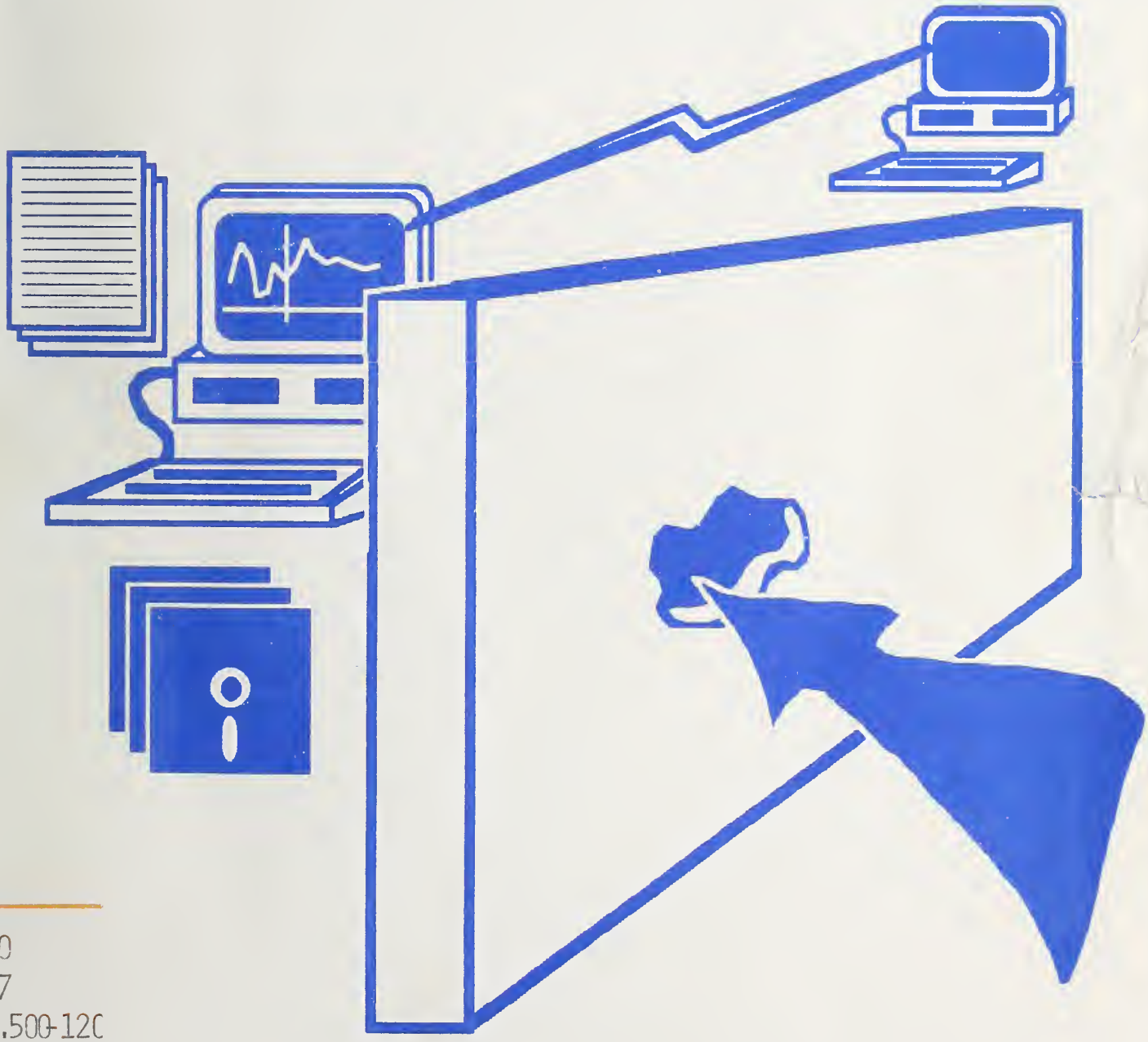
Computer Science and Technology

NBS Special Publication 500-120

Security of Personal Computer Systems: A Management Guide



The National Bureau of Standards[1] was established by an act of Congress on March 3, 1901. The Bureau's overall goal is to strengthen and advance the nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the Institute for Computer Sciences and Technology, and the Center for Materials Science.

The National Measurement Laboratory

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; and provides calibration services. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

The National Engineering Laboratory

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[2]

The Institute for Computer Sciences and Technology

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Institute consists of the following centers:

- Programming Science and Technology
- Computer Systems Engineering

The Center for Materials Science

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-country scientific themes such as nondestructive evaluation and phase diagram development; oversees Bureau-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Center consists of the following Divisions:

- Inorganic Materials
- Fracture and Deformation[3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3]Located at Boulder, CO, with some elements at Gaithersburg, MD.

Computer Science and Technology

NBS Special Publication 500-120

Security of Personal Computer Systems: A Management Guide

Dennis D. Steinauer

Center for Programming Science and Technology
Institute for Computer Sciences and Technology
National Bureau of Standards
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Malcolm Baldrige, Secretary

National Bureau of Standards
Ernest Ambler, Director
Issued January 1985

Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

Library of Congress Catalog Card Number: 84-601156
National Bureau of Standards Special Publication 500-120
Natl. Bur. Stand. (U.S.), Spec. Publ. 500-120, 66 pages (Jan. 1985)
CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1985

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

ABSTRACT

The use of personal computer systems (often called desktop or professional computers) in the office and home environment has placed increasingly powerful information system technology in the hands of growing numbers of users. While providing many benefits, the use of such small computer systems may introduce serious potential information security risks.

Although considerable progress has been made in security management and technology for large-scale centralized data processing systems, relatively little attention has been given to the protection of small systems. As a result, significant exposures may exist which can threaten the confidentiality, integrity, or availability of information resources associated with such systems. To ensure effective protection of these valuable resources, managers, system designers, and users must be aware of the vulnerabilities which exist and control measures which should be applied.

This report describes management and technical security considerations associated with the use of personal computer systems. The primary objective is to identify and discuss several areas of potential vulnerability and associated protective measures. The issues discussed include:

- Physical and environmental protection
- System and data access control
- Integrity of software and data
- Backup and contingency planning
- Auditability
- Communications protection

In addition, a general plan of action for the management of personal computer information security is presented. References to additional information, a self-audit checklist, and a guide to security products for personal computers are provided as appendices.

In general, the term "personal computer" refers to single-user systems. However, most of the discussion in this report applies equally to other types of microprocessor-based systems designed for use in a general office environment (e.g. word processors, workstations, and various types of office and home computer systems).

KEYWORDS: access control; auditability; backup; computer security; contingency planning; cryptology; microcomputers; office automation; personal computers; small computers

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

Designers and users of large automated data processing (ADP) systems have long been aware of the need to provide security and privacy for these systems. However, the number of such people who must worry about these matters has been relatively limited in the past. This situation has changed dramatically with the rapid introduction of personal computers (PCs) into the workplace. Now, literally millions of people are (or soon will be) using personal computers for either business or personal needs.

Along with the obvious benefits available through the use of personal computers, there are some significant dangers which are now being recognized. As more people begin to use PCs, it becomes vital that these dangers and the need for protection be understood. Both equipment and data must be protected, and the protection needs of each are different.

This document is intended to provide both managers and users of personal computers with an understanding of the information security threats involved in using such systems and approaches to reducing the associated risks. This section provides a description of the basic nature of the security problem with personal computers and a guide to the rest of the document.

1.1. BASIC SECURITY CONCERNS

Before discussing specific security considerations for personal computers, it will be useful to define the basic information security problem we are attempting to solve.

1.1.1. INFORMATION SECURITY OBJECTIVES

Regardless of the size or nature of an ADP system or application, the following major **security objectives** must be met:

- Confidentiality of personal, proprietary, or otherwise sensitive data handled by the system.
- Integrity and accuracy of data and the processes that handle the data.
- Availability of systems and the data or services they support.

If these objectives are met, then other assets that are involved with or dependent upon the information being protected will also be protected. For example, meeting these goals will, in general,

ensure that the physical equipment itself is protected from unauthorized access or damage.

1.1.2. THREATS

A wide range of accidental or intentional events can threaten information resources. These threats include the following:

- Environmental hazards
- Hardware and equipment failure
- Software failure
- Errors and omissions
- Disgruntled or dishonest personnel

The various manifestations of each type of threat are potentially endless and depend upon the specific characteristics of the system, data, and operational environment.

1.2. THE NATURE OF THE PC SECURITY PROBLEM

The preceding discussion of information security objectives and threats applies, in general, to systems of any size. Personal computers and other small systems, however, have unique security problems that must be understood if rational and effective security measures are to be implemented. The following is a general discussion of the nature of the security problem as it relates to personal computers.

Although personal computers provide essentially the same functionality as large systems (i.e. they permit the rapid manipulation and examination of large amounts of text and data), there are some characteristics that present special security problems. In general, the differences are the following areas:

- Physical accessibility
- Built-in security mechanisms
- Nature of data being handled
- Users

Each of these is discussed below.

1.2.1. PHYSICAL ACCESSIBILITY

Basic physical protection of a computer system is required to assure operational reliability and basic integrity of hardware and software. Other security mechanisms (e.g. those implemented in systems hardware and software) rely on this underlying level of protection.

A large-scale, multi-user computer system represents a sizable investment and is usually provided with considerable physical and environmental protection. The exposure of the system to damage or unauthorized access can, therefore, be limited. The cost of such protection is a relatively small proportion of the overall investment.

With personal computers, however, physical accessibility is not as easily controlled -- indeed, accessibility is inherent in the concept of a "personal" computer. It is seldom feasible to build a protective "shell" around an individual personal computer. This means that protection against damage, hardware modification, or unauthorized access is difficult to prevent. Since many technical security mechanisms (e.g. access control software and cryptographic routines) are often dependent on the integrity of the underlying hardware and software, these security mechanisms may no longer provide the intended degree of protection.

1.2.2. BUILT-IN SECURITY MECHANISMS

A second security problem with most personal computers is the lack of built-in hardware mechanisms needed to isolate users from sensitive, security-related, system functions. For example, the typical personal computer does not support the following important security mechanisms that have long been available on larger systems:

- Multiple processor states - enabling separate "domains" for users and system processes;
- Privileged instructions - limiting access to certain functions (e.g. reading and writing to disk) to trusted system processes; and
- Memory protection features - preventing unauthorized access to sensitive parts of the system.

Without such hardware features it is virtually impossible to prevent user programs from accessing or modifying parts of the operating system and thereby circumventing any intended security mechanisms.

Figure 1-1 illustrates many of the internal interfaces that exist within a personal computer system. Effective security within the computer itself requires that the paths by which users may access data and system functions be limited and tightly controlled. The hardware mechanisms described above are designed to limit and control these paths.

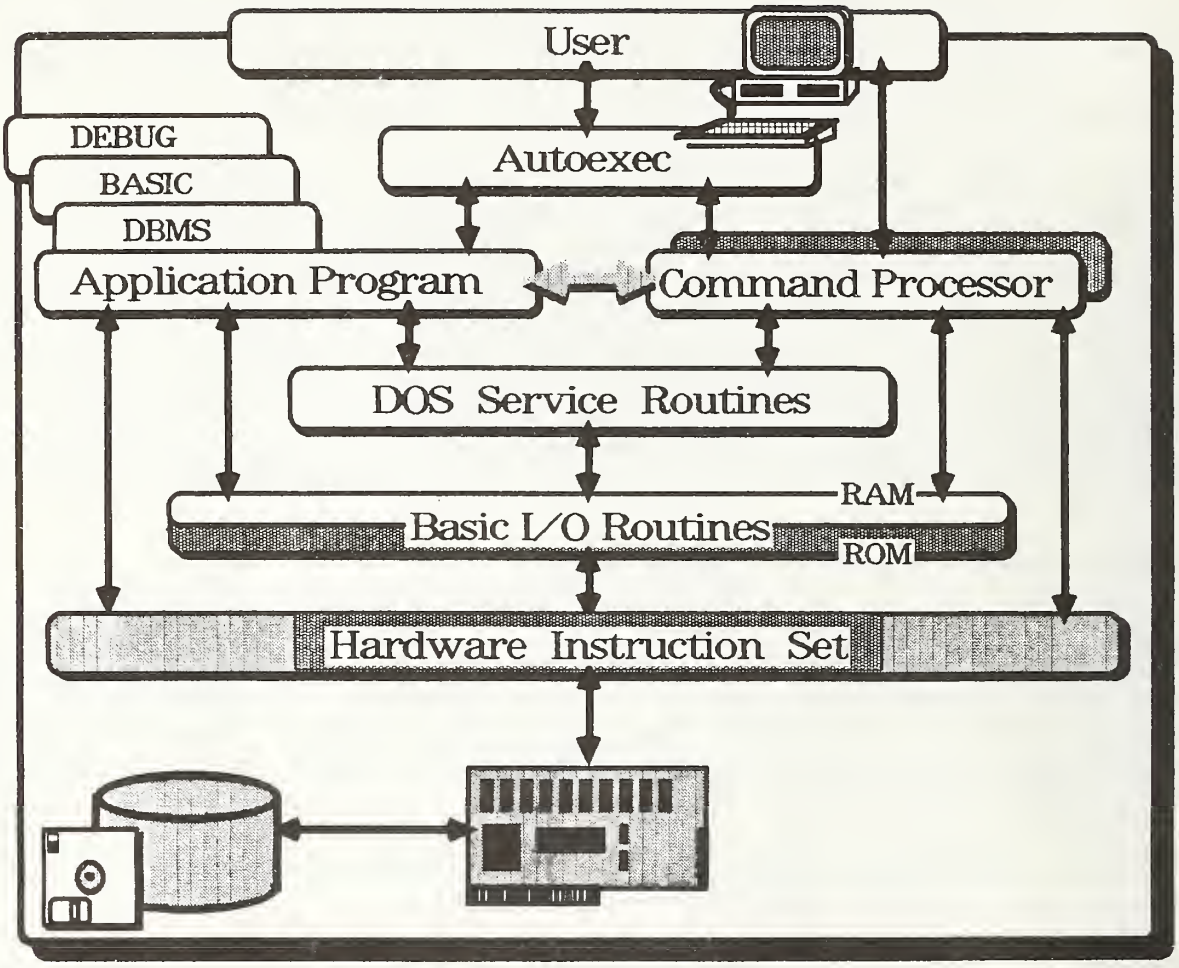


Figure 1-1: Internal Access Paths

It can be seen from the illustration that control mechanisms implemented at a given level (e.g. in an application program or even in the operating system) can be circumvented by using one of the alternate paths. Although is takes a certain level of technical competence to exploit such weaknesses, many experienced personal computer users acquire such skills.

1.2.3. NATURE OF DATA BEING HANDLED

The information processed and stored on personal computer systems often can be more sensitive and accessible than that found on larger, multi-user systems. This is due primarily to the fact that the information on a given machine is often associated with one person or a well-defined group. This information is likely to be in the form of memoranda, reports, spreadsheets, or simple

lists which are readily accessible using software tools familiar to all personal computer users. Finally, such data will tend to be in relatively "final" form, rather than being a mass of unanalyzed or unprocessed raw data. All of this may make the job of searching for specific information much easier than on a large systems with thousands of users and data files.

The personal computer has been called the electronic equivalent of the desk or file cabinet. This is a useful analogy, since users of personal computers should have an inherent understanding of the nature and need to protect items in their desks.

1.2.4. USERS RESPONSIBILITIES

In the past, many of the operational and security-related tasks associated with the use of computer systems were performed by relatively small and well-trained groups of systems and support personnel. This enabled economies of scale, standardization, and general consistency in the execution of such tasks. One of the perceived benefits of personal computers is the reduction of users' dependence on (and, perhaps, frustrations with) a central data processing facility. Along with that independence, however, goes many of the responsibilities that previously were assumed by the central facility. The problems of providing adequate training, assuring consistent procedures (security and otherwise), and minimizing duplication of effort (while retaining necessary separation of duties) are significant issues that make the personal computer environment unique.

1.3. IS THERE REALLY A SECURITY PROBLEM?

It may be argued that a "personal" computer does not need sophisticated security mechanisms and that users need only remove and lock away any diskettes containing sensitive data. Indeed, this concept of the single-user system has resulted in the general lack of security features in personal computers. In the "real world", however, most personal computer systems often are still too expensive to be sitting idle on someone's desk and, therefore, must be shared among several users. To compound matters, the introduction of fixed ("hard") disks for data storage and multi-user systems makes it difficult or impractical for a user to remove all sensitive data from the system. In addition, there may well be a valid concern for integrity of common software shared by several users (e.g. word processors, spreadsheet software, or data base management systems).

Thus, personal computers do, indeed, present data sharing and, therefore, real security problems. However, as will be discussed later, the problem should not be viewed as a PC security problem. Rather, the security of information on personal computers is just

a part of the overall information security issue which management must address. Nevertheless, both managers and users should understand the special security considerations which do affect their use of personal computers.

1.4. HOW TO USE THIS GUIDE

This document does not require an in-depth technical background on the part of the reader. However, it is assumed that the reader has at least a basic understanding of the features and uses of computers in general and personal computers in particular. For additional background, see NBS Special Publication 500-110 [HECHM84] or any of the many books on computer science available in libraries and bookstore. Appendix A contains references to several other publications which address small systems security issues.

The remainder of this document is organized into sections which discuss specific protection requirements of personal computers and a final section which provides recommendations and a general action plan for information security management in an environment containing personal computers. The appendices contain a list of additional references, a security self-audit checklist, and a categorization of commercially available personal computer security products.

2. PROTECTING THE EQUIPMENT

Before considering sophisticated data security mechanisms, it is first necessary to ensure basic physical and environmental protection of the equipment itself. If the computer system is damaged, stolen, or simply not working, most other security concerns are moot. This section describes control measures to provide a safe physical environment for personal computer systems.

2.1. THEFT AND DAMAGE PROTECTION

Protecting the PC (and associated equipment) from theft and physical damage is not a fundamentally new problem; it has been necessary to protect office equipment for years. The only new factors are the relatively high unit value of PC equipment and the need for somewhat greater concern for environmental controls. Otherwise, the physical protection needs of PCs are the same as other valuable equipment in the workplace. Indeed, if an organization has not addressed such problems prior to introducing personal computers, management should re-think its overall loss protection posture.

2.1.1. AREA ACCESS CONTROL

In general, personal computers should not be placed in areas which have no basic physical access controls (e.g. locks on the doors and people present during working hours). This is only prudent, since the value of a typical PC may well be in excess of $2000. Providing such simple and inexpensive controls will minimize not only the theft risk; it will also help reduce exposures to some of the more sophisticated technical problems discussed later.

2.1.2. EQUIPMENT ENCLOSURES

In situations where it is not feasible to secure an entire area, the equipment can be placed in special workstation enclosures which may be closed and locked when the equipment is not in use. This can provide protection for other valuable items such as documentation, diskettes, and other equipment.

2.1.3. EQUIPMENT LOCKDOWN DEVICES

To prevent theft of PC's (and other types of office equipment), several types of equipment lockdown devices are available. These may be used to secure the equipment to a table or other fixed object. Some devices also prevent access to the system power

switch and, thus can help prevent unauthorized use of the equipment.

2.1.4. EQUIPMENT COVER LOCKS

It is becoming increasingly important to prevent unauthorized access to the inside of the PC equipment itself, for the purpose of component theft protection and configuration control. Many systems contain valuable expansion boards (e.g. additional memory, modems, graphics interfaces, etc.) which have become a popular theft target. In addition, system security mechanisms (e.g. cryptography) may be dependent on certain components, and the integrity of such components must be protected. Equipment lockdown devices often provide additional protection against access to the interior of the equipment. Alternatively, devices are available for some systems which simply lock the equipment cover.

2.2. ENVIRONMENTAL CONTROLS

Personal computers are designed to operate in the "typical" office environment (i.e. without special air conditioning, electrical power quality control, or air contamination controls). In general, it can be argued that "if the people are comfortable, the PCs will be comfortable". Nevertheless, special attention should be given to minimizing the environmental hazards to which such equipment is exposed.

2.2.1. ELECTRICAL POWER QUALITY

The typical PC is sensitive to the quality of its electrical power source. It may be helpful if PC equipment can be placed on isolated power sources, although this is not always necessary. Inexpensive devices are available to protect against power surges (spikes) short of a direct lightning strike. If the local power supply quality is unusually poor (e.g. large fluctuations in voltage or frequency, voltage spikes, or frequent outages), then more extensive power conditioning, battery backup, or uninterruptible power supply (UPS) systems should be considered. In most cases, however, it will be sufficient to just keep the computer equipment on a power source separate from appliances or office equipment.

2.2.2. HEAT AND HUMIDITY

The temperature and relative humidity found in the typical office environment are well within the operating limits of most personal computer systems. However, if equipment is used in other

environments (e.g. on a factory floor or an outside location), users should refer to manufacturer specifications for the equipment. If portable systems are being used, care should be taken to avoid drastic changes in temperature or humidity (e.g. transporting a system from the outside into an office). Before operation, sufficient time should be allowed for the equipment to adjust to the new environment.

2.2.3. AIR CONTAMINANTS

The general cleanliness of the area in which personal computer equipment operates has an obvious effect on reliability -- both of equipment and magnetic media. It should be recognized that electronic equipment (including PCs) will naturally attract charged particles in the air. Eliminating such contaminants as smoke and dust will certainly have a beneficial effect on equipment and magnetic media (not to mention people).

2.2.4. FIRE AND WATER DAMAGE

The introduction of personal computer equipment does not represent any more of a significant fire hazard that does any other office equipment. It is unnecessary to install extensive fire and water protection systems similar to those required for major computer facilities. However, the value of the equipment, data and other items in the area may be sufficient reason for a re-examination of fire detection and suppression facilities.

To protect equipment from possible water leaks (e.g. from overhead piping), consideration should be given to inexpensive plastic equipment covers. Such covers will also provide protection from dust and other airborne contaminants.

2.2.5. OTHER ENVIRONMENTAL HAZARDS

2.2.5.1. Static Electricity

Static electrical charges can build up in personnel, especially if carpeting is used. A discharge can occur when the person touches the PC equipment. Such a discharge could cause damage to integrated circuit components or semiconductor memory. This problem can be minimized through the use of anti-static sprays, carpets, or pads. In addition, personnel can be instructed to discharge any built-up static charge by simply touching a grounded object (other than the computer). It may be worthwhile to post signs on each machine to remind users.

2.2.5.2. Radio Frequency Interference

In some isolated situations, radio frequency (RF) interference from other electronic equipment can cause computer equipment to malfunction. However, unless there are major nearby sources of such radiation, this should not be a problem.

2.3. MAGNETIC MEDIA PROTECTION

Particular attention should be given to the protection of magnetic media. Not only is this the primary repository of each user's information, it is perhaps the system component most vulnerable to damage. The following discusses hazards affecting the two primary types of magnetic storage media found in personal computer systems -- fixed and flexible disk systems -- and some general hazards which can affect all types of magnetic media.

2.3.1. FIXED DISK DEVICES

Fixed or rigid disk devices (also known as "hard disks") usually are self-contained sealed units that are relatively well protected from environmental contaminants. However, care must be exercised when moving these units, because of the danger of damage to read/write heads or other internal components.

2.3.2. FLEXIBLE DISKETTES

Virtually every personal computer system has at least one "floppy" disk drive. Flexible diskettes are the most prevalent medium for distributing software and data, and the handling of diskettes is an integral part of using almost any PC. The actual magnetic disk is contained within a protective jacket. However, there must be openings in the jacket for access by the read/write heads of the drive mechanism. These surfaces are particularly vulnerable to damage. Smaller ("microfloppy") diskettes employ a rigid plastic casing with a retractible access cover, thus reducing the vulnerability to rough handling and contaminants.

Potential dangers and proper handling techniques for flexible disks should be well known to all users, however, a summary of general precautions is worth repeating:

- Always store in the protective jacket.
- Protect from bending or similar damage.
- Insert carefully into the drive mechanism.
- Maintain an acceptable temperature range (50-125 F).
- Avoid direct contact with magnetic fields.
- Do not write directly on diskette jacket or sleeve.

Most of these precautions are simply common sense. Nevertheless, many PC users are quite careless in handling such media, and management has the responsibility of providing proper training in this area.

2.3.3. GENERAL HAZARDS

Exposure to ordinary contaminants (smoke, hair, doughnut crumbs, coffee, etc.) is probably the major reason for failures in magnetic media. Therefore, particular care should be exercised to minimize such exposures. Direct contact with magnetic devices should be minimized. It is worth noting, however, that airport x-ray devices and magnets (kept six or more inches away from magnetic media) pose no danger, despite considerable concerns to the contrary.

Simple wear is another cause of failures. Therefore, it is important that backup copies be made of all important disks. Indeed, day-to-day operation should be conducted with a backup copy, and not the master copy of such diskettes.

2.4. MAINTAINING PERSPECTIVE

While physical protection is certainly important, it is important that a sense of perspective be maintained. The typical personal computer installation cannot and, generally, should not be treated like a large data center with respect to physical and environmental protection needs. The amount of protection provided must be determined by the value of equipment and the value of the processing capability (i.e. the system criticality). Depending on the size of the organization and the nature of the processing, the system's criticality may dictate extraordinary physical protection measures.

In most cases, absolute prevention of unauthorized physical access cannot be achieved with reasonable cost constraints. However, it should be possible to ensure that such access is at least detected. For example, a simple cover lock or lockdown device will not prevent a determined thief from stealing the equipment. However, such devices will make it virtually impossible for a person to steal or even gain access to the interior of the equipment without being observed or detected. This usually will provide sufficient deterrence and protection.

Under the assumption that basic physical and environmental protections have been provided, it is now possible to look at several other categories of system and data security measures.

3. SYSTEM AND DATA ACCESS CONTROL

Although there is considerable value in the physical equipment, the purpose for having computer equipment is to handle information. Information and the ability to produce, store, and analyze it ultimately have considerably more value to the organization than the equipment itself. Protecting that information is a more challenging problem than simply protecting the equipment. This should be a major concern to management.

The problem of controlling access to systems and information consists of the following elements:

- Authorization - establishing the rules which determine who may access which systems and information.
- Identification - of users and the systems or data which they are permitted to access.
- Access Control - enforcement of the specified authorization rules.

Each of these is discussed below.

3.1. AUTHORIZATION RULES

The process of access control implies that some rules exist which specify which users are authorized to access which system resources (normally programs or data). Such rules must be established by the "owners" of the resources to be controlled. Authorization rules may consist of nothing more than a statement that only members of a given group or department are to have access to a given computer or application system. On the other hand, the rules may consist of formal definitions of information classifications and rules for accessing each. The type of authorization rules adopted will depend on the needs of each organization. It is important, however, that there be some type of authorization process.

Most automated access control mechanisms (on personal computers and on large-scale systems) are designed to address the former situation, where lists of systems or files and authorized users are developed and subsequently enforced. Enforcement of access control based on classifications of information (sometimes called "mandatory" access controls) are considerably more difficult to implement because of differing classification schemes and the need to provide unchangeable labels on the data to be protected. The mechanisms discussed below for personal computers fall into the first category.

3.2. IDENTIFICATION

For authorization rules to be enforced, it is necessary that users and resources (usually data) be identified. The following is a discussion of this process in the context of personal computers.

3.2.1. USER IDENTIFICATION

In a personal computer environment, user identification may be implicit or explicit. In a typical situation, a user establishes "authority" to use the system simply by being able to turn it on. If such implied identification is to mean anything at all, the system must be a true "personal" (i.e. single user) system and there must be adequate physical controls to ensure that only that user can gain access. Locked offices or equipment enclosures can provides some degree of assurance in this area. If a system is shared, then such simple identification procedures may not be adequate.

3.2.1.1. Initial Authentication

For most situations in which PCs are shared, user identification should be authenticated in some manner. This requires an explicit interaction between the system and the user. This should be accomplished with some type of system "logon" process in which the user provides a non-secret identifier (e.g. name or account number) and some sort of evidence to authenticate that claim (e.g. a password). User logon (authentication) should occur whenever the system is powered up or a new user needs to use the system.

It is worth noting that many user identification mechanisms for personal computers (both commercial products and user-developed systems) often require only a single (presumably secret) code, rather than separate identifier and authentication codes. This is not a good practice, since it does not provide a non-secret identifier for audit and accountability purposes. In addition, it may increase the opportunity for an intruder to guess a valid password, since any of the passords valid for the system will permit access.

Authentication at power-up (and after "system reset") is usually accomplished by a program which interrupts the system initialization process and requires the user to complete a logon process. Most personal computer operating systems provide a facility for an automatically executing ("autoexec") program to be invoked upon system power-up or reset. The actual program, however, must be provided by the user organization. Logon procedures can be developed "in-house", or commercially available products can be installed. Since an effective mechanism

requires relatively detailed technical knowledge, commercial products are often used. Some products involve additional hardware (e.g. expansion boards) which can trap key system events (e.g. power-up or system reset) and take control of the user authentication process. This can reduce the exposure of the authentication process to unauthorized modification, since the necessary hardware and software are often independent of the rest of the computer system.

3.2.1.2. Re-authentication

Re-authentication of the user should also take place whenever it is likely that the user could have changed. This is most easily accomplished in single-user systems simply by having each user turn off the machine after use. This requires each new user to go through the standard user authentication process. However, this is difficult to enforce and is often unacceptable when a machine must be used often, since the power-up process may require a significant amount of time. Alternative techniques include the following:

- Manual System Reset - Require each user to perform a "system reset" (often called a "system reboot") before leaving the machine. This will cause re-invocation of the logon process.
- Automatic System Reset - Set up the application program (or the AUTOEXEC file) to perform a system reset upon completion of processing.
- Automatic Timeout - Modify the operating system to cause a system reset after a predetermined period of system inactivity.

If user identification is established through a logon procedure, then that identification can be used for subsequent access control decisions. However, most single-user systems do not have mechanisms for retaining such identification for the duration of a session at the computer. Therefore, repeating the authorization process may be necessary during the course of a user's session at the personal computer.

3.2.2. RESOURCE (DATA) LABELS

In addition to identifying the user, there must be some means of identifying the resources to be protected. These "resources" are usually files containing data or programs. However, a resource could also be the ability to perform a certain function

within a given application. For the purpose of this discussion, we shall focus on data labeling.

3.2.2.1. External Labels

It has long been accepted practice to label sensitive documents and other materials with clear external indicators. Typically, the front cover (and often each page) of such documents must have a standard marking to indicate classification and handling requirements. Although such labeling is not always as easy to accomplish with the various forms of magnetic media used with personal computers, it is not difficult for floppy disks, the most common form of data storage medium. Diskettes containing sensitive information can be marked with special labels or brightly colored jackets. This will enable personnel to identify readily those materials that require special protection. This also, makes sensitive materials obvious to a would-be thief, so it must be assumed that users will provide appropriate protection for all such materials.

3.2.2.2. Internal Labels

If the operating system or programs are to recognize files containing sensitive information, internal (i.e. machine readable) labels must be present. The standard file management facilities of most personal computer systems provide only basic file identification capability -- the file name. However, it is often possible to store files in specific "directories", thus providing the ability to segregate files associated with each user or by data sensitivity.

3.3. LOGICAL ACCESS CONTROLS

Two basic approaches are available for protecting data. The first approach is to prevent unauthorized persons from gaining access in the first place. The second approach is to deny effective use of information even if access is gained. Logical access controls provide the first type of protection, cryptography provides the second. It is often appropriate to combine both types of protection.

The problems of controlling logical access are different for data stored on removable and those stored on fixed media.

3.3.1. REMOVABLE MEDIA PROTECTION

If the data is resident on removable media, then the simple lock-and-key approach will probably provide the most cost-effective

solution. If diskettes containing sensitive data cannot be protected in this manner (e.g. during shipment), then encryption may be appropriate.

3.3.2. NON-REMOVABLE MEDIA PROTECTION

If data resides on non-removable media (e.g. a hard disk), then preventing access to the data requires controlling access to the machine itself (user identification) and then to the data available to the user.

3.3.2.1. Physical System Access Control

There are several commercial products available to control physical access and use of personal computer equipment. If a given machine must be available for access by several users or cannot be physically locked when not in use, procedural controls may be possible. It is usually possible to provide effective access control to the equipment during working hours because people are present. However, it is often necessary to place equipment in areas which cannot be monitored at all times.

3.3.2.2. Internal Access Control

If equipment must be shared by several users and cannot be monitored at all times, then hardware- or software-based security mechanisms should be considered. Such mechanisms can limit the type of access available to each user. The AUTOEXEC type of facilities available on most personal computers can be used to set up special menu-oriented user interface environments which will limit what each user can do. A more comprehensive approach is to embed access control mechanisms in the operating system to reduce the opportunities to circumvent them. An example of such a control is the intercepting of all file open requests to check for proper user authorization. There are commercial products which are designed for this purpose, or users may develop such software themselves.

3.3.2.3. Potential Problems

However, when such technical access control mechanisms are employed, it must be remembered they are vulnerable to attack if a user has the opportunity to make modifications to the equipment (e.g. by removing or substituting circuit boards) or to the software (e.g. through programming or debugging facilities). Nevertheless, such modifications often require certain technical skills and "unusual" actions (e.g. opening up the cabinet) that can often be noticed by alert employees. If users require only pre-determined functional capabilities (e.g. routine entry of

transaction data), then these types of controls should be fully satisfactory.

It should also be recognized that the type of constrained environment suggested above, except for certain well-defined and restricted applications, may negate the benefits for which the personal computer was originally acquired. It may be easier, cheaper, and more effective in the long-run to put sensitive applications (i.e. those requiring special protection) on different computers.

3.4. CRYPTOGRAPHY

Cryptography is the process of transforming information (cleartext) into an unintelligible form (ciphertext) so that it may be sent over insecure channels. The transformation process is controlled by a data string ("key"). Anyone intercepting the ciphertext while it is in the insecure channel should require the appropriate key to decrypt (convert back to cleartext) the information. The intended receiver is assumed to have that key.

Cryptography not only provides protection against unauthorized disclosure. It also can ensure the detection of unauthorized modifications of information, since any change to encrypted data (without the necessary key) will prevent successful decryption by the intended recipient. It should be clear, however, that cryptography does nothing to prevent modification, or destruction; it simply ensures the detection of such events. Critical data, therefore, cannot be protected simply by encrypting it.

Although the primary application of cryptography is in data communications, it has important applications in a personal computer environment. In effect, personal computers and their storage media can be considered "insecure channels" because of their physical accessibility. The following discusses only personal computer (vs. communications security) applications.

3.4.1. GENERAL CRYPTOGRAPHIC FACILITIES

There are several commercially available software and hardware based products which provide personal computer users with cryptographic capabilities. These products, in general, enable the user to perform the following cryptographic functions.

- Enter or change cryptographic keys
- Encrypt a block of data
- Decrypt a block of data

In some cases, facilities are provided for the generation and

management of keys. Normally, however, this is left to the user. Indeed, this can be one of the major problems in the effective use of cryptography, since the randomness and secrecy of keys are critical to the protection provided by cryptography.

3.4.2. BULK FILE ENCRYPTION

The normal manner in which cryptography is used in a personal computer environment is to encrypt and decrypt entire files. Typically, a user prepares a file (presumably containing sensitive information) and then runs an encryption utility to produce a ciphertext version of the file. The original file should then be overwritten. (See discussion below on data residue). Before using the file again, the utility program must again be used to decrypt and produce a cleartext version of the file. The user is usually responsible for selecting, entering, and remembering the key used for the encryption and decryption process. Commercial cryptographic products usually provide utility programs for bulk file encryption and decryption as well as a utility to overwrite old files.

3.4.3. INTEGRAL FILE CRYPTOGRAPHY

Problems with bulk encryption and decryption of data files include general inconvenience, the need to erase cleartext files, and the personnel training necessary. An alternative for file encryption is to use a cryptographic facility which is integral to the file input/output subsystem. Basically, each block of data to be written to disk is first encrypted, and each block read from disk is decrypted before it is passed to the requesting program. This makes the entire cryptographic process almost transparent to the user and eliminates the inconvenience and dangers associated with bulk file procedures. Users with sufficient technical expertise can implement such a capability themselves. In addition, there are commercial hardware and software products which may be considered.

3.4.4. SELECTION CONSIDERATIONS

In selecting cryptographic products, two basic considerations are important:

- Private vs. public key systems
- Cryptographic algorithm
- Hardware vs. software implementation

It is beyond the scope of this guide to deal with these subjects in detail. However, the following paragraphs address the basic issues.

3.4.4.1. Private vs. Public Key Systems

There are two basic types of cryptographic systems in common use. A "private key" cryptosystem requires that the sending and receiving parties share a common cryptographic key. This key must be kept secret (private) to ensure the security of the encrypted information. This requires special precautions and protocols for the distribution of keys. Indeed, this has long been one of the difficulties in the widespread application of cryptography to large communications networks. In situations involving small numbers of users, this is generally not a significant problem, however.

A "public key" cryptosystem involves pairs of keys, one for encrypting messages and another for decrypting. The encrypting key is public, so than anyone wishing to send a message to a given user can use that person's encrypting key. Only the recipient, however, has the (secret) decryption key. This type of cryptosystem can reduce certain key management problems and can be attractive for large networks of interconnected users.

In both types of system, the selection and protection of keys (even public keys) is critical to the overall security of the system. It is possible to combine the use of each type of system to provide very effective security with relatively little administrative overhead.

3.4.4.2. Cryptographic Algorithms

All cryptosystems require a well-defined process (algorithm) by which information is transformed from cleartext to ciphertext and back to cleartext. It is an accepted principle of cryptology (the design and analysis of codes and ciphers) that the strength of a cryptosystem should not be dependent on the secrecy of the algorithm itself. This enables the exchange of information necessary for design and manufacture of systems incorporating the algorithm. It also permits critical analysis of the algorithm itself. It also eliminates the need to provide physical protection for devices and documentation.

The Data Encryption Standard (DES) is the cryptographic standard for non-classified Federal Government applications. The DES is a private key cryptosystem and is described in Federal Information Processing Standards Publication 46 [FIPS46]. The DES has undergone extensive critical analysis, thus providing a high level of understanding of the level of protection it provides. It is important to note that Federal Government agencies are, in general, required to use the DES for cryptographic applications involving non-classified information.

Although there is no standard public key cryptosystem, there are algorithms that have been published in the open literature. Like DES, they also have received considerable critical review, and the level of protection provided is relatively well understood. Several commercially available cryptographic products incorporate the either the DES or the openly-available public key algorithms.

A number of commercial cryptographic products (both private and public key systems) use proprietary (secret) cryptographic algorithms. Such algorithms are often designed to operate at higher speeds than such algorithms as the DES. However, since the algorithms are not made public, it is difficult to obtain an objective evaluation of their cryptographic strength. It is, therefore, the responsibility of the user to make the necessary determination.

3.4.4.3. Hardware vs. Software

Cryptographic algorithms can, in general, be implemented in either hardware or software. The former approach usually results in much faster operation and better integrity protection while the latter approach is often cheaper and more flexible. Hardware implementations of the DES on a single integrated circuit chip are available and are used in a number of cryptographic products. Full compliance with the DES requires hardware implementation, although software versions of the DES algorithm are available.

3.5. RESIDUE CONTROL

Another aspect of access control that often is overlooked is that of data "residue" left on disk or in memory. This is data that is stored in areas of disk or memory which have been released for reuse. Such information often can be read by subsequent users. A common example of the disk residue problem is associated with the "erasing" of disk files (e.g. with the ERASE or DELETE commands). This process usually results only in the setting of a "file deleted" indicator in the file directory -- not the physical erasure or overwriting of the actual data. It is often a simple matter to reset the "file deleted" indicator and thereby "unerase" the file. In fact, there are many software utilities designed for exactly this purpose. It is dangerous, therefore, to pass files to other users on diskettes which contain "erased" files of sensitive data. The problem also exists for hard disks, since the data remains potentially accessible to subsequent users of the system. Users should also recognize that many common programs (e.g. word processors) create and delete "scratch" files which the user never sees. These files could contain sensitive information and are exposed to the same vulnerability.

This problem can be solved by using a program to "purge" (i.e. overwrite) all file data as part of the deletion process. This might be thought of as the electronic equivalent of the traditional "burn bag" used to discard sensitive information. Although such programs are relatively easy to write, they are usually not provided as standard features of personal computer operating systems. Therefore, they must be acquired or written by the user. If such a utility is not available, then sensitive disk media should not be shared among users. If a fixed disk is used for such data, then the user has three options: use an overwrite utility , encrypt sensitive files, or do not share the system with other users.

3.6. PLACEMENT OF CONTROLS

In general, it is desirable to place control mechanisms as "low" in the system as possible, to reduce the number of alternate paths available for circumventing them. The levels at which such controls can be placed, from "lowest" to "highest", are the hardware, operating system, application program, and user "environment".

Controls placed at lower levels (e.g. hardware or operating system) tend to be stronger, but designing and implementing such controls are often beyond the capabilities of most users. In addition, changes made at this level may impact system reliability and compatibility. Therefore, such controls usually must be provided by the system supplier or other vendors. It is easier for user organizations to implement controls within application systems or to establish limited user "environments" through the use of automatically executing programs. Unfortunately, controls at this level are often easy to circumvent.

3.7. SUMMARY

Personal computers do not, in general, have the type of hardware and operating system support mechanisms necessary for sophisticated security and access control. However, these systems usually are used to handle large numbers of users, so such mechanisms often would constitute needless overhead. Nevertheless, many opportunities exist for providing technical access control mechanisms over personal computers and the data they contain. These mechanisms can be developed by the user or can be acquired commercially. It is important, however, for the user to determine first the type of control actually necessary for a given system, rather than arbitrarily installing sophisticated (and often costly) access controls.

4. SOFTWARE AND DATA INTEGRITY

It has long been recognized that software and data integrity are critical in almost all phases of data processing. In most organizations, information produced on computer systems (usually large-scale systems) and the software used to handle such information has been subject to extensive critical review and error-checking, both during system development and during normal processing. This has enabled a great deal of confidence to be placed in the quality of resulting information and other "products" of computer systems.

The personal computer has made powerful computational and analytical tools available to users throughout many organizations. Increasingly important decisions are being made based on information processed by such systems. Unfortunately, there may be a reluctance to apply the same degree of care (and cost) in integrity assurance as is routinely applied for larger systems. Nevertheless, the formal and "official" appearance of printed materials which can be produced easily by any personal computer can result in unwarranted confidence in the substance of such materials.

To the extent that personal computers are used for routine personal work and are not being used for critical decision-making functions, the lack of formal quality and integrity controls may not be a significant problem. However, for applications which are critical to the organization, there must be commensurate quality controls.

4.1. FORMAL SOFTWARE DEVELOPMENT

In situations where important functions are being performed on personal computers, management should consider application of formal controls over software development, testing, and data integrity. This applies not only to situations where systems are being designed and programmed in traditional programming languages (e.g. BASIC or Pascal). There is increasing use of generic software tools (e.g. spreadsheet and data base management system) to build complex applications. Even though many of the typical programming problems may be reduced in these situations, the need for careful analysis and control is just as important. This may very well require additional training of personnel or the use of specially trained personnel, since system development skills are not a normal part of professional training.

4.2. DATA INTEGRITY CONTROLS

Even a properly functioning application program is of little value if the data it handles is corrupted. Most generic software tools do not provide built-in facilities for checking the integrity of input data. Therefore, it becomes the responsibility of the user to build in such checks. These should include data format and range checks and other redundant cross-checks of results. Managers should require supporting information and evidence necessary to assure that calculations and other data handling operations have been performed properly. It is perhaps most important for managers to require individual accountability and auditability of results before relying on information generated by PC systems.

4.3. OPERATIONAL CONTROLS

When a major data processing application is implemented on a PC, formal operational procedures are as critical as they are for large-scale system. An important application is important regardless of where or how it is processed. Operational procedures should include:

- Data preparation and input handling procedures
- Program execution procedures
- Media (probably diskette or tape) procedures
- Output handling and distribution procedures

These are, of course, the same types of procedures needed for large-scale system applications. It is important to recognize, however, that the personnel performing such procedures probably will not have extensive data processing or operations training and will be performing these duties along with their other responsibilities.

4.4. DOCUMENTATION

Documentation of all aspects of any repetitive activity is critical to its ongoing operation. Again, the use of generic software tools makes some believe that there is less need for documentation. In addition, it is often more difficult to prepare documentation for such systems, since the user interface is often not as simple and straightforward as specially-designed application programs. Rather, the user often must first understand how to use the generic application then must learn procedures for each specific applications. This problem can be alleviated somewhat with the use of facilities in many generic software tools to "customize" an application and thereby simplify the user interface.

4.5. ADDITIONAL GUIDANCE

It is beyond the scope of this document to describe the many types of system and data integrity controls that apply to data processing applications in general. Nevertheless, most of these controls and procedures apply equally to the personal computer environment and should be understood by management. The reader is referred to Appendix A (and, in particular, FIPS PUB 73) for additional information.

5. BACKUP AND CONTINGENCY PLANNING

The problem of backup and contingency planning in a personal computer environment is essentially the same as for other data processing activities. Indeed, for organizations with both personal computers and large-scale systems, the backup and contingency planning should be an integrated process. However, there are special considerations for personal computers due primarily to wide distribution of equipment and number of people now involved. This section discusses some of these considerations. For additional information on contingency planning, the reader is referred to Appendix A.

5.1. ELEMENTS OF CONTINGENCY PLANNING

Contingency planning consists of those activities undertaken in anticipation of potential events which could cause serious adverse effects. This, of course, could apply to individual users and their applications as well as to organizations. In a personal computer environment, one of the key elements in the contingency planning process is the individual user, since there is no central staff to perform many of the important functions.

Contingency plans should consist of emergency procedures, resource (hardware, software, data, etc.) backup preparations, and backup operation plans. In addition, comprehensive contingency plans will include recovery and test procedures. This section will focus primarily on the first three areas.

5.2. EMERGENCY PROCEDURES

In general, the introduction of personal computers into an office environment should not require significant changes in emergency preparations. Any area in which people work and important information is handled should have basic emergency procedures, including:

- Alarm activation and deactivation procedures
- Evacuation plans
- Lockup procedures
- Medical emergency supplies and procedures
- Fire detection and extinguishing equipment
- Bomb threat procedures

If such precautions are not in place, then the introduction of the personal computers may emphasize the need, if for no other reason than to protect the investment in equipment.

5.3. FILE BACKUP

With a personal computer "on every desk", there is obviously a need to encourage regular and systematic backup of files, since such backup can no longer be done centrally and systematically as is possible with a large-scale system. Unfortunately, it often takes the loss of an important file before most users become "converts" to the need for regular backup.

5.3.1. BACKUP APPROACHES

The method and frequency of backup must be determined by each user, based on the storage media and the volatility of the data involved.

5.3.1.1. Full Volume Backup

For data stored on diskettes or other removable media, it is often easiest to make a backup copy of the entire volume (e.g. diskette) after each use or at the end of each day if a given volume is used frequently during the day. This approach eliminates the need to keep track of individual files. If the original volume is damaged, the backup copy is used.

For large capacity, non-removable storage devices, such as fixed disks, it is usually impractical (and unnecessary) to perform full disk copies on a daily basis. In this situation, two basic alternative approaches should be considered, incremental backup and application-based backup.

5.3.1.2. Incremental Backups

In an incremental backup, only those files which have been modified since the last full or incremental backup are copied to the backup medium. This, of course requires a mechanism in the file system to set an indicator whenever a file is opened for writing. Most personal computer operating systems designed to handle hard disk systems have such facilities. It should be noted, however, that full backups are still required (e.g. monthly), since no single incremental backup will contain all files.

Recovery from minor problems (e.g. a single file error) involves locating the latest incremental backup containing the affected file. Recovery from major file loss, however, requires first reloading from the last full backup and then reloading each successive incremental backup. This can be a very time-consuming and error-prone process if there are too many incremental backups between full backups. A reasonable schedule might be a full

backup each month and and incremental backup each week. However, the specific schedule must be determined for each system.

5.3.1.3. Application-Based Backup

Because of the potential complexity of incremental backups and the impracticality of full-volume backup for large capacity volumes, it may be more appropriate to perform backups based on each application or file grouping. Examples of file groups might be individual file subdirectories. Certain file groups (e.g. generic software, which never changes) would need only one initial backup. Software associated with locally-maintained applications needs to be backed up only when the software is changed. Data files can be backed up whenever updated. Although this approach may require more backup volumes (e.g. diskettes), it will generally be easier to organize them and to locate files for restoration than with incremental or full-volume backups.

5.3.2. BACKUP MEDIA

The most common backup medium is floppy disk, since virtually every personal computer has a floppy disk drive. For systems with hard disks, however, a full file backup may require more than 20 diskettes. Alternatives, such as streaming cassette backup systems should be considered if incremental backups to diskette are too difficult or time consuming.

Errors on backup copies can obviously have disastrous consequences. The typical backup utilities available on personal computer systems are basically just file copy functions; they do not contain redundancy mechanisms found in some larger scale systems. Therefore, regardless of the type of backup, only high-quality media should be used. Additional assurance of successful backup can be achieved by performing file comparison of original and backup copies. Most personal computer systems provide disk and file comparison utility programs. In addition, some operating systems provide a write-verification option (which usually may be turned on or off as desired) which will read each disk record immediately after it is written to verify its accuracy. Most backup, file copy, or file comparison utilities will provide a display of files processed. This information should be directed to the printer and stored with the backup media.

5.3.3. STORAGE

It is important for users to understand the threats addressed by backup procedures. The obvious reason for backing up files is to enable recovery of data after loss due to media or hardware problems or accidents (e.g. unintentional erasure of files).

This causes users to store backup copies in a convenient, nearby location. The other threat of concern, however, is loss resulting from a fire, theft, or other event which might involve an entire office or building. In these situations, locally stored backup copies would be lost along with the originals. Therefore, careful consideration should be given to storing periodic archival copies at some location unlikely to be jointly affected by "common" emergencies such as fire or flooding. In situations where personal computers are connected to a data communications network (e.g. a local area network), it may be possible to establish procedures to make backup copies on a separate device, such as a remote host or a file server. This may provide the physically separate storage needed for disaster recovery purposes.

5.4. OTHER BACKUP CONSIDERATIONS

Data files are not the only things that can be lost, damaged, or destroyed. Indeed, without the necessary equipment, personnel, and documentation, the data files themselves may be useless. Therefore, users must identify all elements which comprise their personal computer applications.

5.4.1. EQUIPMENT AND FACILITIES

One advantage of widespread use of personal computers is built-in equipment backup. If one machine is damaged or lost, it may be easy to find a replacement. However, not all systems are compatible. As application systems on personal computers become more complex, it becomes more difficult simply to move to another personal computer. Different equipment options, installation variations, and piracy protection mechanisms used in many popular software packages can make "portability" extremely difficult. It should also be recognized that a major disaster (e.g. a fire or water damage) may affect much more than a single machine or area. Therefore, advanced planning is critical.

5.4.2. SOFTWARE

Application software should be protected in the same manner as data files. Backup considerations may differ, depending on the source of the application software.

5.4.2.1. Commercial Software

Applications on personal computers are often built around mass-marketed "generic" software, such as database management systems, spreadsheet programs, or word processing systems. Licensed software is often costly to replace if not properly registered

with the supplier. Much commercially available software is distributed with piracy protection mechanisms that link the software to a given machine or "system" disk. This may cause considerable difficulties when trying to conduct backup operations on different equipment or with alternate versions of the software.

5.4.2.2. Locally Maintained Software

For locally developed or maintained applications, backup should include source program files and, optionally, loadable versions of all software. The required compiler or interpreter programs should, of course, also be backed up. (See discussion above on application-based file backup.)

5.4.3. PERSONNEL, PROCEDURES, AND DOCUMENTATION

Personal computer applications, especially those involving only one machine and only one person (or a small group), are often unique. Moreover, they are often developed in a much less structured environment than "traditional" data processing applications. Nevertheless, they often require a detailed knowledge of procedures which may not be documented. If such applications have any long term value, it should be clear that their operation should not be dependent on a single persons or small group. In emergency situations, others should be able to understand and use the applications. This requires specific efforts to document procedures and, perhaps, cross-train personnel.

5.5. SUMMARY

Backup and contingency planning are difficult activities, because they concern non-immediate problems and considerable speculation regarding future events. In a personal computer environment, because of the many users who may be involved, these problems become even more difficult. Nevertheless, management must ensure that users are aware of both the need for regular backup activities and that they have the necessary tools and training to perform those activities in an effective and consistent manner.

6. MISCELLANEOUS CONSIDERATIONS

Effective information security involves more than issues and measures discussed in detail in the previous sections. This section discusses several of these additional areas of concern.

6.1. AUDITABILITY

Designers of important applications, whether on small or large systems, will require reliable audit trails. Organizations also may wish to monitor use of personal computers by employees. A single-user personal computer may need special audit trail facilities as an historical record and to aid in recovery from errors. The placement and use of audit trails in personal computer systems, however, requires special considerations.

6.1.1. PLACEMENT OF AUDIT TRAILS

Audit trail information can be recorded as part of an access control process such as those discussed earlier. However, designers should avoid dependence on the personal computer to provide a safe environment for the storage of such data. It may be too easy for a user to modify or delete such data. If it is important enough to keep audit trail information on the personal computer, the system should be provided with appropriate physical and access control safeguards to protect the integrity of that data. If access to a host system is involved, the host is the proper location for the placement of audit data capture mechanisms.

6.1.2. USAGE MONITORING

Organizations with substantial investment in personal computer equipment may wish to monitor the usage of such equipment. Although this is not primarily a security concern, effective monitoring can have security benefits. The types of event that may be of interest include:

- System startup
- User session initiation and completion
- Program initiation and completion
- Access to certain data files

It is, of course, possible to require users to maintain manual logs of such activities, but this is likely to be ineffective. It is possible to develop or acquire software which will record basic system usage information. This requires, at minimum, the use AUTOEXEC-type routines and may involve modifications to operating system functions to ensure that all relevant activity

is logged. In addition, it will require a reliable source of date and time information (e.g. an internal clock-calendar) and methods to protect the log information from modification or destruction. Management must decide if the user constraints needed to meet these requirements are justified by the usage information that will be obtained.

6.2. MULTI-USER PERSONAL COMPUTERS

The is an increasing number of microprocessor-based systems that are capable of supporting several concurrent users. Some of these systems have advanced hardware that supports multiple processor states, virtual memory addressing, and other hardware features that are needed to provide adequate user isolation and security. Such systems, despite their size, are functionally the equivalent of multi-user minicomputer and mainframe systems. Therefoe, if they will be supporting users with security requirements, they must be provided with appropriate administrative and physical protection to enforce those system security features that may be present.

Most multi-user microprocessor systems, however, simply allow one or more processors and memory segments to be shared, with no attempt at assuring security (i.e. user isolation and access control). Such systems are not appropriate for groups of users who have a need to control data access among themselves, since any control mechanisms are likely to be ineffective.

6.3. COMMUNICATIONS ENVIRONMENTS

In most organizations, the personal computer is but one of several types of data processing devices used. Increasingly, there is a need to connect personal computers as terminal devices to larger host systems or to connect two or more personal computers in networks. The security issues in each of these situations are basically the same as have always existed in multi-user host systems and data communications networks, respectively. There are some unique issues, however, which should be addressed by managers.

6.3.1. TERMINAL EMULATION

When a personal computer is used as a terminal device to a host system, the basic requirements for security and access control remain with host. As far as the host is concerned, there is just another terminal out there. It must be recognized, however, that the personal computer has the ability to upload (send to the host) and download (receive from the host) large amounts of data

at rates often exceeding those possible with ordinary terminals. This may be possible even with the same speed communication lines because the personal computer's disk drives may be used, thus eliminating the printer or keyboard. The amount and types of data that can be downloaded is still, however, under control of the host.

Communications software for personal computers often provide the facility to store telephone numbers and logon sequences for frequently called host systems. A significant potential problem exists when users store passwords or other sensitive information in this manner. In effect, the security of the host is now dependent on the physical security provided over the personal computer and its files. Users should be instructed never to store host system passwords or other sensitive information in communication software control files.

6.3.2. THE PERSONAL COMPUTER AS HOST

Personal computers are often used as single user host systems. A typical situation would involve a personal computer and an autoanswer modem that permits a person to use the system remotely. A simple logon protocol is appropriate in this situation. If only one person is intended to use the system, a simple (well selected) password should suffice. However, if several users are to be allowed access, and there is a need to monitor and control the system, a traditional user identifier and password logon process should be used.

6.3.3. PERSONAL COMPUTER NETWORKS

When two or more personal computers (or similar devices) are connected in a network, communication security becomes a problem. It should be recognized that in most local area network (LAN) systems, all nodes have the ability to read all traffic on the network. Therefore, privacy cannot be assured without the use of cryptographic protection. Most commercially available data encryption devices will work with personal computers as well as other devices. There are also available devices which are incorporated into the personal computer (i.e. expansion boards) which include complete communications and cryptographic protocol functions.

6.4. ELECTROMAGNETIC EMANATIONS

All electronic equipment emanates electromagnetic signals. For some equipment (e.g. computers, communication lines, and data terminals) these emanations may carry information which can be detected by appropriately placed monitoring devices. Security

measures intended to combat this problem are known as "Tempest" controls. Applications involving classified (National Security) data generally must be processed on equipment that has been specially shielded or modified to minimize emanations. Although the technical requirements for such shielding are classified, Tempest-certified equipment is available for purchase by non-defense users -- at a considerable price premium. Except for classified applications, it is the user's responsibility to determine if the extra cost is justified.

6.5. THE MICRO AS AN ACCOMPLICE

The danger posed to host systems due to increasing availability of personal computers (i.e. the potential of the personal computer as an "accomplice") has received considerable attention in the news and entertainment media. This is perhaps the greatest security concern expressed by managers regarding personal computers.

Although there is certainly some reason for concern, it is important to recognize that almost no new host system security threats result directly from the use of personal computers. The personal computer is functionally the same type of threat as a "dumb" terminal, and adequate security measures for terminal access have been available for a long time. Even such seemingly exotic threats as programming a personal computer to generate automatically thousands of telephone numbers and passwords are easily defeated with available mechanisms -- if they are used. To the extent that security problems exist for an organization's remotely-accessed host systems, the fault probably lies with inattentive or imprudent management, not with the introduction of personal computers.

6.6. ADDITIONAL ISSUES

There are many other issues involving the rapidly expanding use of personal computers that must be faced by management. These include the problems of controlling licensed software, personal use of equipment, and employees working from home. Each of these has some clear security implications. However, most of these involve policy and administrative considerations that are outside the scope of this document.

7. MANAGING THE PROBLEM

The preceding sections have described the nature of security exposures facing the users of personal computer systems and some of the specific control measures which can be used to reduce those exposures. This section provides an overall management perspective to the problem and an approach to effectively managing information security in a personal computer environment.

7.1. INFORMATION SECURITY MANAGEMENT - AN OVERVIEW

Information security management involves more that just providing security for various computer systems. The following is a brief overview of the process.

7.1.1. PROTECTION STRATEGIES

There are three basic strategies for protecting information resources from the threats listed above:

- o Prevent threats from striking; or
- o Detect that threats have struck; and
- o Recover from damaging effects.

Any given security measure will fall into one or more of these basic strategy categories. The objective of security management is to select cost-effective control measures which involve **all** of the above protection strategies, not just one or two.

7.1.2. A GENERAL APPROACH TO SECURITY MANAGEMENT

It should be obvious that the above strategies are not, in themselves, of much value to a manager or user concerned with protecting information. A systematic approach to identifying and implementing security requirements is needed. In general, such an approach should include the following activities:

- o Asset Identification - identifying and classifying the information and other assets that require protection.
- o Risk Assessment - identifying and evaluating the threats, specific vulnerabilities, and degree of exposure (risk) to information assets.
- o Control Selection and Implementation - selecting control measures which provide cost-effective reduction of exposure.

- o Audit & Evaluation - on-going activities to review the continued effectiveness and appropriateness of controls.

The underlying objective of these activities (and, indeed, the challenge to management) is the selection and implementation of **cost-effective** control measures. With unlimited resources, virtually any level of security could be achieved. However, no rational organization should commit resources in excess of the risks involved. The key, therefore, is **risk management.**

7.1.3. RISK ANALYSIS AND RISK MANAGEMENT

The concepts of risk analysis and management are central to any rational information security program. The purpose of risk **analysis** is to determine the exposure to loss (usually expressed in expected dollar loss per year) for a given system. Risk **management** is concerned with reducing those risks to an acceptable level. That level will be determined by balancing the cost of alternative control measures against their risk reduction characteristics. Basically, the risk manager must minimize total security-related costs, which consist of expected losses plus the cost of controls.

7.1.3.1. Focusing on Information Assets

When analyzing risk, it is important to view the problem as an **information** security problem, not a **computer** security problem. This is particularly true as the personal computer becomes just another office tool such as the typewriter, dictating machine, or telephone. Risks are related primarily to **information** and only secondarily to the physical devices on which that information may be stored or processed.

7.1.3.2. Risk Analysis Activities

In general, risk analysis consists of the following steps:

- o Potential Loss Analysis - determining the potential losses which could be suffered **if** various adverse events were to occur.

- o Threat Analysis - identifying the source and likelihood (e.g. occurrences per year) of adverse events actually occurring.

- o Exposure Evaluation - combining estimates of potential lost and frequency of occurrence to obtain estimates of **expected loss** (usually expressed in dollars per year).

In concept, this process involves the use of quantitative estimates of potential loss, occurrence rates, and loss expectancies. For large, centralized data processing activities involving many applications and users, the process of formal risk analysis may be costly and time-consuming. Nevertheless, such a relatively complex environment requires a careful and systematic analysis. In a small systems environment, however, the risks and the associated need for detailed analysis are probably less. The primary focus should not, however, be on the value of the equipment involved.

Except for the obvious need to provide physical protection for the equipment, the security concern (particularly in a small systems environment) should be with the **application**, not the equipment. If a system is not being used for sensitive or critical applications (which, in many cases, it will not), then a formal (i.e. quantitative) risk analysis is not necessary. If, on the other hand, a highly sensitive or critical application is being run on the small system, then a detailed risk assessment must be performed **regardless of the value of the computer equipment itself.**

For additional information on risk analysis, see the references in Appendix A, in particular, [FIPS65] and [FIPS31].

7.1.4. SECURITY MANAGEMENT PROGRAM ELEMENTS

There are many possible ways to structure an effective security management program. The key requirement is to **establish** a **formal program.** This is of particular importance in a small systems environment because of the large number and relative autonomy of people who are likely to be using such systems in a typical organizations. Without some formal security management structure and associated guidance, these various users cannot be expected to apply consistent and effective controls. The following are the elements of such a program which are required for Federal agencies (in accordance with OMB Circular A-71, Transmittal Memorandum 1, July 27, 1978):

7.1.4.1. Responsibility

There should be a formal assignment of authority and responsibility for information security management for the entire organization. This applies to information in **any form**, whether it be on a personal computer, a mainframe system, or on paper. However, the basic operational responsibility should be placed with the people who "own" the information, have the incentive to protect it, and have the necessary authority and resources, i.e. the **user** organizations. Therefore, except for development of

policy and guidance, a single point of responsibility for personal computer security is probably inappropriate.

7.1.4.2. Personnel Screening

Many security controls ultimately depend on trust in individuals. Therefore, there should be some process to screen personnel who are authorized to access sensitive information systems. This does not imply, however, that special screening is needed simply because a person will be using a computer system. Most organizations have pre-employment screening procedures and, if needed, security background investigations. If such screening is considered sufficient for the employee's position description, it should be irrelevant whether or not a computer is used as part of the job.

7.1.4.3. Management Control Procedures

Management should establish formal control procedures over the development and use of information systems. This is more easily done when such information systems are relatively well structured and distinct. Many of the ad hoc uses of personal computers are not, however, well defined or structured. Nevertheless, if important decisions are based on the results of personal computer applications, management must establish procedures to ensure the accuracy and integrity of the information generated.

7.1.4.4. Risk Analysis

There should be periodic formal assessments of threats and of risk associated with sensitive information systems. This is required as a basis for selection of cost-effective control measures for those systems.

7.1.4.5. Contingency Plans

The continued availability of many information systems are important or even critical to the organization. Therefore, management should establish formal plans and procedures to respond to emergency or disaster situations which would disable or make such systems unavailable.

7.1.4.6. Procurement Procedures

In general, it is more difficult and costly to "retrofit" security measures into systems after they have been implemented. Therefore, it is important the security requirements be specified

early in the design or procurement process. There should be policies and procedures for ensuring that security requirements are specified in all procurements of systems and equipment.

7.1.4.7. Audit and Evaluation

Systems, organizations, and environments change. This often results in changes in the risks facing an information system. There should be a program of regular audits and evaluations of sensitive systems to ensure the continued adequacy, effectiveness, and appropriateness of security measures.

The elements listed above do not, in themselves, assure appropriate protection. Rather, they provide a consistent framework within which to build an effective information security program.

7.1.5. MANAGEMENT'S ROLE

As is the case for any security program, it is management's responsibility to provide the lead in assuring security for personal computer systems. This is all the more important due to the growing number people in the organization who are or will soon be involved in the use of such systems. Management should focus on a) protecting information, not computers and b) emphasizing the use of a risk management approach to make protection decisions, and c) assigning responsibility (and necessary authority) for security to the actual "owners" and users of the information resources.

7.1.5.1. Information vs. Computer Security

Perhaps the most important thing that management can do in addressing the personal computer security problem is not to view it as a personal computer problem. Since personal computers represent only a tool (albeit a ubiquitous one) in the organization's overall information handling process, management should address the overall automated information security problem. This approach will help ensure consistency of policies and procedures and the involvement of everyone in organization. Although the technology and economics of security have changed, the basic objectives have not -- the confidentiality, integrity, and availability of information resources must be protected.

7.1.5.2. Adopting a Risk Management Approach

Because valuable and potentially sensitive information resources increasingly are being handled throughout the typical

organization, it is all the more important that management adopt a risk management approach to implementing security measures. This approach requires that three elements be analyzed: the value of assets being protected, the nature and likelihood of threats facing those assets, and the cost-effectiveness of existing or potential safeguards. This does not necessarily dictate the use of highly formal, quantitative risk analysis procedures in all situations, although such procedures are often still appropriate. For a single personal computer application, a less formal, qualitative analysis might well be sufficient. However, for applications involving multiple PCs, networking, or host systems, the analysis would require a considerably more rigorous process.

7.1.5.3. Individual Responsibility

Despite efforts to the contrary, users of large, centralized ADP applications seldom consider themselves individually responsible for the security of those systems. With personal computers, users (and their management) can no longer avoid those responsibilities. Therefore, it is important for management to ensure that policies and procedures are made clear to all personnel and that necessary resources are provided to enable compliance.

7.2. A PLAN OF ACTION

No "cookbook" approach to information security can be provided for managers and users of personal computers. However, the following is a recommended plan of action that may at least get the process started.

7.2.1. ESTABLISH AN INFORMATION SECURITY POLICY

A formal information security policy (not a **computer** security policy) is a prerequisite to a workable security program. This requires, at a minimum, identifying the types of information requiring protection (e.g. personal, trade secret, etc.) and specifying the control measures which apply to each type of information (e.g. storage, transmittal, disposal) . If such a policy exists, then **all** information in the organization -- not just that in a specific format (e.g. paper) -- will be addressed in a consistent manner.

Many organizations have security policies which apply to traditional (e.g. hardcopy) documents. In general, these policies need only be reviewed and, where necessary, modified to include information in other forms, such that residing on magnetic media. This again, makes the "electronic desk" concept a useful analogy.

7.2.2. DEVELOP AN INVENTORY OF APPLICATIONS

Most organizations in which personal computers are used find quickly that it is useful, indeed necessary, to maintain an inventory of equipment and software. Similarly, it is important to develop an inventory of "applications". Each component should attempt to identify various applications and the associated information processed on the components computer systems. For personal computers, it may be easiest to start with each hardware system and document the following:

- System identification, location
- Responsible user (i.e. the "owner")
- Other Users
- General categories of sensitive information handled
- Specific, identifiable applications
- General description of access controls and other security measures currently in place

This is the first step in developing an understanding of the extent of any potential security problems and needs.

7.2.3. CONDUCT A RISK ASSESSMENT

The previous step will provide an overall assessment of basic risks. For those systems or applications which process sensitive or critical applications, a more detailed assessment of risk should be performed. The risk assess process was described earlier.

7.2.4. SELECT CONTROL MEASURES

For those systems or applications for which risks are determined to be unacceptable, additional control measures must be implemented. In general, such controls will fall into one the following categories.

- Physical Protection - As noted earlier, traditional physical control measures (e.g. locks) will prove to be the most cost effective approach.

- Administrative Procedures - Policies and procedures will play a significant role in the control structure.

- Self-Developed Software - In many cases, simple programs or automated procedures ("batch files") can be used to provide a controlled environment for users. It may also prove worthwhile to make certain modifications

to the operating system or key application programs to provide additional access controls.

- o Commercial Security Products - In addition to all the steps described above, management will find a growing number of security-enhancing products available on the commercial market. Some of these were described in earlier sections of this report, and an outline of several types of such products may be found in Appendix C.

Since the "basic" personal computer generally provides very little in the way of security mechanisms, it is the user's responsibility to provide whatever controls deemed necessary. There may be a temptation to favor the fourth category above (commercially available products). It is important to note, that security cannot be achieved simply by installing gadgets. Without physical and administrative controls, such devices can usually be circumvented will little effort.

When considering technical security products (e.g. access control packages, password schemes, etc.), an additional caution is appropriate. Because of the two fundamental security weaknesses of personal computers which were discussed earlier, (i.e. physical accessibility and lack of hardware security mechanisms), users should be wary of claims for products (particularly software) which claim to provide "absolute" security. Without certain physical controls and limits on what users are permitted to do once in the system, such claims are meaningless.

7.2.5. AUDIT AND MONITOR THE RESULTS

After selecting and implementing appropriate security measures for personal computer systems (and, it is hoped, other information systems), management should conduct some type of post-implementation review and subsequent periodic audits. This is needed to ensure that control measures are, indeed, in place and operation and that they remain appropriate as the organization and its information environment change.

7.3. OPPORTUNITIES

Despite the potential problems, one should not be left with the impression that personal computers represent unreasonable security risks. It should be clear that the benefits of personal computers will continue to outweigh most perceived risks, and, therefore, personal computers will continue to be introduced at a rapid pace. Indeed, it is possible to minimize most of the risks

discussed above. In addition, there are some unique security advantages offered by personal computers.

7.3.1. USING EXISTING SECURITY TECHNOLOGY

Most control measures that have been used for large scale systems (e.g. administrative controls, separation of duties, physical and environmental controls, etc.) apply equally to personal computers. The primary difference is one of scale; it is difficult to justify an expensive access control system for a single personal computer. On the other hand, simple physical controls, such a lock on the door or the equipment itself, can be both cheap and effective. Similarly, since relatively few people must share data on a given machine, the controls over data access can be relatively simple (e.g. keeping sensitive data on removable diskettes or selective encryption of such files).

New microprocessor technology will continue to provide personal computers with more of the hardware features previously available only in larger systems (e.g. virtual memory addressing and multiple processor states). This, too, will enable current security technology to be applied to smaller systems.

7.3.2. ISOLATING SENSITIVE SYSTEMS

A unique opportunity offered by the relative low cost and availability of personal computers is the ability to isolate completely a particularly sensitive application. Rather than applying strict controls over every user of a large multi-user system, it may be less expensive and more effective to implement a sensitive application on its own dedicated hardware. This offers isolation and security without the usual overhead necessary in a resource-sharing environment.

7.4. SUMMARY

This report has discussed some of the security issues that must be addressed by any organization using or contemplating the use of personal computers. There are, of course, many other areas relating to personal computers and information security in general which have not been discussed. The reader should refer to Appendix A for additional publications on these topics.

Personal computers offer tremendous opportunities for improved productivity, and their introduction into the office environment will continue to grow. It would be hopeless (indeed, counter-productive) for the over-zealous auditors or security officers to attempt to stop this process. However, this does mean more

people and more points of potential security exposure with which management must deal. These are not insurmountable problems, but they do require a extra degree of special attention and creativity on the part of both management and users.

7.5. WHERE TO FIND ASSISTANCE

Despite its special dimensions, the security of personal computer systems is just an extension of the overall problem of information security. As such, these security concerns often can be addressed through existing resources, including an organization's own data security group, professional organizations, consultants, trade publications, and professional literature.

The National Bureau of Standards, Institute for Computer Sciences and Technology (ICST) provides guidance to Federal agencies and the private sector on a broad range of data security issues. This takes the form of Federal Information Processing Standards (FIPS) and guidelines, special research publications, and various cooperative efforts. Several ICST publications on information security are listed in Appendix A.

A. REFERENCES

AFCC83 Air Force Communications Command. A Small Computer Security Handbook. Data Systems Design Center, Gunter Air Force Station, AL. Jul 21 1983, pp16.

BOUNW83 Bound, William A. J. "Securing the Automated Office". Computer Security Journal, Fall-Winter 1983, pp97-103.

DUFFT81 Duffy Jr., Thomas F. and Lee, Ronald G. Micro Computer Audit Workprogram. Graduate school paper. California State Polytechnic University, Pomona, CA. Jan 1981.

FIPS31 Guidelines for Automatic Data Processing Physical Security and Risk Management. National Bureau of Standards. Feb 1974.

FIPS38 Guidelines for Documentation of Computer Programs and Automated Data Systems. National Bureau of Standards. Feb 1976.

FIPS39 Glossary for Computer Systems Security. National Bureau of Standards. Feb 1976.

FIPS41 Computer Security Guidelines for Implementing the Privacy Act of 1974. National Bureau of Standards. May 1975.

FIPS46 Data Encryption Standard. National Bureau of Standards. January 1977.

FIPS65 Guidelines for Automatic Data Processing Risk Analysis. National Bureau of Standards. Aug 1979.

FIPS73 Guidelines for Security of Computer Applications. National Bureau of Standards. Jun 1980.

FIPS83 Guideline on User Authentication Techniques for Computer Network Access Control. National Bureau of Standards. Sep 1980.

FIPS87 Guidelines for ADP Contingency Planning. National Bureau of Standards. Mar 1981.

FIPS88 Guideline on Integrity Assurance and Control in Database Administration. National Bureau of Standards. Aug 1981.

FIPS101 Guideline for Lifecycle Validation, Verification, and Testing of Computer Software. National Bureau of Standards. Jun 1983.

Appendix A

FIPS102 Guideline for Computer Security Certification and Accreditation. National Bureau of Standards. Sep 1983.

GELLS83 Geller, S.B., Care and Handling of Computer Magnetic Storage Media. NBS Special Publication 500-101. National Bureau of Standards, June 1983.

GRANP83 Grant, Peter; Riche, Robert. The Eagle's Own Plume. U S Naval Institute Proceedings. Jul 1983, pp29-34.

HANSJ83 Hansen, James V. "Audit Considerations in Distributed Processing Systems". Communications of the ACM. Aug 1983, pp562-69.

HECHM84 Hecht, M, et al. Microcomputers: Introduction to Features and Use. NBS Special Publication 500-110. National Bureau of Standards. Washington, DC. March 1984.

HIGHH84 Highland, Harold Joseph. Protecting your Microcomputer System. John Wiley & Sons, Inc., New York. 1984, pp38-42.

KINGM83 King, Martin J. "Microcomputers - The Central Support Approach". EDPACS. Dec 1983, pp1-4.

MAIRW72 Mair, William C.; Wood, Donald R.; and Davis, Keagle W. Computer Control and Audit. Institute of Internal Auditors. Altamonte Springs, FL. 1972.

MURRW83 Murray, William H. "Good Security Practices for Personal Computers". Computer Security Journal. Fall/Winter 1983, pp77-83.

MURRW83A Murray, William H. "Good Security Practices for Dial-up systems". Computer Security Journal. Fall/Winter 1983, pp83-88.

PERRW83 Perry, William E. "Auditing the Small Business Computer". EDP Auditor Update. Sep/Oct 1983, pp7-8.

PRICW83 Price Waterhouse. Microcomputers: Their Use and Misuse in Your Business. Price Waterhouse. Jan 1983, pp31.

SCHAT83 Schabeck, Timothy A. Managing Microcomputer Security. Computer Protection Systems Inc., Ann Arbor, MI. Jul 1983.

STEID84 Steinauer, Dennis D. Security in Small Computer Systems. Auerbach Publishers Inc. 1984.

STEID84A Steinauer, Dennis D. "Security of Personal Computers: A Growing Concern". Computer Security Journal. 1984.

VONGP83 Von Glahn, Peter G.; Farber, David J.; Walker, Stephen T. The Trusted Office of the Future. University of Delaware. Newark. Oct 24 1983.

Note: Federal Information Processing Standards (FIPS) publications are available from the National Technical Information Service, Springfield, VA 22161. NBS Special Publications are available from the Government Printing Office, Washington, DC 20402.

B. PERSONAL COMPUTER SECURITY SELF-AUDIT QUESTIONNAIRE

Evaluation of information security risks is often a complex process. Risk are dependent upon many factors, including the sensitivity and criticality of the information involved and the operational environment (physical, organizational, technical, and otherwise). It is not a situation that lends itself well to checklists or other "cookbook" approaches.

Nevertheless, it is often helpful for an individual manager or user to conduct a relatively simple self-audit of potential information security risks. This questionnaire is intended to assist managers to conduct such an informal self-audit. The questions are intentionally general in nature, since the adequacy of control measures is dependent on many factors that cannot ignored, including the operational requirements and sensitivity of information on each system. In situations where a personal computer is used for a relatively well defined and understood set of applications, this self-audit process may provide a good evaluation of the associated risks. However, if the personal computer is part of one or more larger applications (e.g. part of a network, the questionnaire must be used with care.

It generally will not be possible to answer each question for the organization as a whole. If this were done, the honest answers would always be "no". Questions must be addressed to individual systems or organizational components. It should also be noted that this is by no means a comprehensive list of issues that should be addressed. No attempt has been made to include a list of traditional data security and integrity control practices that should be considered regardless of the nature or size of equipment involved. The reader is referred to Appendix A for additional information on such topics. This questionnaire is only intended as a starting point.

ORGANIZATIONAL AND POLICY

Are there organizational policies and procedures which address the handling of sensitive and proprietary information?

Are the procedures for the protection of sensitive information handled on PC consistent with those for other types of sensitive information in the organization?

Are policies regarding personal use of PC equipment and software clearly stated?

USER AWARENESS AND TRAINING

Are users provided with adequate training and awareness of organizational information security policies and their individual responsibilities?

In each of the areas discussed in this questionnaire, are users provided adequate training in the performance of required procedures and the use of necessary equipment or systems?

PHYSICAL AND ENVIRONMENTAL PROTECTION

Is equipment provided with adequate protection from theft, damage, and unauthorized use?

Is electrical power quality satisfactory? If not, are surge suppressers or other power quality enhancement equipment used?

Are temperature and relative humidity maintained within acceptable limits?

Is equipment protected adequately form airborne contaminants (smoke, dust, etc.)?

CONTROL OF STORAGE MEDIA

Are there procedures for external labeling of sensitive materials?

Are there adequate storage facilities for security sensitive media (hardcopy, removable magnetic media, etc.)?

Are there procedures to ensure the proper handling and storage of magnetic media (to minimize physical or magnetic damage)?

Are there procedures for the proper disposal of sensitive media (e.g. shredding of paper, degaussing of diskettes, etc.)?

DATA AND SYSTEM INTEGRITY

Is common-use (shared) software protected from undetected modification?

In situations where important decisions are based on data produced by a PC, are there adequate procedures to validate results?

Are users provided with adequate training in the use of the software tools they are using?

Are major PC application systems subjected to formal system development controls?

SYSTEM AND DATA ACCESS CONTROLS

If a system is intended for use only by specific users, are there adequate methods (physical or otherwise) to prevent unauthorized use?

If there are multiple users of a system using a fixed disk, are there adequate mechanisms to provide needed file access control?

If access control hardware or software is used:

-Is the user interface sufficiently constrained to prevent users from circumventing the control mechanisms?

-Is there a method to prevent users from using an unauthorized copy of the operating system?

If cryptography is used, are there adequate key selection and management procedures?

Are users provided with utilities (and training) to overwrite sensitive disk files or system memory?

CONTINGENCY PLANNING

Are there adequate procedures and equipment for handling emergency situations (e.g. fire, flooding, emergency evacuation, bomb threat, etc.)?

Are routine backup procedures for data and software adequate for the sensitivity, criticality, and volatility of such information?

Are critical materials (i.e. data, software, equipment, documentation, etc. needed for backup operation) stored and available at offsite or otherwise safe locations?

Are there formal plans for the backup operation of critical functions and for eventual recovery from contingency situations?

Is readiness to respond to contingency situations tested and reviewed periodically?

AUDITABILITY

If audit trails are needed for a PC application, is the user interface sufficiently constrained to prevent unauthorized modification or destruction of audit trail data?

PC TO HOST CONNECTIONS

Are measures taken to prevent the practice of storing sensitive host logon information (e.g. passwords) in PC terminal emulation software? If not, are such PC systems provided with adequate controls to prevent unauthorized access (and thereby access to associated host systems)?

If a PC is used to prepare and pre-edit transactions for submission to a host-based system, are there redundant edits and audit trail mechanisms at the host to protect against corruption of transactions prior to receipt at the host?

Are host system security mechanisms adequate to:

-Prevent unauthorized access to system facilities and data?

-Monitor and, if necessary, limit the type and volume of data that may be downloaded to a remote device?

PC NETWORKS

If PC systems are connected to a local area network and there is a requirement for message security, are there adequate cryptographic or other communications security measures.

If a PC is accessible for remote use, are there adequate user identification and authentication mechanisms in the PC to prevent unauthorized access?

MISCELLANEOUS ISSUES

Is there adequate monitoring, control, and accountability of PC equipment and software?

Are there policies and procedures to monitor and control the use of PC related devices, software, and supplies?

Are there procedures to ensure compliance with licensed software and proprietary information protection agreements?

C. PERSONAL COMPUTER SECURITY PRODUCTS

The basic personal computer often has little in the way of protection features. Those users with specific security needs must first determine an acceptable balance between the risk they face and the cost of additional control measures. The main body of this report has described the types of control measures that should be considered. This appendix provides an outline of several types of commercially-available products which can provide additional protection in several areas. This list focuses on products designed specifically for personal computers and does not include other security and environmental control products such as locks, fire detection and suppression equipment, alarm systems, shredders, and a wide range of other products and services.

This list describes only types of products that are available, rather than listing specific vendors or products by name. It should also be noted that the mention of a specific type of product does not imply any direct or indirect endorsement by the National Bureau of Standards.

PHYSICAL ACCESS CONTROL AND THEFT PROTECTION

Products in this category provide physical protection of equipment from damage, theft, and general physical access. Therefore, they also provide a first line of control over system and file access.

- Lockable equipment enclosures and workstations
- Equipment lockdown devices
- Power switch locks
- Equipment cabinet or enclosure locking devices
- Equipment removal detection devices

ELECTRICAL POWER QUALITY CONTROL

This class of product provides protection from variations in electrical power which could damage or impair the reliability of equipment.

- Surge suppressers
- Power "conditioning" systems
- Uninterruptible power supply (UPS) systems

ENVIRONMENTAL PROTECTION

These products are intended to maintain acceptable environmental conditions for equipment.

- Fire detection and suppression equipment
- Water detection alarms
- Temperature and relative humidity monitors
- Dust covers
- Static mats, sprays, or grounding devices
- Dust filters, fans, etc.

MAGNETIC MEDIA PROTECTION

- Lockable storage devices
- Color coded labels and jackets
- Protective containers and mailers
- Degaussing and destruction equipment
- File encryption systems

SYSTEM AND FILE ACCESS CONTROL

This category of product provides user control over access to system facilities or individual files and programs. User identification and authentication may also be provided.

- User Authenticators - devices or software to require users to identify themselves before access to the system is granted. These usually require the entry of a password to gain access.

- Card or badge readers - devices which read information from magnetically coded cards (e.g. credit cards) for entry to the system and use for access control decisions.

- Authentication code devices - devices which work in conjunction with system software to generate a session-unique authentication code to be input by the user.

- File access control systems - modifications to operating system service routines which limit which files or directories a user may access.

- Port protection devices - devices which control remote access to a system. These devices normally are inserted between the computer system and modem. They require remote users to provide user authentication (usually a password or code). Some systems provide a call-back option in which the line is disconnected, and

the user is called back at a pre-determined telephone number.

CRYPTOGRAPHIC SYSTEMS

These products use cryptographic protection for various operational requirements. Cryptographic systems may have any or a combination of the following characteristics or features:

- Hardware or software implementation of the cryptographic algorithm.
- Hardware or software implementation of supporting functions.
- Private or public key cryptographic approach
- Automatic or manual key generation, entry, storage, and distribution.
- Proprietary or public (e.g. DES) algorithms.

It should be noted that some of the products listed under System and File Access Control also use cryptographic protection.

- General purpose cryptographic facilities - hardware or software that provides basic crypto functions (set key, encrypt, and decrypt). Users must build specific applications around these products.
- Bulk file encryption utilities - programs which enable a user to encrypt or decrypt a specified data file. The user normally is required to enter the cryptographic key. Some systems act directly on the original file (thus destroying its original contents), while other systems produce a separate file (requiring use of an overwrite utility to prevent access to the original file).
- Integral disk encryption systems - usually hardware and software that causes all disk write (or read) operations to be encrypted (decrypted), thus eliminating cleartext on disk while not changing the application interface.
- Communications encryption systems - devices which provide integral communications and cryptographic facilities to enable secure communications among PC systems.

MISCELLANEOUS

- System Utilities - software designed to enable use of write-protect, "hide" files, and other system facilities which can be used for additional protection.

- CRT Privacy Screens - covers for CRT screens which limit screen viewing to a narrow angle of view, normally sufficient only for the user.

INDEX

☆U.S. GOVERNMENT PRINTING OFFICE: 1985-461-105/10184

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NBS/SP-500/120	2. Performing Organ. Report No.	3. Publication Date January 1985

4. TITLE AND SUBTITLE

Computer Science and Technology:
Security of Personal Computer Systems: A Management Guide

5. AUTHOR(S)

Dennis D. Steinauer

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

National Bureau of Standards
U.S. Department of Commerce
Gaithersburg, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

National Bureau of Standards
Institute for Computer Sciences and Technology
Center for Programming Sciences and Technology
Gaithersburg, MD 20899

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number:84-601156

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

This document is a security guide for managers and users of personal computer systems. It describes the nature of information security problems involved in the use of personal and other small computer systems and provides guidance for addressing those problems.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

access control; auditability; backup; computer security; contingency planning; cryptography; microcomputers; office automation; personal computers; small computers.

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

66

15. Price

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SCIENCE & TECHNOLOGY

Superintendent of Documents,
Government Printing Office,
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Bureau of Standards Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NBS Technical Publications

Periodicals

Journal of Research—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent Bureau publications in both NBS and non-NBS media. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).
NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.
Order the **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*
Order the **following** *NBS publications—FIPS and NBSIR's—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Bureau of Standards
Gaithersburg, MD 20899