


✓

[illegible]

•

Foreword

The Committee on Integrity and Management Improvement (CIMI) developed this leaflet for all EPA employees who depend on microcomputers to perform their jobs. As a followup to CIMI Computer Advisory 89-1 (June 1989), this leaflet addresses threats and vulnerabilities involving microcomputer security with emphasis on the individual's increasing role in safeguarding microcomputer equipment. The Agency has spent millions of dollars on computer hardware to enable employees to work efficiently and effectively, and each of us has a responsibility to protect these investments. The guidelines in this leaflet should be useful in this effort, but are not intended to be all inclusive. Specific local conditions or changing technology may warrant additional security measures.



John C. Martin
Chairman, Committee on Integrity
and Management Improvement
Environmental Protection Agency

Background

EPA uses thousands of microcomputers to track various types of data. More and more microcomputers/terminals are either networked together or connected to a mainframe sharing data, information, software, and operating systems, all capable of accessing vast quantities of data. As a result of this ease of access, threats and vulnerabilities to computer resources are increasing. EPA, like other Federal agencies, is concerned about unauthorized and illegal activities, e.g., unauthorized access to privacy, proprietary, or other sensitive records; use of computers for personal use; and inadvertent errors and omissions. All of these activities revolve around the accountability and responsibility of the individual user.

Computer crime losses alone cost billions annually. While deliberate computer crime is a significant concern, wasteful and abusive practices, accidents, and errors by individual users are even more prevalent. Nationally, employee-committed crime, waste, and abuse account for an estimated 70 to 80 percent of the annual loss related to computers. These factors underscore the seriousness of computer-related losses. They also explain why additional regulations and legislation are being developed to ensure that adequate safeguards are provided and that actions are taken to prevent further unauthorized activities.

Computer Security: Threats and Vulnerabilities

Computer security has many threats and vulnerabilities involving the individual user. A threat is any activity, deliberate or unintentional, with the potential for causing harm to an automated information system. Power surges are greater hazards to a personal computer (PC) than to a computer terminal. Programs, data files, or Random Access Memory contents can be damaged or an entire disk rendered unreadable. Protecting power lines is essential for critical PC systems' operations.

Threats may be intentional or accidental acts of behavior that can cause harm to automated information systems, e.g., improper handling of source documents, tapes, disks, and printouts; data alteration; operator error; and disgruntled employee access. Generally threats originate from personnel who come in contact with the system on a daily basis. Threats are frequently man-made and disguised as computer codes embedded in computer programs (also known as "viruses") or implanted into computer systems by hackers, who are capable of either destroying or denying service of computer assets such as data, hardware, software, and communications. In almost all instances, the individual user is responsible for the computer related threat which

computer resources. Computer security threats are threats to these assets. Computer security vulnerabilities are the computer weaknesses that can cause harm to computer resources, such as software, hardware, data, and communications. Together, these threats and vulnerabilities can impact computer resources through:

Destruction — computer equipment or program software is totally lost or damaged;

Disclosure — sensitive data or personal information protected by the Privacy Act is divulged to an unauthorized recipient;

Modification — a program application or stored data becomes altered or damaged due to input error or unauthorized access;

Denial of Service — assets exist but cannot be accessed or used for a period of time; and

Misappropriation — assets are used dishonestly or illegally.

The following sections address some major types of computer security related vulnerabilities/threats and the potential impact on computer resources. Recommended safeguards, controls, and countermeasures are listed for each security type.

General

Regardless of the nature of the threat or vulnerability, certain standard security measures should always be followed. These include:

- limiting access to authorized users;
- keeping all software and equipment in secured/locked facilities;
- guarding against power surges by using protective devices such as surge suppressors; and

- developing and implementing policies and procedures regarding proper operating practices and preventive maintenance

Software Security

Software security is the prevention of deliberate or inadvertent unauthorized manipulation of computer programs. Threats and vulnerabilities entail program errors, unauthorized automated routines, and inadequacies/flaws in system software which are sometimes obtained through "bulletin boards," enabling unauthorized access to hardware, data or programs.

Probably one of the most dangerous threats that has surfaced in recent years is the "virus." A computer virus is a program that contains instruction codes to attack ("infect") other software programs by modifying them to include a copy of itself. With this "infection" capability, viruses can spread from program to program, computer to computer, and network to network, corrupting programs and data. Microcomputers, mainframes, and worldwide computer networks are all being infected. Because a virus can carry other program codes along with it, the nature of the damage it can do is limited only by the creativity of the attacker. Viruses can even reinfect programs that have been cleaned up, thus surviving many generations of program changes. Even the most thoroughly verified program can become infected again. A single programmer with a PC can cause computer problems anywhere, anytime. Examples of viruses are:

Trap Door — a set of instruction codes embedded in a computer operating system that permits access while bypassing security controls

Trojan Horse — an unauthorized individual who gains entry into a computer system through hidden codes, also capable of disguising its format, putting up messages,

- use write-protect tabs to prevent programs/data from being overwritten inadvertently
- make backup copies and store in a secure place
- use automatic backup features built into software programs.
- use a software management tool that allows authorized users access to modify code
- the LAN Administrator should periodically run a virus detection software package to detect viruses; and
- report anything unusual or out of the ordinary as soon as possible

Hardware Security

Hardware (physical) security involves protecting and controlling electric, electronic, and mechanical equipment used for processing data, e.g. PC's, monitors, data terminals, minicomputers, etc. The scope of physical security has broadened in an effort to restrict access to authorized users to prevent untrained or malicious individuals from damaging or making inappropriate use of computer resources.

Recommended safeguards to ensure physical security are:

- restrict modifications and maintenance to authorized/properly trained personnel,
- ensure employees know who is cleared for access and can identify them on sight,
- question strangers,
- prohibit smoking, drinking, and eating in the immediate vicinity of the microcomputer equipment,

- assure that there is a fire protection system within the rooms where microcomputer equipment is used
- develop and maintain an inventory of hardware;
- restrict access to a PC or workstation when it is unattended by requiring a password to be entered when first powering up the system; and
- restrict access to a PC or workstation by using a screen saver that requires a password to be entered to exit the screen saver

Information Security

Information security revolves around safeguarding the processes of data origination, input, processing, and output. The purpose is to ensure that adequate controls are maintained to assure the accuracy and integrity of information, and that it is protected from unauthorized access, destruction, modification, and disclosure.

Computer-related theft, fraud, and abuse involve such activities as data diddling — changing information at the time of input into the computer or during output (forging documents, exchanging valid disks, or falsifying data upon input); and browsing — looking in others' files without authorization, searching through trash containers to find passwords to gain access to computer files, and literally looking over one's shoulder.

Theft of information in the microcomputer area commonly involves copying or using software programs for personal and/or personal business use.

To ensure data integrity:

- use software, hardware, and procedural controls to restrict access to on-line files to authorized users;
- develop, document, and implement procedures for identifying, correcting,

data. The following are some of the steps that users should take to protect their data and the system:

- develop and implement step-by-step procedures that users should take when operating a computer system
- position monitors so people will minimize unattended viewing
- label and store in a secure location any floppy disk containing sensitive data
- erase data from a data commonly referred to as "wiping" from a hard disk before allowing it to be re-used for the purpose of being replaced or sent out of the building to the trash can
- use additional software to track system procedural controls on the systems identified as containing sensitive data of Local Area Network (LAN) systems and
- avoid storing sensitive data on LAN servers and do not connect them to organization's main frame

Also, users need to be aware that simply erasing a file with the `DEL` or `ERASE` command does not prevent a user from recovering the erased data. There are many file recovery utility programs available that can find, track and/or overwrite the file again. Another alternative is to reformat the disk and format the disk.

Personnel Security

People are the most serious threat to computers and automated information. The unintentional errors people commit occur more frequently and cause more costly damage than do deliberate acts of sabotage. Unwittingly, people enter incorrect data into the computer or erroneously alter data. It is important to remember that all security measures are vulnerable to users who have legitimate access. The internal personnel security is to ensure that employees know

information security requirements and are aware of their responsibilities. The primary mission is establishing and maintaining an ethical, technically proficient, informed, and trusted work force.

Thefts which occur are generally intentional; however, thefts can occur unintentionally, e.g., when an employee copies licensed software to use on his/her home computer and does not realize it is a violation. Employees need to be aware that this is a serious copyright violation and could result in a \$100,000 fine. Common abuses include using computers for personal business; browsing through records; preparing personal-use software programs; and creating team rosters, scores, and handicaps for sports-related interests. Abuses such as these are a violation of the Standards of Conduct and can result in disciplinary action. Federal property (including property leased by the Government) cannot be used for other than official business.

Studies have revealed that the majority of computer violations are carried out by authorized users, not outsiders. It is believed that a well-trained employee is one of the most effective safeguards against a threat or vulnerability to personnel security.

It is estimated that 50 to 80 percent of the problems incurred with automated systems are due to lack of employee training and development of skills. To ensure adequate personnel security:

- alert employees to the organization's information security policies and the individual's own responsibilities within the agency through information security training;
- publicize procedures for reporting security violations and irregularities;
- inform staff that unauthorized duplication and use of licensed software violates the law.

- indoctrinate new employees on their ethical responsibilities.
- require personnel to sign a statement that they understand their information security responsibilities.
- maintain close and effective communications with your staff; and
- incorporate computer security compliance into job performance standards

Microcomputer Security Reminders

Maintaining Your Disks

Computer disks are fragile and should be safeguarded as follows: 1) store in protective jackets; 2) protect from bending; 3) do not touch window area of disks; 4) prevent erasures by keeping disks away from magnetic sources such as radios and telephones; 5) store in secure containers, such as metal cabinets, protected from fire and water damage; and 6) handle disks according to their security markings.

Eight Common Don'ts

- Don't smoke or have food or beverages near the computer.
- Don't leave the computer on and unattended.
- Don't use the computer for personal business.
- Don't have automated information in only one place—back it up.
- Don't copy licensed software packages and don't use copies someone else has made.
- Don't treat all automated information the same. Know what needs to be secured and do what needs to be done.

[illegible]

Conclusion

Microcomputers are not a serious problem and responsibility. Because of the PC's intelligence capability and programmability, its local storage capability, its hardware and software configurability, and its ability to accommodate various peripheral devices, it is not hard to find that any type of security system can be easily designed to utilize and maximize the PC hardware and software using the following program. In addition, it is important to know that the computer programs are not the only product that can be used to protect the information. It is very important to have a good understanding of the computer system and its components, and to have a good understanding of the computer system and its components, and to have a good understanding of the computer system and its components.

[illegible]

U.S. Environmental Protection Agency
Region 5, Library (PL-12J)
77 West Jackson Boulevard, 12th Floor
Chicago, IL 60604-3590