OSRA

OFFICE SYSTEMS RESEARCH JOURNAL

The Journal of the Office Systems Research Association
Vol. 11, No. 1, Fall 1992

Information Protection in Automated Offices

Hossein Saiedian
Steve Bang

University of Nebraska
Omaha, Nebraska

Abstract

*An **office information system**, consisting (minimally) of several interconnected computer systems, makes it possible to automate many structured office tasks and/or improve the effectiveness of office workers in performing unstructured tasks. As a result, valuable information is stored in electronic media that is more difficult to protect than either traditional manual office systems or traditional centralized Automatic Data Processing (ADP) systems. In this paper, we identify and explain threats to office information, in the form of malicious acts and unintended mishaps. We believe that before an information protection plan is formulated, the threat should be assessed. The time and expense devoted to information protection should be commensurate with the threat and the cost of lost or stolen information. We provide guidelines for a combination of security mechanisms and policies to protect office information.*

An office is the central part of an organization that receives, generates, stores, and distributes information, and manages and coordinates the organization's activities. Much more than a physical entity, the office houses and facilitates a set of organizational relationships and procedures that are focused on the creation and distribution of information.

In recent years, there has been an increasing demand for computer systems to support routine and casual office information processing activities. Under the theme of *office automation*, considerable research work has been done (Tsichritzis, 1985; Arn, 1988; Barcomb, 1989) and both office automation equipment and computer-supported cooperative work systems for office use are emerging as commercial products. Office automation goes beyond the older office mechanization technologies, and consists of the integration and support of various office procedures such as document preparation, electronic filing, electronic mail, administrative and decision support, etc., by networked computer systems. Communication systems are necessary to integrate and automate office procedures.

Almost all work done in any office involves some form of information. Some offices deal directly with customers and clients,

receiving orders and requests, sending these orders and requests to other offices, preparing invoices, and answering inquiries or complaints. Other offices provide leadership and management services to the organization. Executives establish and communicate policy. Accounting offices process and store financial information. Personnel offices recruit employees and store employee performance reports. Based on these functions, we can define an office as a place where information is received, generated, modified, stored, and communicated.

Information is defined as any fact or knowledge. This includes numeric, sound, graphic, and textual information. Some simple examples include personal data on employees, customers, and clients, inventory records, sales records, production records, invoices, account receivable statements, letters, memos, policy statements, personnel performance reports, forecasts, drawings, charts, forms, and designs. Information also includes more abstract ideas and documents such as business proposals, product designs, marketing plans, and corporate strategy. The variety of information is practically endless.

Since information plays such a central role in an office, it is an asset that is very valuable to the organization. Managers make decisions based on available information, financial information is used to bill customers and reimburse suppliers, and customer orders determine production requirements. Loss of information can be fatal to the organization. Clearly, information should be protected from loss, alteration, or theft. As we shall see, this is becoming more difficult to do.

In the "old days," office workers performed many tasks with typewriters, adding machines, hand-delivered mail, hand-written memos, telephones, and filing cabinets. Information was always recorded in visible, human-readable form, such as a letter or report. Workers and managers at all levels understood what information was available and how information was processed and communicated. Since the information and the media was well understood, managers knew that access to information should be limited, and physical security measures could be taken to limit access.

Woo & Lochovsky (1986) classify office tasks into *structured* and *unstructured* tasks. Structured tasks are of a routine nature for which some prescribed step-by-step solution exists. Unstructured tasks on the other hand require creativity and human intervention and are, therefore, difficult to completely automate. An office information system (OIS) can more specifically be defined as a set of diverse, physically dispersed, autonomous, and highly interactive components, connected via a computer network. The purpose of the OIS is to automate mostly structured office tasks. These tasks are more complex than word processing by itself, but there is an established step-by-step procedure. A typical structured office task requires gathering information from several sources and securing the approval of several authorities. In a manual system, a form or folder full of forms is the conduit for gathering information and approvals. The forms are hand-carried or sent by inter-office mail to each office. An example in a university is an application for graduate degree candidacy. The candidate obtains a form from the Graduate Studies Office. He or she fills in personal information, previous education background, and a planned curriculum. Then a faculty advisor reviews the application and either signs and forwards it to the department chair for approval or returns it to the candidate for changes. The department chair then can approve it and forward it to the Graduate Studies Office. There, a copy is sent to the candidate and the original is filed. An OIS could automate the process. The OIS could create a file with an electronic copy of the application form. The candidate or the secretary taking the application could enter the required information from a terminal and send the file to the advisor. The advisor could indicate recommended changes and return it or indicate approval and forward it to the department chair. The department chair could indicate approval and forward it to the Graduate Studies Office. There, it would be electronically filed and an approval copy sent to the candidate. This automation is known as *office automation* (OA).

OISs come in many different combinations of components, so they must be broadly defined. However, an essential characteristic is that most of the computing power resides in a collection of microcomputers or work stations, rather than a minicomputer or mainframe. A communication network allows the microcomputers to share files and to pass messages. OIS components include microcomputers, work stations, application software designed for office

automation, communication network hardware and software that enable information to be transferred from one component to another, and peripheral devices such as printers, plotters, and scanners.

Information protection methods and policies that apply to manual office procedures are not sufficient for automated offices. OA introduces new vulnerabilities to the loss or misuse of information. The system encodes information and stores it or communicates it in a form that is not human-readable. Stored information can be quickly destroyed, copied, or transmitted to another computer. These activities are not readily detected.

An OIS also lacks many of the information protection features of a traditional automatic data processing (ADP) system. In contrast to an OIS, traditional ADP environments consist of large mainframe computers and minicomputers and have been in existence longer and have more sophisticated information protection provisions. Traditional computer systems are centrally located in a highly controlled and protected environment that is ideal for expensive electronic equipment. Cipher locks and intrusion alarms provide physical security. Special fire detectors, fire extinguishers, air conditioners, and electrical power conditioners safeguard the equipment. A trained staff operates the computers. Office workers have limited access to them only by means of a remote terminal. Traditional computer systems have operating systems with security provisions to limit access to the software and information stored on the system. These larger computers usually have database management system (DBMS) software that efficiently stores and retrieves information. The DBMS has security features that provide additional information protection.

The components of a modern, computer-based OIS are physically located in the office where many people have access to them. Most microcomputers, including MacIntosh and IBM PC or compatibles, use operating systems that do nothing to protect information. Physical access to the machine gives a person access to all of its software and data files.

This article discusses information protection issues peculiar to OIS (in contrast to manual office procedures and more traditional ADP systems). In the next section we describe some potential problems caused by either malicious acts or by unintended mishaps. Then we discuss the need for an assessment of OIS vulnerabilities, followed by some information protection mechanisms and policies that apply to an OIS, and our concluding remarks.

Threats to the Office Information Systems

Threats to the OIS can be either malicious acts by people or unintended mishaps. In many cases the outcome is the same whether the cause was malicious or accidental. For example, information can be modified or lost due to a malicious act or due to an unintended mishap. Many information protection safeguards apply to both forms of threats. We will first look at malicious acts, and then unintended mishaps.

Malicious Acts

Malicious acts can be committed by employees of the organization as well as outsiders such as customers, competitors, software vendors, service people, professional criminals, or even individuals who view these acts as a recreational sport.

Malicious acts are often in the form of unauthorized viewing (browsing) or theft. Information can also be modified or destroyed entirely (Vaughn, Saiedian & Unger, 1993). We will examine overt acts by individuals and malicious software, and attacks on the availability of OIS resources.

Browsing

Browsing is systematic or casual examination of stored information by someone who should not have access. This can happen either because the OIS has no security mechanisms to prevent it or because the browser has successfully bypassed the security mechanisms. This gives an employee, customer, or competitor access to financial or personal information that they should not have. For example, most employees should not have access to salary information or performance reports on other employees. Customers and competitors should not have access to sales and production information or product designs.

Most microcomputer operating systems do not protect information stored on a fixed disk. Anyone who has physical access to the computer can browse the stored information. It is even easier to browse files that are on removable magnetic media such as diskettes.

They can be inserted in any machine and browsed.

In a local area network (LAN), one microcomputer is a server. It has a large fixed disk which holds files that are shared. LAN software typically requires that users log in with a secret password before they can have access to any files. In addition, files on the server are segregated into several directories. The LAN administrator specifies the users that have access to each directory. These safeguards provide adequate protection for information provided the users and the administrator have the discipline to comply with the required procedures. However, if access to directories is not properly limited, or if passwords are not protected, information stored on the LAN server can be browsed.

Theft of Information

If browsing uncovers valuable information, theft is often the logical next step. There are many ways this can be done, depending on the safeguards in place. We will describe several methods. Diskettes can be stolen. This is very easily done by employees who have access to the diskettes. A diskette is physically small but holds a large amount of information. It can easily be carried in a brief case or purse. In general, information on a fixed disk or LAN that can be browsed (as described earlier) can also be copied to a diskette. Once copied, the diskette is easily taken away. However, copying is impossible when a microcomputer does not have a diskette drive.

More sophisticated methods of stealing information include intercepting communication channels. This is possible when commercial telephone lines are used to transfer information. Telephone signals are often transmitted through the air with microwave technology. An antenna can be erected to eavesdrop on these signals. It is also possible to tap telephone wires.

One of the most sophisticated means of intercepting information is by detecting electromagnetic emanations. When electric current passes through a wire, electric and magnetic fields are induced. If the current is fluctuating, as it must to communicate information, some of the wiring will behave as an antenna, radiating electromagnetic waves. The strength of these signals dissipates with distance, and many computer components operating in a small area create a lot of noise for a would-be eavesdropper. Intercepting the information carried by these emanations is a great technological challenge and, therefore, not likely to be successfully used against most organizations.

Another very sophisticated method of stealing information is to use covert channels. Here, information is encoded inside some other information. For example, a system variable is periodically modified according to a code. Covert channels are usually slow and require the cooperation of some person or some program that has permission to access the information.

Unauthorized Modification

Information can be modified to change its meaning or to obliterate it. Examples include changing financial or inventory numbers for monetary gain, changing a personal performance report or product evaluation to make it more favorable, or deleting orders, reservations, or shipping instructions. As a result, dissatisfied customers take their business elsewhere.

A related problem arises when an automated office task requires that certain individuals indicate their approval on an electronic document. This might be an approval of a purchase order or the approval of some other action. If another person can impersonate the approval authority, then the document can be falsely approved.

Unauthorized modification can attack stored information or information that is passing through a communication network. In the first case, the perpetrator gains read/write access to a stored file and modifies it. As stated earlier, most microcomputer operating systems do nothing to deny read/write access to information stored on their fixed disks. A person can modify information stored on a LAN server if he or she has been given read/write access. If read/write access is denied, a person can look for holes in the security software. For example, he or she can try to guess the password for someone who has access. A program containing a virus or Trojan Horse can sometimes assume the identity of someone who has read/write access. These programs are described below.

Alternatively, information that is transmitting a network is intercepted, modified, and sent on to its destination. This is a much more sophisticated attack, and it is quite unlikely on many networks because of timing constraints.

Malicious Software

Software can be used in two ways to commit malicious acts. A computer "virus" is a piece of code that inserts itself into a host (including the operating system) to propagate (Reynolds, 1991). A virus is, thus, a malicious piece of software that is hidden in a program. When the program is executed, the virus takes control at some point and copies itself onto other program files in the same system. It then returns control to the main program. If any of the infected program files are copied onto another system, the virus spreads on that system, too. Eventually, many computers acquire copies of the virus. The virus is designed to detect a triggering event that causes it to do some mischief. For example, it might check the system clock and delete some files on Friday the Thirteenth. There are many other triggering events, and the mischievous action can range from displaying a message on the screen to modifying or destroying information or programs.

The detailed issues related to *computer viruses* is beyond the scope of this paper. Readers are encouraged to see Peter Denning's timely work entitled *Computers Under Attack: Intruders, Worms, and Viruses* (Denning, 1990) for a comprehensive discussion of viruses. In his book, Denning collects some of the most informative, provocative, and frightening reports on the vulnerability of computer systems to harmful attacks. The articles recounted in Denning's book are a pointed warning that our computer systems are already under attack, that the privacy and integrity of information in our personal, business, office, and research activities are seriously threatened and that the security of free societies is on the line.

A Trojan Horse is similar to a virus but lacks the capability of copying itself and spread to other systems. It is a program that performs useful functions but has concealed in it the capability to perform harmful or destructive functions. The Trojan Horse is given or sold to the victim in hope that the program will be installed and executed. Trojan Horse programs vary greatly in their intended ill effect. They can defeat security controls, steal information, modify information, or destroy files.

A variation of the Trojan Horse is the false login program. This program displays a screen that appears identical to the system login screen. An un-suspecting person attempts to login at the terminal, and the false login program accepts the login ID, and prompts for the password. The password is entered, and the program displays a phony error message, such as "Invalid Password." The false login program now has the ID and password, so almost anything can happen next, depending on the nature of the system. Files can be destroyed, modified, or stolen. The ID and password can be stored for later use.

Most microcomputers do nothing to prevent the installation of a false login program. As a defensive measure, the computer can be cycled off and on before every login, if there is any possibility that someone has had access to the machine. However, in many microcomputers it is possible to include the false login program in the start-up procedure. For example, in an IBM or compatible PC using DOS, the program can be invoked by the AUTOEXEC.BAT file.

Denial of Service

The last form of malicious act we consider is denial of service. We will not elaborate on active, overt activities such as electronic jamming and cutting communication or electric power lines. These are a problem for military organizations but these attacks are readily detected and most offices rely on law enforcement for protection against the most overt, destructive attacks.

We instead consider passive or covert activities that are more difficult to detect. A communication network can be attacked by occasionally altering messages. The altered messages never reach their destination or they arrive in unusable form. The communication network, therefore, has diminished capacity for valid traffic.

Other computer resources can also be denied. For example, all of the disk space can be filled with useless information, or the CPU can be kept busy with unproductive processing. The goal of this is to use up all of the computer resources with useless information so that the system cannot be used as intended.

Unintended Mishaps

Even in the most congenial environment, where no one would commit a malicious act, there is the danger of unintended mishaps.

These events share many of the same damaging effects as malicious acts: modified or destroyed information and denial of service. Many safeguards provide protection against both kinds of threats.

Unintended mishaps can cause hardware failures and accidental damage to magnetic disks or tapes. Computer components can simply wear out or a harmful event can damage them. Lightning and static electricity can destroy electronic components. Loss of electrical power erases the information in a computer's memory. A person can carelessly or unwittingly put a magnetic tape or diskette near a magnet, causing a loss of information. A disk drive has a delicate magnetic head that is moved by an electric motor. A "head crash" is a collision of the head and the disk, causing damage to one or both of them. This can result in the loss of all information on a fixed disk. Dirt can damage diskettes and disk drives. LAN cables are relatively durable but it is possible to break either a cable or a cable connector. Buried underground cables are particularly vulnerable to any digging. More catastrophic damage can be caused by fire, explosion, flood, or storm.

Operator error can unintentionally modify or delete information that is either in main memory or in storage. For example, person can delete the wrong file or overwrite a valuable file. Also, a person can forget to save information to disk before closing a file.

Threat Assessment

All organizations face similar risks regarding unintended mishaps. Most of these risks are well-known and there are readily-available safeguards to protect against them. These will be discussed in more detail later. We turn first to assessing the threat of malicious acts.

Malicious Acts

The threat of malicious acts varies widely, depending on the nature of the organization. What information is stored on the system? What would be the cost if the information were lost or stolen? How great is the motivation for espionage and sabotage? What resources are available to those who wish to do harm to the OIS? Where is the OIS vulnerable? These questions must be asked and answered. The level of effort spent on information protection should be commensurate with the threat. It would be foolish to commit great resources to information protection if the threat is low. Conversely, it would be foolish to leave the OIS relatively unprotected if the threat is great.

The greatest threats are aimed at government organizations responsible for diplomacy, law enforcement, and defense. This is because they have information that has life-and-death importance and compromise of this information can influence the outcome of international negotiations and war. A foreign state can apply vast resources for espionage and sabotage, and they have strong motivation to do so. Military and defense organizations are well aware of these threats, and they will not be discussed further here.

Next to political and military motivation, the greatest motivation is probably money. Electronic funds transfer is normally done by mainframe computers, not by an OIS, so that is beyond the scope of this article. An OIS may be used for payroll, accounts payable, and accounts receivable in a small business. An OIS may also handle product designs and planning information that could give a financial advantage to a customer or competitor.

Industrial and commercial corporations and other government agencies also have large financial assets. In addition, they have OISs containing valuable information. Some of this information would be valuable to competitors and some of it is personal information on customers, clients, and employees.

The organization has an obligation to individuals to protect personal information such as salaries, financial assets, tax information, telephone numbers, addresses, dependents, academic records, credit reports, and performance reports. In some cases, disclosure of information would violate the law. In most cases, disclosure would tarnish the image of the organization and destroy trust in it.

Information protection safeguards can be expensive and they can cause inconvenience to office workers. An organization must weigh this expense and inconvenience against the potential for harm if information is lost, modified, or stolen.

Unintended Mishaps

The threat of malicious acts depends on the nature of the organization's business. The threat of unintended mishaps depends on the reliability of the OIS software and hardware, the physical nature of

the office environment, and the skill of the office workers.

Some OIS programs automatically save information to non-volatile memory (disk) at frequent time intervals. Most programs prompt the user to save information before a file is closed. Programs can also warn the user before writing over an existing file. These features help reduce the likelihood of operator error. Most hardware used for OIS is highly reliable, but fixed disks have delicate moving parts that vary in reliability.

Many office buildings are well-built and provide excellent protection against fire, storms, and flood, but problems can still exist. If there is sprinkler system or other fire extinguisher systems, the OIS could be exposed to damage from water or chemicals. If an OIS is installed in an industrial environment, there can be dangers of dust, corrosive fumes, and vibration.

The danger of operator error depends largely on the skill and experience of the workers. Novices have no idea how quickly and permanently they can destroy information. Conversely, workers who have some experience with computer systems are sensitive to the need to frequently save their work to disk and to regularly back-up their disks.

Information Protection Guidelines and Recommendations

Information protection encompasses all of the measures taken to safeguard the information system. It requires a combination of threat assessment, safeguards, and policies. A threat assessment will identify risks and determine how much effort is needed to safeguard information. Then, a combination of safeguards and policies is needed to protect information.

Several information protection guidelines are suggested below that should help protect an OIS. It is important to note that these are merely guidelines and each OIS installation must implement a combination of these and other safeguards to protect information.

Goals of Information Protection

Information protection has two goals. The first is to preserve the availability of information and other computer resources for legitimate uses (i.e., to make sure that the OIS can be used as intended to contribute to the objectives of the organization). The second goal is to prevent unauthorized access to information and other computer resources, particularly when such access will adversely affect the objectives of the organization.

Establish Policies to Support Mechanisms

Successful information protection requires a combination of physical and software safeguards together with policies and effective management to correctly implement these safeguards. For example, it does no good to install a lock if there is no policy requiring it to be locked at appropriate times or if there is no management to monitor the safeguarding procedure.

There are commercial programs designed to detect viruses. They can detect certain specific viruses and certain classes of viruses, but they should not be relied upon completely because it is usually possible to design a virus that is not detected. There is constant competition between those who create viruses and those who create virus protection programs.

The best way to defend against viruses is to use only software that is known to be free of viruses. Do not copy software from a home computer to an office computer, and do not use software from public bulletin boards. If there is any doubt about the source of a program, it should be tested on a single system before putting it on a computer connected to the LAN.

In an office, there are usually some workers who are determined to use their favorite software. If the office does not provide the software from a reliable commercial source, these workers will provide their own copies. This is a good way to infect a system with a virus. The best way to prevent this in a LAN environment is to provide employees with microcomputers that do not have a diskette drive. Only the LAN server requires a diskette drive. The LAN server can be physically controlled so only the administrator has access to it. This prevents others from putting infected software on the system.

Most of the preceding discussion on viruses applies to Trojan Horse programs. Again, the most effective defense is to avoid unreliable sources of software. Could the software provider benefit from a Trojan Horse attack? If the answer is yes, find another source or thoroughly test the software before using it on real data.

Cryptography and Authentication

Office tasks involve a large volume of data exchange. (The term data here refers to both *raw* and *processed* data.) Both local and wide area networks are often used for exchange or transmission of data. While one aspect of securing office data is to prevent unauthorized access to files in the computer, another aspect is protecting data that is being transmitted. The purpose of *encryption* is to make data which is being transmitted unintelligible to eavesdropper.

Conceptually, encryption works as shown in Figure 1. Office data to be transmitted is represented by *DATA*. The sender converts *DATA* into encrypted form, *DATA'*, and the receiver converts *DATA'* back to *DATA*: Both sender and receiver must have an agreed upon *key*, *K*, for encryption and *decryption* purposes. Two functions are required: *EK* and *DK*, where the latter is the inverse of the former. *EK* converts *DATA* into encrypted form *DATA'* using *K* while *DK* recovers *DATA*.

Effective encryption will render the information meaningless to anyone who does not have the key. This will prevent browsing and theft. It also will prevent unauthorized modification where the meaning is changed but not destroyed. Encryption can be applied to both stored information and information being transmitted on a network.

History is full of examples of encryption schemes that have been broken. In fact, only one encryption scheme devised before 1970 is still unbroken. This should provide ample warning against using any ad hoc encryption method when better alternatives exist. The Data Encryption Standard is extremely difficult to break, is available in commercial products, and is adequate for most OIS applications.

Backups

Backups provide a high level of protection against many forms of malicious acts and unintended mishaps. There are two important forms of backup. First, it is important to frequently copy information from computer memory to non-volatile storage, e.g., a fixed disk. Some word processors and database management systems automatically copy information to disk at frequent intervals. Other programs only save information when the user requests it. Frequent backups will minimize the damage when a power failure, operator error, or other malfunction causes the loss of computer memory.

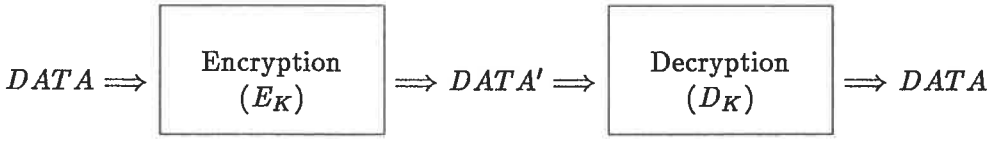
The second form of backup is to copy information from fixed disk to diskettes or tape. If information on a fixed disk is destroyed by a virus, Trojan Horse, some other malicious act or operator error, the most recent backup copy can be restored.

Security Software with Passwords

The common operating systems for IBM PC and compatibles and the MacIntosh do not offer password protection. Physical access to the machine gives access to the programs and information on the machine. On the other hand, systems like Unix and LAN software require the user to enter a login identification and password before access is given to any software or information.

Passwords are useless if they are not protected. Any written record of passwords must be stored in a safe. Passwords should be random sequences of letters and numbers. Words and proper nouns

Figure 1
Abstract Representation of Encryption/Decryption



are too easily guessed and provide little protection against a sophisticated intruder. Physical access to the server must be limited to the administrator to prevent someone from bypassing the security features.

Physical Safeguards

Physical safeguards protect against illegal intrusion by people and physical hazards such as fire, power failure, and voltage spikes.

Intrusion alarms and locks prevent outsiders from having access to the OIS equipment. Diskettes and tape backups can be stored in a safe or other locked enclosure, depending on the level of protection that is desired.

LAN workstations that do not have a diskette drive are becoming more popular today. This is due in part because of the cost savings, but these workstations also make it impossible for a well-intentioned employee to introduce a virus by running a program that came from an unreliable source. It also eliminates one way of copying information onto diskettes to steal it. In some cases, it is necessary to arrange the office equipment so visitors cannot view the computer monitors. This is important if the monitors display information that should be protected or if displayed information would give a visitor some insight into how to attack the system.

Fire can totally destroy all information as well as the expensive computer equipment, so the office should be equipped with fire detectors and Halon fire extinguishers. These fire extinguishers use a gas that does not harm computer equipment.

Power failures and voltage spikes can erase volatile computer memory and damage computer components. An Uninterruptible Power Supply (UPS) with voltage spike suppression gives the best protection against these hazards. A cheaper alternative is a voltage spike suppression device alone. This may be sufficient if frequent backups are made and the loss of some information is tolerable. Even a good voltage spike suppressor will not protect from a direct lightning strike, so it is a good precaution to turn off computer equipment during a thunderstorm.

Once again we repeat that successful physical protection requires a combination of physical safeguards together with policies and effective management to correctly implement and monitor these safeguards. For example, it does no good to have a policy for safeguarding against illegal intrusion without having an effective procedure for implementing it and a management to monitoring it regularly.

Discussions and Conclusions

In this paper, we attempted to show that the provisions of information protection in an automated office environment is different from that found in traditional office environments. We discussed several areas of security concerns in an office environment to support this argument.

We further attempted to outline some guidelines to prevent and/or solve some of the office information protection problems. Although a large variety of possible security measures have been proposed for various computing systems (e.g., databases, operating systems), these measurements in most cases cannot be directly applied to an automated office environment. The office systems managers thus have to realize that they must tailor a security program which best reflects their security requirements.

It may be a long time before attaining a secure office information system status in an organization. Internal needs and reviews have to be developed to identify and assess problem areas and management dedication in both spirit and pocketbooks are needed. Managers must consider questions like "how much money are we willing to allocate towards security measures?" and "what is our current security level, and is that adequate?" (Bakst, 1990). It is interesting to note that according to Farhoomand & Murphy (1989), in a survey of Fortune 500 companies with average MIS budget of approximately $20 million, over half allocated less than 0.5 percent to security!

A completely secure system or model may never exist for an office environment. The best that can be achieved is to obtain an acceptable level of security and to proceed with the understanding that new threats will always develop.

References

Arn, J. (1988). *Office automation: An information systems approach.* Boston, MA: Boyd & Fraser.

Bakst, S. (1990, June). Beware of potholes on the path to PC security. *The Office*, pp. 44-47.

Barcomb, D. (1989). *Office automation: A survey of tools and technology*. (2nd ed.) Bedford, MA: Digital Press.

Denning, P. J. (Ed.). (1990). *Computers Under Attack: Intruders, Worms, and Viruses*. Reading, MA: Addison-Wesley.

Farhoomand, A.& Murphy, M. (1989, January). Managing computer security. *Datamation*, pp. 67-71.

Reynolds, J. (1991). The helminthiasis of the Internet. *Computer Networks and ISDN Systems*, 22(5), 347-361.

Tsichritzis, D. (Ed.). (1985). *Office Automation*. New York, NY: Springer-Verlag.

Vaughn, R., Saiedian, H. & Unger, E. (1993). A survey of security issues in office computation and the application of secure computing models to office systems. *Computers and Security, 12*(1).

Woo, C. & Lochovsky, F. (1986). Supporting distributed office problem solving in organizations. *ACM Trans. on Office Information Systems, 4*(3), 185-204.