1994

Microcomputer security

American Institute of Certified Public Accountants. Information Technology Division

INFORMATION TECHNOLOGY DIVISION

Microcomputer Security

PRACTICE AID

AICPA
American Institute of Certified Public Accountants

Notice to Readers

This practice aid is one of a series of aids that provide accounting professionals with information about the implementation of a particular technology. These aids are issued by the AICPA Information Technology Division for the benefit of Information Technology Section Members. This aid does not establish standards or preferred practice; it represents the opinion of the author and does not necessarily reflect the policies of the AICPA or the Information Technology Division.

The Information Technology Division expresses its appreciation to Trevor J. Williams of Clark Whitehill, London, England, for the use of the material in the publication *PC Security*, ©1993, and the AICPA Management Consulting Services Division for the use of the material in their publication *Microcomputer Security*, ©1990.

Various members of the 1992–1993 AICPA Information Technology Executive Committee were involved in the preparation of this technology bulletin. The members of the committee are listed below.

Michael W. Harnish, *Chairman*
Steven W. Bare
L. Gary Boomer
Terry L. Campbell
David J. Duray
Philip H. Friedlander
Donald W. Hunt
James C. Kinard
Christopher J. Leach
Robert R. Moeller
Amy Chen Pierce
William L. Reeb
Philip J. Scissors
Larry J. Wolfe
Robert C. Wynne

Richard D. Walker, *Director*
Information Technology Division

Nancy A. Cohen, *Technical Manager*
Information Technology Membership Section

INFORMATION TECHNOLOGY DIVISION

Microcomputer Security

PRACTICE AID

AICPA
American Institute of Certified Public Accountants

1 2 3 4 5 6 7 8 9 0 IT 9 9 8 7 6 5 4

Library of Congress Cataloging-in-Publication Data
Microcomputer security/Information Technology Division.
p. cm.
ISBN 0–87051–148–3
1. Microcomputers— Access control. I. American Institute of Certified Public Accountants. Information Technology Division.
QA76.9.A25M55 1994
005.8—dc20 94–2017
CIP

Table of Contents

Chapter 1. Introduction

How do you keep data on a microcomputer secure? What are the risks and what is the best way to control them?

Although business computers were once considered personal computers, useful for little more than small word processing or clerical applications, now, whether freestanding or connected to others in a local area network (LAN), they are used to manage the information and data for significant areas of many organizations. The rapid growth of network systems and the widespread use of notebook and portable computers have made large volumes of confidential data easy to access and difficult to secure.

This practice aid considers a number of common problems of microcomputer security. Security concerns differ from user to user. In some instances, the system and data may be so unimportant that no security is required. At the other extreme, an organization may be so dependent on the microcomputer system, or its data may be so vital, that disclosure of the data could ruin the business. With the growing trend away from centralized computer systems to microcomputer-based LANs, organizations are increasingly dependent upon the information contained in their systems.

In addition to a general discussion of microcomputer security risks, this practice aid considers the different types of security measures available, from the simple, such as locking away diskettes—to sophisticated access controls and encryption.

Scope of This Practice Aid

Security has always been a concern in business. A key responsibility of management is to safeguard the assets of the business, which include computerized accounting records and other information. If computerized data are lost and unrecoverable, changed by unauthorized persons, or stolen and used by a competitor, the business is at risk of financial loss.

The hard and soft costs of electronic data processing (EDP) resources are significant. Hard costs include the purchase prices of microcomputers, network communication devices, and various peripheral devices such as printers, tape drives, or scanners. Soft costs include those associated with training personnel, implementing the system, and developing backup and recovery procedures.

Microcomputers perform a variety of functions, some of which were previously performed exclusively on minicomputers and mainframes or on dedicated computing equipment, such as word processors and computer-aided design/computer-aided manufacturing (CAD/CAM) equipment. One result of this shift is a decentralization of information processing and dispersion of an organization's EDP resources from a highly centralized primary computer system, controlled by an information systems department, to a highly distributed, end-user-controlled microcomputer environment. Although these microcomputers offer a flexible processing environment, they pose potential problems for a business's traditional control systems, which management usually oversees within a normal organizational structure. The functions performed on these microcomputers may not be integrated into the company's internal control structure. Additionally, microcomputers may increase rather than decrease the concentration of duties within a functional area, making control procedures more difficult to implement. Consequently, microcomputer security is a concern to all businesses.

This practice aid provides practitioners with an overview of microcomputer security. It may also help practitioners and members in industry to better understand the work of computer security specialists and to develop policies and procedures for internal operations involving microcomputer resources. The exhibits in appendix A that appear at the back of this practice aid may be of assistance in reviewing an organization's security. This practice aid focuses solely on *microcomputer* security. Although there may be some similarities in security issues for microcomputers and larger, more traditional computer systems, the microcomputer introduces a special set of security problems to business management and the practitioner. These problems are presented here as they relate to the single-user microcomputer, microcomputers in a LAN, and microcomputers communicating with other microcomputers or larger scale processing systems.

This practice aid does not address the issues involved or the methods by which security may be studied and evaluated when an audit of financial statements is being performed in accordance with generally accepted auditing standards (GAAS).

Portable Computers: A Gift to the Thief

Portable computers are perhaps the most vulnerable of microcomputer devices. Once devices about the size of a briefcase that could be lugged from place to place, these machines have shrunk to a truly portable size. Today, portable computers may take the form of laptops, notebooks, or even hand-held processors not much larger than a videocassette. Because of their small size, these highly portable computers can be left on trains, left behind during vacations, stolen during burglaries, and taken from cars. More commonly, they are left in open office areas without being switched off or locked up. Portable computers may contain business plans, analyses of operating results, and confidential reports. They should be kept secure to prevent unauthorized persons from gaining access to the data contained in them.

Many of the security measures used for more traditional computer systems are not practicable on portable computers. For example, depending on the operating system, traditional network password protection may not operate on the hard disk of a computer that is not attached to the network. Other hardware security devices such as disk-drive locks and key-card access prevention devices often will not fit onto a notebook or portable and would be impractical even if they could.

Microcomputer Networks

Although the easy access afforded by LANs makes them attractive to end users, this system's connectivity can cause security risks. If the network also has communication links to remote sites or dial-in facilities, the security problem is exacerbated.

At the heart of every traditional LAN configuration is a specialized computer called a file server. This file server contains all the programs and data files needed by most users. A spreadsheet program and all individual user files, for example, might be located on one file server. If the program files for that spreadsheet software were to be corrupted, no one on the entire network could use the spreadsheet software. If an executable file from this spreadsheet system were to become corrupted with a virus, anyone running that spreadsheet on the network would contract the virus program.

Chapter 2. The Root of Microcomputer Security Problems

Users who do not appreciate the potential for data loss can cause significant microcomputer security problems. Valuable information and data files are often stored on a number of microcomputers throughout an organization, and users may be unaware of or lackadaisical about the need for control over that data.

The lack of file protection is another significant security exposure common in microcomputer operating systems. Although some more current operating systems offer limited file protection and control over the manipulation and deletion of files, significant damage can occur simply because an operating system does not use adequate file protection procedures. For example, in an MS-DOS environment, one *delete* command can erase huge amounts of data in one fell swoop, without so much as the message, *Are you sure you want to delete this file?*

A thriving sector of the software industry—manufacturers offering add-on security packages—has developed to reduce exposure to microcomputer operating system security risk. However, purchasing and implementing a security package is not enough.

The concept of *total* security is important. A well-implemented log-on system may be rendered useless if backup tapes of sensitive data are left in unlocked rooms. An organization must develop a series of specific action points to improve its microcomputer security:

- Set a security policy.
- Identify what needs to be kept secure and consider the threats.
- Determine the needed physical security.
- Decide on the level of logical access control that is required.
- Educate users in security risks and what procedures they must observe.
- Implement security procedures.
- Monitor the effectiveness of the procedures.

The number of microcomputers connected to centralized computer systems, either directly or through LANs, has grown enormously. The microcomputer has thus become the ideal platform for infiltration into these centralized systems. For example, many organizations preprogram their mainframe access log-on sequences into microcomputers for *one-touch* log-on. Although this simplifies access for the individual microcomputer user, unauthorized persons could access that log-on menu to gain access to the mainframe system.

Microcomputer Security Risks

Risk can be evaluated as the likelihood of loss and the seriousness of the problem if loss or damage occurs. The problem may be a breach of confidentiality, loss of commercial secrets, or a concern of simple operational logistics. Although microcomputers themselves are relatively inexpensive, the data on them may be significantly more valuable. The likelihood of loss depends on what threats there are to the system and its data, as well as the existing controls to provide a degree of protection. The following are some common threats:

Accidents

Accidents represent a very common threat. Data loss can result from many areas within a system, such as disk failure, faulty hardware, or corrupt software. However, in most cases the loss is an accidental result of data files being overwritten or removed. Even experienced programmers overwrite data files by mistake, since microcomputer operating systems will, in many cases, overwrite a file without informing the user.

Casual Threats

People may casually browse through the system and possibly cause damage or see private information. Leaving data files lying around is as much a computer problem as it is one with manual files. This kind of negligence is common in the microcomputer environment, where users frequently borrow others' machines or leave their own equipment running overnight without password protection.

Viruses

The initial panic over computer viruses has now dissipated into a rather more realistic outlook. However, the threat should still not be underestimated and antivirus policies and measures should be in place.

Hackers

A hacker is someone who improperly accesses computer systems. Hackers have a variety of motives for hacking, from the challenge of penetrating a password-based system to malicious or criminal purposes. Hackers can be disaffected employees trying to cause damage or just people pursuing a misdirected leisure activity. It is important not to underestimate the technical ability of hackers.

Measures of Protection

A number of security measures can be taken. Some may require that additional security software be purchased. Each of the following measures combats one or more security risks.

Physical Security

Physical security controls prevent unauthorized persons from gaining physical access to computer systems and their data. This basic security control can be very effective. For example, extensive password and encryption controls may not be as secure as simply keeping the information on removable diskettes, which can be locked in a safe. Locking away the sensitive data and the computer system reduces the threat that unauthorized persons will copy or see the information. Of course, there is still a security risk if "secret" copies are taken while the data are being used.

There are several aspects of physical security to consider: the location of the computers, the power supply to the computers, access to the equipment, and fire risk.

If a building's physical security is adequate, its microcomputers may be considered safe from threats by outsiders. However, microcomputer systems are often exposed to the risk of improper access from persons inside the organization. If the system and its files contain confidential data, it is advisable to lock the room where it is kept.

Microcomputer use has proliferated dramatically in recent years, yet the simplest and most obvious physical security procedures are often overlooked. The basics of physical security are as follows.

- Notebook computers should not be stored in cars.
- Equipment should be clearly labeled with non-removable tags.
- Individuals should keep portable equipment as carry-on baggage.
- The room in which the microcomputer is stored when not in use should be locked.

Most desktop machines can easily be secured with their own supplied locks and keys. Some computers have locks which also secure the case, which is an additional and useful form of security. Locks can even be installed on the floppy disk drive, physically preventing a user from inserting a diskette without the key and stopping the perpetrator from booting up from a diskette containing an operating system copy. This last measure is particularly effective in a network environment.

Microcomputer power supply is often overlooked. However, the proper flow of constant power is as essential to microcomputer operations as it is in a mainframe or minicomputer environment. More and more companies are now using battery-backed regulated power supplies for file servers and other critical personal computers.

In some geographical areas of the world, main sources of electric power can suddenly *spike* or surge, resulting in the loss or corruption of data on a microcomputer system. A regulated power supply will help to control this problem. Reliable surge protectors are now inexpensive, small, and readily available. These devices are useful even in areas with a stable electricity supply, if the computer is installed in or near a factory or workshop where high levels of power may be drawn at irregular intervals.

Having a power supply with a battery backup and warning alarm will allow the user to save all current data in the event of a power outage. Some notebook computers have built-in batteries. If accidentally disconnected from the external power supply, the computer automatically reverts to its battery.

Although office buildings should have fire detection and prevention equipment, it is often worthwhile to take additional measures with microcomputers by installing smoke detectors and suitable extinguishers. Halon-type extinguishers are recommended for computer equipment, but their use may be regulated by local environmental ordinances. Backup copies of all operating systems, whether on backup cassettes or diskettes, should be kept in fireproof safes. This also affords security against unauthorized access. Sensitive or irreplaceable data should always be backed up at least *twice*, and the backups should be stored in different places.

Managerial Controls

The integrity of applications and executable files is extremely important. The following risks must be prevented:

- Users may put their own, possibly pirated, software onto organization microcomputer equipment.
- Users can delete application programs or files that are needed for the effective operation of application programs.
- Users can modify application programs.

It is extremely important to prohibit users from loading their own software onto the business organization's microcomputer, for reasons both of piracy and virus protection. Copied software is often illegal software, unless it is *freeware* or a demonstration disk whose publisher has expressly permitted copying. The Software Publishers Association (SPA) is an organization which, in addition to its other functions, enforces copyrights of member companies' proprietary programs. When the SPA receives evidence of the use of pirated software, it will investigate and, if necessary, take legal action against unlicensed users. In a number of major organizations, the SPA has found hundreds of pirated programs, resulting in significant fines and embarrassment for the guilty parties. Management often has no idea how much illegal software exists within their organization. A systematic software license *internal audit* is recommended to reduce exposure to civil and criminal prosecution.

Copied software also introduces the very real likelihood of a virus. Each time a diskette is read by the disk drive, a virus can reproduce. Therefore, all diskettes (whether data files or applications) should first be scanned for known viruses. For further details on virus protection, see the AICPA Information Technology Section's *Technology Alert* on viruses, reprinted in appendix B of this aid.

Boot or Switch-On Security

Microcomputers are at their most vulnerable at the moment they are turned on. If security is to be effective it must be established at this time. A microcomputer should boot up into its security system and the user should not be allowed to use *any* part of the system at all until some initial identification is entered.

Effective switch-on security should prevent booting from a diskette. Most new microcomputers can be configured with a switch-on password. Some new computers have three levels of passwords built in, with an optional key lock on the case. Obviously, in order for this type of security to remain effective, the fewest possible people should be given the password.

Initial boot security is often all-or-nothing and may be appropriate in some circumstances.

Access Rights

Some security systems simply have an initial boot password used by everyone. This gives a measure of security but does not allow any distinction to be made among the various users and their access rights and does not allow any form of user identification logging. A better system involves some kind of log-on screen that allows the user to enter his or her personal identification, normally a user ID and a password. The classification of the user allows the security package in use to decide which applications and files the user may access. Sophisticated security systems will also determine how limited or broad a given user's access must be; whether, for example, an operator needs only to look at data in a file or be able to change that data. This feature is an integral part of operating systems such as UNIX and its variations.

Current versions of MS-DOS allow users to make files hidden or read-only, but these changes will affect *all* users, not just specific ones. Attribute changes in DOS can also be easily reversed by anyone with some knowledge of the operating system, since no password is involved. Some security packages come with menu systems that can be made to show different options to different users. In addition, the system can maintain a log showing who has logged on, for how long, and (if linked to a menu system) what they did. This useful management tool should be carefully reviewed and analyzed.

Additional security on networks can be obtained by protecting each networked microcomputer or node with its own boot security, such as a hardware card-swipe system.

User Authentication

Only those individuals authorized by management to use the system and its information should have access to it. Authorization can occur at four levels:

1. Operating system
2. Application system
3. Program
4. File

Access is usually controlled by a password. Depending upon the design of the supporting security software, a password can even limit access to one part of an application if that is all that is necessary. The microcomputer system specialist should assess the current password structure at each level, considering the following:

- How are the passwords managed? In a small operation, the owner may assign passwords; in a large business, a security manager or a system administrator may either assign passwords or ensure that users select and control their own passwords.
- What is the password structure? Are passwords at different system levels sufficiently unique? Are they shared in any manner? Are they changed periodically, either by the security manager or automatically by the system?

With more complex microcomputer installations, such as LANs, the operating system may use passwords to provide extensive security throughout the system. These passwords can regulate which hardware devices are available for use as well as the directories that may be entered. This procedure, however, is not limited to LANs. Even a single-user system can have a system monitor to determine who is using the system, which files and programs are being accessed, and when an activity occurs. The information can be reported periodically on an audit log. When such an audit log exists, an appropriate person, such as the system manager, should review the log on a regular basis and investigate any unusual entries.

A call-back approach is an appropriate security procedure for remote-system access to or from a microcomputer. It requires a callback to an authorized telephone number before allowing a user access at an off-site premises. Otherwise, either software security or manual measures must be developed to assure that only authorized users can access the system from remote locations. For especially sensitive situations, passwords can be combined with some form of hardware, such as an access card, to further identify a user. Even biometric security techniques, which identify a person based on fingerprint or retinal comparison, can be used. However, these techniques are costly and are not yet perfected.

Encryption of Data

Data security involves preventing information in disk files from being read by unauthorized people. To be effective in a microcomputer environment, data security almost invariably involves encryption of the files.

There are a few more modern methods of access restriction than encryption. The most common is to hide a directory from the DOS operating system. This stops access to all files in a directory and is a useful way to achieve security in low-to-medium security situations. Obviously, this type of security will not stop the determined hacker from access to data in the files.

In a number of security systems, the file allocation table—the record of what files exist and where they are located on the disk—is encrypted. These types of systems will not prevent someone familiar with a programming language, such as C or ASSEMBLER, from looking directly at information contained on the disk, although this is not an easy task.

Data encryption is the most popular form of data security and can be achieved in two basic manners:

- One encryption technique is known as the terminate-and-stay-resident (TSR) method. This involves having the encryption program remain resident in memory and automatically decipher the file when the user opens it, and encrypt it when the user writes it back to disk or copies it. The program normally knows which user it is addressing, and allows access to files accordingly. When TSR systems are in use, it is very worthwhile to make frequent backups of data, since it may not be possible to recover encrypted data in the event of system failure.
- The second way is to manually run a program that will encrypt or decipher a file. If the file is accessed while encrypted, the casual user will only see garbage data. This is a safer or slightly more reliable system than a TSR but provides more hassles, and also relies on users remembering to re-encrypt a data file every time it is used. The data is, of course, unencrypted when it is being used.

Data can be encrypted in a number of ways, but the methods can be roughly divided among three types of encryption algorithms:

- The Rivest-Shamir-Adleman (RSA) algorithm is considered the most secure, but only a few microcomputer packages use it. An encryption key is used to encrypt the file. Even if this encryption is known, the file cannot be deciphered, since a decryption key is also needed. Both these keys are based on prime numbers, and keys of reasonable length would produce a code that would take hundreds of years to decipher. However, with the advances in technology, mathematicians have recently deciphered the RSA algorithm. This will not cause a threat to an RSA scheme in general. By increasing the size of the prime number, the system will remain relatively secure.
- The Data Encryption Standard (DES) algorithm is the current industry standard for most packages and is very secure. It uses the same key for encryption and decryption, so knowledge of the key must be kept confidential. It is much easier to implement as a TSR program than is RSA. The DES algorithm is almost always used by the more sophisticated TSR microcomputer encryption programs.
- Most other algorithms used are proprietary, in that they have been developed by the software company for a particular package or range of their packages. These do not, in the main, involve keys chosen by the user. In some cases, the purchased software packages are given individual serial numbers, which are used by the encryption program. These packages are considered generally secure, but not as secure as DES or RSA.

Deletion of Files

If a file is deleted in a DOS environment, the file is not physically erased; the disk index to it is simply deleted. This means that various commercially available microcomputer utility packages can be used to retrieve the file and undelete it. A number of users are very grateful for this possibility. However, any files with confidential data should be physically *wiped* when finished. A utility to completely erase a file (sometimes called *super erase* or *file wipe*) is strongly recommended, since the File Delete command on microcomputers does not actually destroy information on the disk. An experienced user can then look directly at the disk and thus have access to deleted information.

Back Ups of Key Files

Backup procedures vary depending on the particular system involved. Factors to consider include the transaction volume, the frequency of data updates, and the company's need for historical record retention. Backup procedures for microcomputer systems may not seem necessary to the end user on a freestanding microcomputer system. Usually, such procedures are not considered until a need for recovery arises. However, computer security specialists should evaluate each system and recommend which backups will remain on-site and which will be kept off-site. In each case, the organization must secure the backup media in an appropriately rated container, able to withstand fire and extreme temperatures.

It is also important to determine to what extent the organization has tested its backup and recovery policies and procedures. A review of the testing approach and results will provide evidence of the organization's ability to recover from a disaster.

Sensitive items, such as password lists and copies of system and user documentation, should be kept secure and apart from day-to-day business areas. Policies to ensure continuity of operations include cross-training personnel in several functions and requiring specified vacation policies.

Regular data back up is extremely important. This is especially true when using TSR encryption programs, although the backup must also be secure. Even when users are editing a document or spreadsheet, they should be encouraged to perform file saves at regular intervals. Files should be backed up on diskette at the end of each session. It is also a good idea to back up the entire hard disk at least once a week onto cassette-based tape-streamer devices or similar backup systems. The security of these backup files is very important, since an entire system can reside on a few high-density tapes.

For important files, or files which reside only on diskette, it makes sense to have two backups. The separate physical storage of diskettes and tapes can be a logistical problem, but could prove worthwhile in the long run. Five-and-a quarter-inch diskettes are particularly susceptible to dust damage, and although three-and-a-half-inch floppies are slightly tougher, they too are vulnerable to rough treatment.

Chapter 3. What to Look for in a Microcomputer Security Package

Once security requirements have been evaluated, then an action plan needs to be formulated. This plan should include establishing a security policy, including some physical security measures and file backup procedures. In many cases, some form of boot access security will be required along with facilities to provide for the encryption of data. These measures will require the purchase of a security package. Which package is best depends on the unique security needs of each organization. Generally speaking, however, the higher the price of a package, the more features it offers.

Physical Devices

Most security systems rely on a password known only to the authorized user. However, many systems allow multiple incorrect access attempts and many users choose easy-to-remember names as passwords that can easily be guessed. In other instances, microcomputer users write down their passwords, leaving them in an easily discoverable location, or they may be observed by others as the keys are entered. To compensate for this password weakness, several systems use a hardware device such as a card, a diskette, or a token that has to be read before access is allowed. Additionally, some systems disable floppy diskettes until after the password has been entered in order to prevent the computer being booted up from a diskette and circumventing the security system.

Screen Lock-Out

Users sometimes leave their machines switched on when they are away from their desks—during lunch or overnight. To protect from this potential problem, resident software packages are available that log off the computer after a set time period.

Multiple Users

Some microcomputers are normally used by one person, so a single password is adequate. However, where a computer is shared by a number of users, each perhaps using different packages or parts of a system, a more sophisticated security package is required. In this case, it is advantageous to employ the *user concept* of a security package. In this scheme, the system recognizes the person who is logging on by his or her user ID and a separate password. Each user would be assigned an ID based upon that users' name. For example, if the organization security administrator establishes a six-character user ID based upon the first initial and the first five characters of the user's last name, John Smith would have the user ID JSMITH and Mary Johnson would have MJOHNS. This system is made secure with passwords, known only to the individual users. To access the system, each would enter his or her user ID, followed by the password.

Although this type of system is more complicated to administer, much better control can be exercised. In particular, a user log can be kept and reviewed. This type of system should be combined with procedures for changing passwords at regular intervals. In more sophisticated systems, passwords will be required to change at specific time intervals.

Encryption

There are always risks that security systems can be bypassed and that data, whether on hard disk or on a backup floppy, can be read by another application or transferred to another computer for examination. Consequently, if a high level of security is required, all confidential files should be encrypted. As discussed previously, specific utilities are available to encrypt and decrypt files. While the file is in its unencrypted state, it is vulnerable, and it is better to have a system that decrypts and encrypts as the file is read into or saved from a particular application. This type of system always needs testing because all applications may not work with all security packages.

Menu System

Some security packages are combined with a menu system. As well as making things easier for the user, these systems can have separate menus for each user just showing the available options at his or her security level. A more detailed log of what users have been doing can also be maintained.

Chapter 4. Other Security Software Considerations

As well as choosing an appropriate microcomputer security package that offers the appropriate features, the individuals selecting security software should also take into account the following:

Installation and Maintenance

Is the software easy to install and maintain? Has a simple installation routine been included with the package? Can the parameters and settings of the package be changed easily?

Ease of Use

How is the system presented to the user? The system must always be easy to follow, especially when running through menu systems. Ambiguities in menu options can lead to unintended features being used; for example, a file could be erased by mistake.

User Documentation

Are the manuals easy to follow? Particularly with security packages, it is important for manuals to be precise and usable. Chatty manuals can cloud important issues and confuse the user. Conversely, highly technical manuals are also difficult to read.

User Segregation

The features of the package that isolate one user from the next should be examined if the microcomputer is likely to be used by many users regularly. Some packages can stop individual file access while others will only prevent access to directories.

The Audit Trail

This feature records user IDs and log-on and log-off times. More sophisticated packages will record the times and the specific applications accessed.

Virus Protection

Better packages have some form of virus prevention, which will often check for unauthorized disk reads and writes, or for boot sector data. However, the sophistication of virus programs tends to increase with the sophistication of the programs used to detect viruses. For increased security, a good stand-alone virus detection package should also be used. Upgrades of this package should be installed as they are released.

Invisibility

This is the extent to which the package can be ignored in normal use. Some packages will encrypt and decipher files as they are opened or written to disk. TSR systems offer this encryption "on the fly."

Upgrade Ability

Can the package be upgraded? This upgrade could be to a more secure software version, to a hardware identification version (for example, key-cards or tokens in addition to standard password and user ID), or to a complete hardware system.

Compatibility

Care must be taken to ensure the package will work alongside the operating system in use. Many packages now state that they are compatible above a specific DOS version.

Chapter 5. Conclusion

There is no one solution, even in general topics, to any particular security problem. The more thought that goes into the security system, the fewer loopholes will exist. However, there will always be loopholes in any security system, and the main objective must always be the minimization of risk.

It is important that a specific security policy is created by management in conjunction with computer technical staff. Proper procedures for computer security must be constructed and observed. Ongoing reviews and checks are critical to any system, since initial good intentions are often forgotten as work builds.

Simply purchasing a security package is not enough. It has to be implemented, and this requires administration and discipline. The higher the level of security required, the more administration, discipline, and cost is involved. However, the cost of being insecure is probably greater.

Appendix A. The Assessment of Security

Exhibit 1
Hardware and Software Checklist

1. Name of Company _____
   a. Division names or locations _____
   b. Location of EDP, if any _____
      Senior EDP representative _____
   c. Attach a corporate and EDP organizational chart.

2. Equipment Configuration(s)

Description	Quantity	Manufacturer	Model	Communications*	LAN*	Location
File Server						
CPU						
Memory Size						
Disk Size						
Tape Backup						

Where a LAN is used, describe the topology scheme. Provide a diagram of the equipment used, including wiring paths, terminals, printers, communication interfaces, and so on.

Personal Computers						
CPU						

Describe the general characteristics of each workstation in use in terms of memory size, disk capacity, and so on.

Printer						
Other						

3. Software

	Manufacturer	Name	Version
Operating system			
File server			
Workstation			
Application systems			
Spreadsheet			

(continued)

*Answer yes if communications and/or LAN apply.

	Manufacturer	Name	Version
Database	_____	____	_____
Word processing	_____	____	_____
Accounting			
Application 1	_____	____	_____
Application 2	_____	____	_____
Application 3	_____	____	_____
Application 4	_____	____	_____
Telecommunications	_____	____	_____
Other	_____	____	_____

Provide diagrams of the applications used.

4. Remote Databases
   a. List all remote public and corporate databases used.
   b. Identify any internal databases (or other applications) that outside users may interact with via telecommunications.

Exhibit 2
Microcomputer Security Questionnaire

Organization and Administration

1. Give the full name and title of the person(s) within the organization responsible for general as well as microcomputer security. If a local area network (LAN) is used, who serves as the network security officer?
2. Obtain all documentation on policies regarding security of data processing activities. If an electronic data processing (EDP) department exists, describe its relationship to microcomputer use in the company. Does it set policies and procedures for microcomputer acquisition, use, and security?
3. Describe the extent of custom programming for microcomputer systems. Is such programming done internally or contracted out to a consulting group?
4. What policies exist, if any, for the acquisition of packaged software systems? Are there approval requirements for such purchases?
5. Is a contingency EDP plan in place? If not, is one justified based on the client circumstances?
6. Are copies of critical software, data files, templates, and documentation stored off-site or in another acceptable location?

Operations — Processing Procedures

1. For transaction-processing systems, describe the procedures for user authorization (by application) on workstations. Who is responsible for determining work assignments and monitoring assignment completion?
2. Describe the password authorization system for —
   a. File server access.
   b. Application access (by task within each application).
3. Determine specific measures taken to secure key data files (by application) from unauthorized modification.
4. Determine what utility software exists for a variety of functions, such as restoring data from lost files, master files, or transaction files.
5. Identify other applications exposure areas that warrant security treatment.

Operations — Nontransaction-Oriented Systems

1. Identify the other microcomputer-based applications that are not routinely processed, for example, spreadsheets, databases, and so on.
2. Describe the control procedures used to document, test, and retain these applications as a permanent record. Who is responsible for securing this information? Is off-site storage (separate from the end user) used?
3. Describe the password authorization procedures for these applications.

(continued)

Access Controls — Hardware

1. Is there a physical inventory of all equipment used (including serial numbers)?
2. Are manufacturer's security locks used? Are keys stored under an adequate control procedure?
3. If a LAN is used, is physical access to the file server adequately controlled?
4. Is the workstation equipment adequately secured? Is access to work areas adequately controlled?
5. Are diskettes and other magnetic media secured to prevent unauthorized use?

Access Controls — Other

1. What security procedures exist to prevent unauthorized access to telecommunications? Is the access restricted during nonbusiness hours?
2. Are activities automatically logged according to type, time, and initiator?
3. Describe existing backup and recovery procedures. Has the company tested these procedures?
4. Describe the process for changing security access to microcomputer systems after someone has been terminated.
5. Describe the policy for password rotation.

Appendix B. Technology Alert—Virus Update

January 1993

Virus Update

By Robert C. Wynne, CPA

The Michelangelo scare of over a year ago, for the first time made the general public and the small business community aware of viruses and their potential disastrous consequences to the data on their computer systems. Newspaper articles, especially from the *Wall Street Journal, NY Times,* and *USA Today* acted as public service announcements and focused management on addressing the problem of virus infection within even their smallest computer systems. Many companies purchased various anti-virus software programs to find out if they had been infected by the Michelangelo or any other virus that their new software package could find.

Several of my clients found out that their computers were infected. Their anti-virus programs remedied the problem and they suffered no data losses. This easy fix has caused a new problem. They now have become complacent about computer viruses and some have even stopped using routine safe computer practices. They feel that their outdated anti-virus programs are still keeping their computers safe from software viruses.

Our firm has continued to educate clients that the anti-virus software they purchased last year is no longer effective. The programs only know the older viruses that were identifiable when the software was issued. Clients have not updated these year-old programs. These are some of the same people that will immediately buy the latest update of their spreadsheet or word processing program, even if they are only using one tenth of the power of the old version, and have no idea if the new version has any applications they may need.

The National Computer Security Association and all major software houses that produce anti-virus programs continually inform us through our trade journals that approximately 3 new viruses are being created each day. These ingenious creative programmers with their destructive streak are not only from the United States. Many other countries are contributing, especially from Eastern Europe and Asia.

Many of the older viruses were relatively easy to find because they each had a unique identity similar to a fingerprint, that, even when modified by another programmer to make it slightly different, could be found by anti-virus software. There now exists a new form of virus which is called a polymorphic or changing virus. It doesn't leave an identifiable fingerprint. These viruses mutate and change their signatures with each infection. Most older programs bought specially for the Michelangelo virus have no way to identify these newer viruses. To make matters worse, there is a set of tools commonly called the Mutation Engine, available to anyone who wants to search just a little, to help develop these new viruses. Groove and Pogue are two of the first viruses to use the Mutation Engine. Groove is a memory resident infector of COM and EXE files, which displays a message at about 12:30 a.m. each day. Pogue infects files on execute and close, and on May 1 all day, or each day before 7 a.m., the system will generate noises

---

Robert Wynne is a partner in the accounting firm Salada, Wynne, Kling & Company, P.C. of Niagara Falls, New York. In this Alert he discusses his firm's experience with computer viruses.

Reprinted, Robert C. Wynne, "Technology Alert — Virus Update," AICPA, 1993.

from the computer's speaker. Another major new virus type is the stealth virus group. This type will tell the older type anti-virus programs that the infected programs are the same size and date as they were before they were infected. This means that client's computers may be infected but wait to do their damage unannounced by these older anti-virus programs until it is too late.

Some of the recommendations that we make to our clients to protect themselves from the ever growing number of computer viruses are as follows:

- Continue to practice safe computing. Nothing can replace being careful.
- Never introduce an untested floppy disk into your system. This includes new commercial programs as well as clients' disks. Also ask service technicians to be careful when working on your computers. Check these machines when the technicians are finished working using your newest anti-virus software.
- Always keep a bootable DOS disk (system disk) with all the drivers needed as well as your newest anti-virus software, write-protected and ready to check your computer on a routine basis. To create a system disk, type one of the following commands:

  For a formatted disk: sys a:
  While formatting: format a: /s

- Always protect your original disks after installing the programs on your hard drive. They will be available in case you need to reinstall.
- If you use commercial bulletin boards for other than reading E-mail, especially to download programs, be sure to check all the files downloaded with your latest anti-virus program before using them in your computer.
- Sign up for an anti-virus update service. They usually have an annual maintenance agreement and updates are scheduled at least quarterly, while some are even monthly. Several services have 24 hour Virus Faxlines for manual updating on new viruses that have been found between the BBS updates. Some even offer newsletters.

Recognized major anti-virus software vendors include:

McAfee Associates	1–408/988–3832
Symantec	1–800/428–6800
Central Point Software, Inc.	1–503/690–8090
Fifth Generation Systems	1–800/225–2775

Glossary

Application System

A specific task-oriented system comprising numerous programs (for example, general ledger and accounts payable).

Authentication

The process of determining if the user trying to enter a particular system, program, or other device is authorized to do so.

CAD/CAM (Computer-Aided Design/Computer-Aided Manufacturing)

Integration of computer-aided design with computer-controlled manufacturing.

Call-back Approach

An authenticating procedure used in telecommunications that calls back the user once a request is made to use a system. This ensures that the user is working on an authorized hardware device or is in an authorized physical location.

DES (Data Encryption Standard)

NIST-standard encryption technique that scrambles data into an unbreakable code for transmission over a public network. It uses a binary number as the key for an encryption that offers more than 72 quadrillion combinations.

Directory

A list of files (programs and data) stored on a hard or floppy disk.

Electronic Bulletin Board

Computer-based information, in the form of programs and files, that remote users can access via telecommunications.

Encryption

Using special algorithms to secure data (programs, data files, passwords) by scrambling it.

Executable Program

A program that is in machine-readable form.

File Server

A computer on a network that acts as a host to nodes on a LAN. The server handles file management, input/output control, and network security.

Freeware

Software distributed without charge. Ownership is retained by the developer who has control over its redistribution.

Hacker

A person who breaks a code and gains illegal entrance into a system.

Local Area Network (LAN)

A system of multiple, interconnected electronic devices.

Menu

User options, representing actions, that are displayed at the beginning of a program. Selecting a particular action initiates the next step in a program.

Microcomputer

A small standalone computer built around a microprocessor.

Minicomputer

A general-purpose computer similar to a mainframe computer in function, but with memory and speed between those of a microcomputer and a mainframe.

Network

A connection between two or more computers that allows information sharing.

Operating System

Software that controls the execution of programs and that may provide other system-management facilities, such as scheduling, input/output control, disk storage management, and related services.

Password

A key word or number code, known only to the authorized user, that permits access to programs and files.

RSA (Rivest-Shamir-Adleman)

A highly secure encryption method by RSA Data Security, Inc., that uses a two-part key. The private key is kept by the owner; the public key is published. Data is encrypted by using the owner's public key, which can only be decrypted by the owner's private key.

Spike

Also called a transient, a burst of extra voltage in a power line that lasts only a fraction of a second.

Surge

Oversupply of voltage from the power company that can last up to several seconds.

Surge Protector

A device that detects and corrects irregular electrical patterns to prevent damage to a computer.

System Administrator

The person responsible for maintaining the computer system, including hardware and software assignments, updates, and problems.

Telecommunications

The process of transmitting information between separate facilities by electrical, optical, or acoustical means.

Topology

The arrangement of pathways in a network (for example, rings, in which messages pass through stations, in turn; stars, in which messages pass through a central node; and buses, in which each message is presented to all nodes).

TSR (Terminate and Stay Resident)

Programs that remain in memory so that they can be instantly popped up over some other application by pressing a hot key.

Uninterruptible Power Supply (UPS)

A device that maintains an electrical current for a predetermined period of time. It allows continuing operations or sufficient time for the user to power down until normal electrical supplies are restored.

UNIX

A multiuser, multitasking operating system from AT&T. It runs on computers from micro to mainframe. UNIX is written in C, which can be compiled into many different machine languages, causing UNIX to run in a wider variety of hardware than any other control program.

Virus

An unauthorized program that enters a computer system and damages operating or application systems.

The Information Technology Section

IT Section Membership

The AICPA IT Section provides products and services which will allow you to keep pace with changes in technology and increase your competence in information technology. It will also offer advice that will help you provide information technology services in a more professional — and profitable — manner. Annual membership dues are $100. Section benefits include —

- Subscription to the IT Section's quarterly newsletter, *InfoTech Update,* with essential information on new developments in the ever-changing world of technology.
- Practice aids, technology bulletins, and research reports.
- At least four issues of *Technology Alerts* — one-page releases on up-to-the-minute topics.
- Vendor discounts on selected products and publications.
- Discounted registration to the annual Microcomputer Conference.

For more information on IT Section membership, please call Nancy Cohen at (212) 596-6010.

AICPA INFORMATION TECHNOLOGY PUBLICATIONS

IT Practice Aids Series
CPA Firm Technology Planning Guide
Image Processing and Optical Character Recognition — How They Work and How To Implement Them
Computer Disaster Recovery Planning Guide
Microcomputer Security

IT Technology Bulletins Series
Memory Management
Executive Information Systems

IT Research Reports Series
Audit and Security Issues With Expert Systems

Ready to join now? Send the completed application form to Nancy Cohen—Information Technology
American Institute of CPAs
1211 Avenue of the Americas
New York, NY 10036–8775

MEMBERSHIP APPLICATION FORM

AICPA INFORMATION TECHNOLOGY MEMBERSHIP SECTION

Please enroll me as a member in the AICPA Information Technology Membership Section through July 31. I understand that the $100.00* dues fee covers all membership benefits.

☐ **Payment enclosed** ☐ **Bill me**

Signature _____

Name _____

Firm _____

Address _____

City _____ **State** _____ **Zip** _____

Member Number _____

Business Telephone _____

CODE – PA: MS
(PA: MS)

***Dues will be prorated quarterly.**