ Assign data security responsibility to owners [users] of the data.
- ✓ Use the data security risk analysis method.
- ✓ Consider calling on an independent data security analyst or consultant (25).

With the countermeasures listed throughout this paper, help from qualified consultants and auditors, the organization's data can be secured from many of the perils mentioned. But, as changes to the system develop over time, only thorough, periodic reviews and drills can maintain the desired level of security to the organization's data assets.

Chapter V

DISCUSSION

Expert Review

James Bush, Field Service Technician for Honeywell Federal Systems, a Division of Groupe Bull reviewed this paper. He made several comments along the lines of clarification, but saw no flaws in overall presentation.

Mr. Bush has a wide variety of experience in mainframe, mini, and personal computer programming, as well as extensive experience in computer hardware installation and maintainence. His latest project involves the installation of 82 Apple MacIntosh computer work stations at Scott Air Force Base. His comments follow:

Backup and Recovery

> Backup and recovery cannot be stressed enough. I remember installing a DEC system for a medium sized business --an insurance agency-- some years ago. Included in the installation were two huge hard disks, one used mainly for system and applications software, the other for a large database.

At the time of installation, the manager and his staff were checked out on backup and recovery procedures. The customer's auditor recommended periodic backups of the database and off-site storage.

To make a long story short, after about six months we received a frantic call from the insurance company. There had been a terrible storm that knocked out power for several hours. When electricity was restored, both hard disks would not come up.

We spent considerable time trying to recover data on the hard disks, but the heads had gouged the surface of the media rendering them absolutely useless.

The moral here is that over the entire six months of operation, not once had they taken the trouble to back up the system. Their accounts receivable, accounts payable, customer records and many other files were lost forever. Edsel Murphy was right. If something bad can happen, it will. Murphy was certainly proved right by the insurance company.

The other point about hard disks that I feel does not get enough coverage is that they have a limited life span. Disk drives today are very reliable. The mean-time-between-failures is rated in the tens of thousands or hundreds of thousands of hours. That doesn't mean however that *your* hard disk will last that long. Sooner or later the disk is literally going to fly apart. For this reason, if for no other, the wise DP manager will back them up (hard disks) on a regular basis.

System Security

My work at Scott Air Force Base has taught me that even professionals who are used to physical security do not pay attention to data security unless they are forced to do so.

Part of the problem is that encryption and other security measures slow down the overall performance of the system considerably. There is always a trade-off between ease of use and tight security. Unfortunately you can't have both so you have to reach a compro-

mise. This compromise is based on the sensitivity or value of the data.

Passwords

We have designed a password program that forces password changes and also denies the user super-easy passwords. In fact, the program looks for characters not usually associated with passwords like an "at" (@) sign or asterisk. The unusual characters make it that much harder to guess passwords.

Mr. Bush's comments dovetail nicely with the general background information obtained during research, and the articles cited throughout the paper.

The next section lists three additional areas of study that could lead to a new awareness of computers and their use.

Suggestions For Future Research

Destructive Nature Of Hackers

Hackers have anti-social tendencies and very often project a bleak view of life in general. Below are illustrations to suggest that many hackers have a proclivity for destructive, and/or self-destructive behavior. The examples that follow illustrate the darker side of the hacker psyche.

The first example is a computer hacker that apparently could not live with the guilt and scandal associated with his theft of account names and passwords from United States military computers. The West German hacker, Karl Loch was suspected of providing code words for Western computers for the Soviet KGB. He was found dead on June 5, 1989. Wolfsburg, West German police found Koch, 24, burned to death. Police speculated that Loch doused himself with gasoline and set himself on fire. There were no signs of foul play (AP).

Secondly, members of the West German Chaos Computer Club of Hamburg illegally accessed international phone lines to enter NASA and military networks in the United States. It took three months of work to eradicate all traces of the club's work (Roberts, Kane 17).

The third illustration concerns the Milwaukee 414s computer club that crashed the Sloan-Kettering cancer monitoring system in New York. The club successfully infiltrated over 60 systems before detection. One of these systems was a super-sensitive nuclear weapons establishment in New Mexico (McAfee 45).

Lastly, William Troy Landreth, author of *Outside The Inner Circle*, now lives on the streets in San Diego. He is a drop out from society. Even though Landreth had over $9,000 in book royalties in the bank when he was given probation for wire fraud, he chose to live his life on park benches by day and shelters and doorways by night.

Landreth, with an IQ of 186, well into the genius category, perhaps summed up the true feelings of many hackers. The 24 year-old left an eight-page letter when he dropped out saying:

> I was bored in school, bored traveling around the country, bored getting raided by the FBI, bored in prison, bored writing books, bored being bored. I will probably be bored dead, but this is my risk to take (AP).

An in-depth study of the hacker mentality could lead to new insights into their compulsion for invading other systems. Are they playing God? Why are they more comfortable with computer keyboards than face to face confrontations with humans? I believe this would make an interesting study for those interested in the psychological makeup of hackers, and their compunction to intrude into systems illegally.

Endeavors to Secure Computers

The military and the National Security Agency (NSA) among others are striving to build the most secure computer possible. The Tempest standards -- fiber optic communications interconnections, shielded computer centers to prevent radio frequency leakage, new methods of encryption-- are today's most stringent standards for securing computers and data. Comments by David A. Gabel in PC Magazine describe Tempest standards:

> Tempest represents a closely held body of techniques for ensuring that computing equipment and other communications devices do not act like a broadcast antenna, letting secrets into the airwaves or other media that might be picked up by an eavesdropper. It is the centerpiece of the Department of Defense's (DOD) security requirements for all computer systems (97).

Obviously, this would be a tricky area to investigate since many of the techniques are secret at this time. Some techniques are most likely overkill for business computer users. However, some of the techniques will be available in coming years for use by any computer user who needs to protect data from invasion. As more information becomes available, this could develop into an interesting area of study.

Introductory Manual For New Hires

Due to the time constraints imposed finishing this paper and working two jobs, I did not pursue the idea of constructing a computer security manual aimed at business new hires. I believe the information contained in this paper, plus additional research could result in a concise, factual manual for new employees.

In informal discussions with several people involved with computers in their work, I found that most companies did not have a formal computer policy indoctrination for those new to the company.

A generic manual that each DP center could build on would be a great asset to business. I envisioned a "fill in the blanks" format that admin-

istrators could either photocopy or typeset depending on their needs. It would go a long way toward making employees aware of the reasons for security.

The dark side of computer hackers, new computer security techniques, and an introductory computer security manual for new employees are my three suggestions for further research in this broad, ever-widening area of computer security and data integrity.

Works Cited

Augarten, Stan. *Bit by Bit: An History of Computers*. New York. Ticknor & Fields. 1984.

Baker, Richard H. *The Computer Security Handbook*. Blue Summit, Pennsylvania. TAB Books Inc. 1985.

Bidgoli, Hossein, and Azarmsa, Reza. "Computer Security: New Managerial Concern for the 1980's and Beyond." *Journal of Systems Management*. October, 1989: 21-27.

Bienkowski, John. "Telcom and Data Security." *Bank Bytes*. March, 1987: 9.

Bloom, Robert. "Computers Don't Commit Crime." *Data Management*. July, 1983: 14-16.

Bolt, John A. "Protecting Computers From Hackers Crucial to Doing Business, Experts Say." *Associated Press*. April 4, 1989.

Bradford, Michael. "Plan for Computer Security, Experts Say." *Business Insurance*. November 12, 1984: 88-89.

"Biometric Cops: High Tech Security Guards are Putting a New Lock on Security." *Business Wire*. October 13, 1989.

Cane, Mike. *The Computer Phone Book*. New York. New American Library. 1983

Carter Lindy Keane. "Master That Disaster." *Association Management*. April, 1988: 79-84.

Cook, William J. *The Joy of Computer Communication*. New York. Dell. 1984.

"Corporate Security: Update '83." *Dunn's Business Month*. December, 1982: 91-94.

Deitz, Larry. "Computer Security in the MicroAge." *Computers & Electronics*. June, 1984: 68.

Dotto, Lydia. "The Magic Word Spells Open Sesame." *Canadian Business*. May, 1983: 72-74.

Drahos, Leslie, "The Key to Good Security." *GPN Magazine*. October, 1983: 12-20.

Fallon, William K., Ed. *AMA Management Handbook*. Second Edition. New York. American Management Associations. 1983: 8-40.

Fife, Dennie W., Hardgrave, Terry W., Deutsch, Donald R. *Database Concepts*. South-Western Publishing Co. Cincinnati. 1986.

Fites, Phillip, Johnson, Peter, Kratz, Martin. *The Computer Virus Crisis.* New York. Van Nostrand Reinhold. 1989.

Fish, Toni B. "Are You Doing Anything?" *Computerworld.* June 3, 1987: 23.

Gabel, David A. "Tempest: The Watchword for Federal Security." *PC Week.* May 12, 1987: 87-88.

Gauthier, Michael R., and Buchanan, Julie K. "Planning for Data Doomsdays" *Across The Board.* October, 1989: 47-51.

"Genius Computer Hacker Now Living on the Streets." *Associated Press.* San Diego. March 19, 1989.

Good, Phillip I. *Increasing Your Business Effectiveness Through Computer Communications.* Radnor, Pennsylvania. Chilton Book Company. 1985.

Greenberg, Ross M. *Flu_shot +, A Form of Protection From Viral and Trojan Programs.* New York. Software Concepts Design. 1990.

Harris, Norman L. "Rigid Administrative Procedures Prevent Computer Security Failure." *Data Management.* December, 1984: 13-16.

Hassett, James E. "Hot and Cold Data Centers" *Datamation.* March, 1981: 176-180.

Hiltenbrand, Jean. "Records Retention: Manager's Involvement is Crucial." *Data Management.* July, 1983: 18-20.

Kenda, Margaret. *Crime Prevention Manual for Business Owners and Managers.* New York. American Management Associations. 1982.

Keogh, James Edward. *The Small Business Security Handbook.* Englewood Cliffs, New Jersey. 1981.

Knapp, Thomas J. "Selling Data Security to Upper Management." *Data Management.* July 1983: 22-25.

Kroeber, Donald W. and Watson, Hugh J. *Computer-Based Information Systems: A Management Approach.* New York. Macmillian Publishing Company. 1984: 182-244

Landreth, William, and Rheinbold, Howard. *Out of the Inner Circle: A Hacker's Guide to Computer Security.* Bellevue, Washington. Microsoft Press. 1985.

Marks, Howard. "For Your Ears Only: PC Security Modems." *PC Magazine.* February, 27, 1987: 241-248.

McAfee, John, and Haynes, Colin. *Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System.* New York. St. Martin's Press. 1989.

McCown, Davis. *Computer Security: The Newsletter for Computer Professionals.* Number 86. Northborough, Massachusetts. 1989 3-4.

Mills, Louis R. "Four Simple Encryption Techniques Help Ensure Data Integrity." *Data Management.* December, 1984: 22-23.

Missouri Revised Statutes. Cumulative Supplement 1989. Volume 2. Jefferson City, Missouri. 1989: 1502-1505.

Much, Marilyn. "Gearing up for Disaster." *Industry Week*. January 21, 1980: 79.

Murphy, Brian J. "Telecommunications Talk." *Creative Computing*. January, 1984: 266-270.

Murry, Toby. "Don't Get Caught With Your Plans Down." *Records Management Quarterly.* April, 1987: 12-17.

"NEMA's Fire Safety Guidelines." *Buildings.* April, 1984: 94-97.

"News Executives Charged With Computer Hacking." *Associated Press.* Tampa, Florida. May, 11, 1989.

Nicholai, Carl. "Encryption Decyphered." *Computers and Electronics.* June, 1984: 64-70

Pomeranz, Felix. "Technological Security." *The Annals of the American Academy of Political and Social Science.* Number 498. July, 1988: 70-81.

Price Waterhouse. *The Computer Virus Handbook.* New York. Price Waterhouse. 1989.

"Probation Ordered for Two TV News Executives." *Associated Press.* Tampa, Florida. May 19, 1989.

Roberts, Ralph and Kane, Pamela. *Compute!s Computer Security.* Greensboro, North Carolina. Compute! Publications. 1989.

Ratliff, John. "To Sell Disaster Recovery, Think in Terms of Corporate Insurance." *Data Management.* December, 1984: 17-19.

Reppert, Barton. "Computer Ethics." *Assiciated Press.* November 26, 1989.

Rothfeder, Jeffrey. "Is Nothing Private?" *Business Week.* September, 4, 1989: 74-82.

Rowley, James. "Jury Indicts Cornell Student of Computer Virus Allegations." *Associated Press.* Washington. July 26, 1989.

Scawthorn, Charles, and Gates, William E. "Secure Data Centers From Seismic Disturbances." *Data Management.* February, 1985: 30-33.

Sherizen, Sanford. "Successful Security Relies on Corporate Awareness Training." *Data Management.* December, 1984: 10-12.

Stifter, Frank. "Power Surveillance Can Control Dubious Data." *Data Management.* July, 1983: 26-27.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York. Doubleday. 1989.

"Suspected KGB Computer Hacker Apparently Commits Suicide." *Associated Press*. Wolfsburg, West Germany. June 5, 1989.

Tangorra, Joanne K. "Insurance Against Disaster." *Datamation*. July, 1982: 70.

"Three Charged With Giving Soviets Info From Western Computers." *Associated Press*. Frankfort, West Germany. August 16, 1989.

Victor, Jesse. "UPSES Keep Pace With user's Needs." *Mini-Micro Systems*. April, 1986: 93-102.

Ward, Gerald M. "Securing a Micro-Mainframe Link Demands Detailed Action Plans." *Data Management*. December, 1984: 20-21.

Wolfsey, Marvin M. "User Identity Precedes Friendly Computers." *Data Management*. December, 1984: 15-16.

Wood, Robert Chapman. *Connections: Telecommunicating on a Budget*. Grandview, Illinois. Scott, Foresman and Company. 1986.

Yonda, Marge. "No GIGO Allowed." *Modern Office Technology*. September, 1985: 126-130.

Zalud, Bill. "Computer Criminals Will be Prosecuted: Adopting a Prevention First Attitude." *Data Management*. April, 1983: 30-45.

Interviews

Deal, John. Partner, Botz, Deal & Company, P.C. Personal Interview. May 17, 1990.

Hoven, Dean. System Security Administrator for Citicorp MBT Information Systems. Personal Interview. March 3, 1990.

Bush, James. Field Service Technican, Honeywell Federal Systems. Personal Interview. April 15, 1990. Follow-up Telephone Interview. June 1, 1990.