PN-ABG-422

68863

COMPUTER SECURITY AWARENESS

A.I.D. WORKSHOP, 1989

COMPUTER SECURITY AWARENESS SEMINAR

TABLE OF CONTENTS

LETTER TO STUDENT 1

INTRODUCTORY THREAT SCENARIO 3

INTRODUCTION 4

- Factors Affecting the Spread of Security Problems 4
- Security Regulations 6

SEMINAR OBJECTIVES 7

- Measurable Objectives 8

DEFINING THREATS AND VULNERABILITIES 10

- Basic Security Terms 10
  - Assets in an Automated Environment 11
  - Vulnerabilities 13
  - Understanding Threats 15
    - External/Internal Threats 16
    - Environmental Threats 18
    - Technical Threats 19
  - Impact on Computer Resources 21
  - Preventive Measures 22

BASIC SECURITY POLICIES AND PRACTICES 23

- Countermeasures 23
- Physical Security Measures 24
  - Security of Operational Environment 24
  - Security of Storage Media 27

Environmental Controls 28
Data/Information and Software Security 31
Information Security Measures 32
Password Security Procedures 34
Password Protocols 36
Data Security and Integrity 39
Software Security 41
Administrative/Procedural Security 43
Communications Security 45
International Communications System (ICS) 45
Personnel Security 46
A.I.D. SPECIFIC SECURITY PROCEDURES AND POLICIES 48
Roles and Responsibilities of Security Personnel 48
Management Responsibilities 49
Operational Responsibilities 49
Systems Security Officer (SSO) 50
Systems Manager (SM) 51
User Responsibilities 52
A.I.D. Specific Administrative Controls 53
Log and Record Keeping 53
IDs For Visitors 53
System Maintenance Procedures 54
Extended Operations 54
Microcomputer Security 55
COMPUTER RELATED CRIME AND ABUSE - STRATEGIES FOR PROTECTION 57

What is a Computer Virus? 57
What can a Virus do to your System? 59
How Does a Virus Spread? 60
Trojan Horses and Other Methods of Spreading Viruses 61
How Great Is Your Exposure? 62
Strategies for Protection 63
Avoiding Viruses 63
Detecting Viruses 65
Getting Rid of Viruses 66
RISK ANALYSIS AND CONTINGENCY PLANNING 68
Analyzing Risks 68
Making Contingency Plans 69
KEY POINTS TO REMEMBER 72
CROSSWORD 73
APPENDIX .....
Glossary i
Recent Occurrences of Computer Viruses vi
Bibliography vii

LETTER TO STUDENT

Dear Student,

This is your class guide to effective security practices and procedures. This guide should be used *in conjunction with* other security related documentation for your computer systems, and the A.I.D.Automation Security Guidebook.

We believe that learning is an *active* process and this belief is expressed in our curriculum design.

The workbook contains an outline of the topics covered in this course. It also contains exercises which you will be performing in class and that we recommend you review after class.

This workbook is not intended to be used as a stand-alone tutorial. Thus, we have not included every single detail in a particular process. The workbook was designed to be used *along with the instructor*, who will clarify concepts and provide additional information.

We require that you listen, think, try out the exercises in class, and, hopefully, as a result, understand them.

Your time in class is the perfect opportunity to *ask questions*. We also suggest that you write notes in the workbook and use class time to clarify any questions you might have.

Through a combination of the components listed below, we will help you understand the basic issues in computer security and utilize them in your daily work:

- Expert instruction
- Workbook
- Situation simulations, case studies and other exercises
- Your own effort

The *instructor*, the *workbook*, and you, the *student*, must work together actively to complete the learning process. This triumvirate forms a system in the same way that the individual components of a computer form a system.

When you leave class *you* must spend time reviewing class topics and practicing them, otherwise you will not retain very much of what you learn in this course.

We hope you enjoy this learning experience and welcome your constructive comments.

Sincerely,

The Staff of Future Enterprises

Note: You may notice as you go through this workbook that the bottom of each page includes a revision date and that all pages may not have the same revision date. For example, one page may have been revised on August 25, 1988 and another page may have been revised on September 16, 1988. A later date simply indicates that the information on that page has been updated.

Introductory Threat Scenario

Take a few minutes to read the following scenario. Then attempt to answer the questions listed below. We understand that you may not have all the answers at this point. The idea is to establish the context for the seminar and to start introducing the relevant terms.

> *In the Fall of 1987, hackers in West Germany broke into the NASA computer network. This network contained technical information from space shuttle flights that allowed scientists and engineers in various universities and research centers to quickly send or receive technical data from space flight. Over a four-month period, these hackers were able to manipulate files at will. They reportedly gained access to information by asking the NASA computer for information stored under such key words as "Shuttle," "Challenger," and "Secret". Before they departed the network, they turned loose a virus into the system which destroyed a number of files.*
>
> Excerpt from OPM Security Guidelines

1. What is the threat being described in the above scenario?

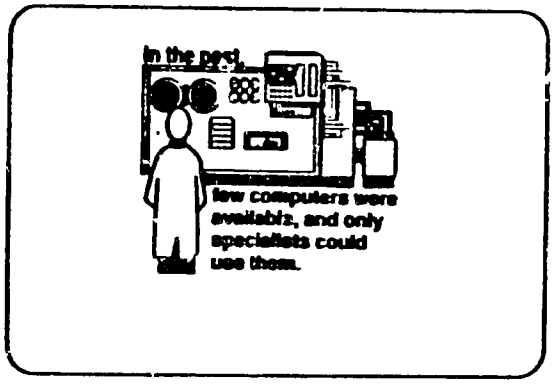
2. What is the impact of this threat to a computer system?

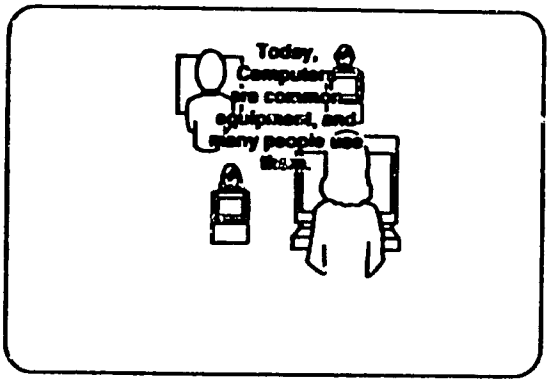
3. What are some of the policies and practices that could have prevented such a threat?

INTRODUCTION

Factors Affecting the Spread of Security Problems

In the early days of computer usage, the need for security was minimal, since the systems were housed in large isolated facilities, and accessed by a very *small number* of specialized people.



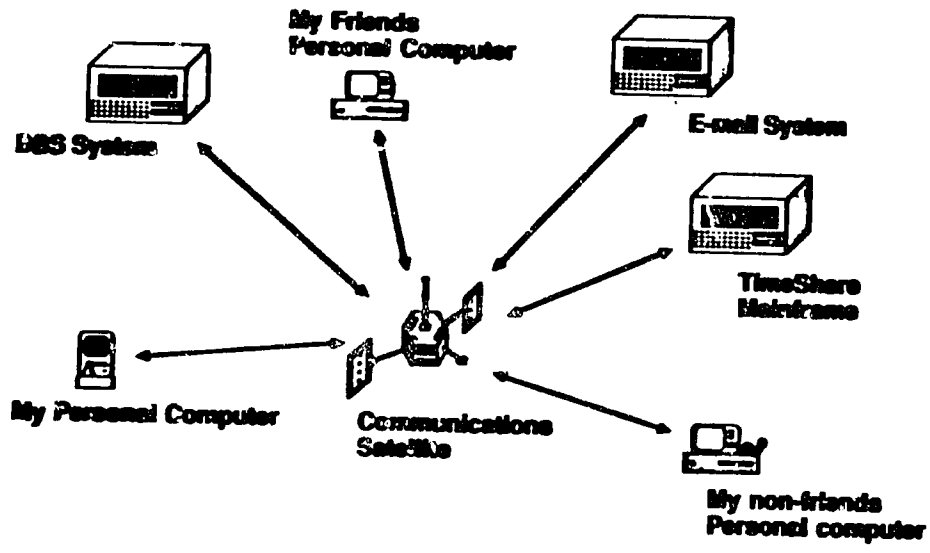


Today, however, a very large number of people depend on computers to get their work done. The *personal computer* has changed the way institutions handle information. Data which was once locked up in file cabinets or stored in mainframes with limited access, is now created, manipulated and shared on every desktop. This certainly fosters greater productivity, but it also creates security problems.

As a result of the *ease of access* to both equipment and information, risks to computer resources have increased significantly. Computer fraud, waste and abuse have become troublesome aspects of the Information Age. With disturbing frequency, computer systems have succumbed to a variety of security violations, including:

- diversion of payment to unauthorized parties
- unauthorized access to sensitive information
- misappropriation and damage of computer resources
- waste and inadvertent errors

Another reason why computer security is becoming a serious problem, and could be catastrophic in the near future, is linked to a recent trend in the development of computers: *connectivity*. Connectivity means people can share data, programs and computers. Unfortunately, it also makes it possible for security problems to spread much further, faster, and easier than it was possible in the past. For example, a vandal could *attack* all the people on a network with the same computer virus program. The figure below illustrates how groups of systems can communicate with each other through a network - thereby spreading viruses and other security problems much further.



In today's environment, it is not unusual for several computers to be linked to one another or to a mainframe, sharing data, information, software and operating systems. This makes it very easy for unauthorized persons to gain quick access to vast quantities of personal, proprietary or sensitive information.

Security Regulations

The increased use of computers and automated technology has created considerable management and security problems. While deliberate computer crime is a significant part of the threat picture, wasteful and abusive practices, accidents, and errors represent approximately 60% of the total computer-related losses.

According to a study conducted by an insurance company, personal computer losses alone reached an estimated $250 million during 1986. Theft and power surges accounted for approximately 75% of these losses. Through proper training, these types of losses can be significantly minimized.

In response to the above security concerns, legislation was introduced in both the 99th and 100th Congresses to provide for *computer security awareness training.* These actions resulted in the passing of the **Computer Security Act** of 1987 (Public Law 100-235). This Act *mandates* periodic training in computer security awareness and accepted security practices for *all* employees who are involved with the management, use or operation of Federal computer systems within or under the supervision of a Federal agency.

It is felt that a major contributor to computer-related losses is the *lack* of security awareness and concern. Such awareness can stop accidents and errors, promote adequate information security controls, and prevent and/or detect computer crime.

COMPUTER SECURITY AWARENESS SEMINAR

SEMINAR OBJECTIVES

Owing to the vast amount of sensitive information stored in today's computers, security is of vital concern. The purpose of this seminar is to provide participants with a basic awareness of computer security, to sensitize them to the need for security practices in the workplace, and to motivate each individual to practice effective security techniques.

The seminar attempts to raise the level of consciousness and provide an overview of all aspects of computer security, including physical, data and personnel security.

The overall seminar goals are to help participants:

Understand the basic concepts of computer security.

Appreciate the significance of implementing effective security procedures.

Become aware of the major threats and vulnerabilities in today's environment.

Be able to establish procedures for maintaining and monitoring security.

Have an overall appreciation of a secure computer environment.

Measurable Objectives

At the end of the workshop you will be able to:

1. Threats and Vulnerabilities

____ Define basic security terms such as assets, threats, vulnerabilities and countermeasures.

____ Identify the various categories of threats present in today's environment.

____ List two examples from each category.

____ Name four ways in which threats and vulnerabilities can impact computer resources.

2. Basic Security Practice and Policies

____ List three physical security measures to safeguard computer assets from theft, physical damage and unauthorized access.

____ Suggest four ways to protect sensitive information from unauthorized access and disclosure.

____ Generate effective passwords to control access to information.

____ List two ways of preserving data integrity to ensure accuracy and completeness.

____ List the four most serious areas of personnel vulnerabilities and suggest countermeasures to remedy the situation.

3. A.I.D. Specific Security Procedures

____ Identify the roles and responsibilities of persons associated with maintaining security.

____ Implement A.I.D. specific security policies, and administrative controls.

____ List user responsibilities in maintaining security.

____ 4. Identify three preventive measures for avoiding viruses.

____ 5. Conduct a risk analysis to assess risks to computer resources.

____ 6. Develop a contingency plan.

____ 7 Explain how an effective computer security program will benefit and support A.I.D. functions and operations.

Note: Security issues dealt with in this course pertain only to *unclassified* information, which may still be sensitive, but not classified. It is important to be aware that just because information is not classified does not mean that it is not sensitive. All classified documents are processed through TEMPEST machines. Each office has its own security procedures for protecting *classified* information.

Course Format

The course will be taught in a lecture/discussion format. Students will have ample opportunity to process what they have learned through situation simulations, case studies and other exercises.

Take the time to do the exercises interspersed throughout the courseware. These *short-delay recall exercises* are really another teaching strategy since they reinforce the learning experience by representing the knowledge in another way. Such exercises reinforce the learning experiences by providing an opportunity to practice with tentative knowledge. This helps in retaining knowledge for longer periods of time so that it can be applied to work related problems.

DEFINING THREATS AND VULNERABILITIES

In this section we will introduce you to some of the basic terms associated with computer security, and review the threats and vulnerabilities present in today's automated environment. We will also examine how these threats affect computer resources, and discuss the importance of implementing proper security measures.

Basic Security Terms

In order to understand and implement computer security policies and procedures, it is important to become familiar with certain basic terms such as:

- Assets
- Vulnerabilities
- Threats
- Safeguards, countermeasures and controls

Assets are the hardware, software and information present in an automated environment. *Threats and vulnerabilities* are the flaws and weaknesses that damage, endanger, or pose a risk to assets, and *countermeasures* are the steps taken to minimize vulnerabilities and protect against threats.

The rest of this section is devoted to an elaboration of the first three terms listed above, with particular emphasis on threats and vulnerabilities and how they impact computer resources. Countermeasures or safeguards to counteract these threats and vulnerabilities will be discussed in the next section.

Assets in an Automated Environment

In an automated environment, how would you define assets?

An asset is defined as:

> *any software, data, hardware, administrative, physical, communications or personnel resource within an information system or activity.*

Assets could take the form of one or more of the following:

- Information
- Hardware
- Software
- Facilities
- Communications
- People

Examples of hardware assets include a computer monitor, central processing unit (CPU), keyboard or mainframe terminal. Software assets include application programs that are used to perform operations such as word processing, database or spreadsheet functions. Facilities assets include both the areas that house the equipment and computer resources, such as the Information Center, as well as the storage areas and the communications network.

Information[1] is perhaps the most important asset you might have and will be a major focus of this seminar. Information assets include both hard copies and disk copies of all information processed within the organization, such as memos, reports, financial documents, databases, etc. Examples of personnel assets include data entry operators, security officials, programmers, end users etc.

---

1 The terms data and information are often used interchangeably, but they refer to two distinct concepts. Simply stated, data are raw facts, while information is data placed in a meaningful context for its recipient. Data are usually simple items that taken alone do not constitute meaningful information. Information consists of data that has been purposely manipulated and arranged to be meaningful to a recipient.

EXERCISE

1. Which of the following are assets?

   a. A computer center
   b. An organizational database
   c. A software library
   d. A library of backup files
   e. All of the above

2. List two examples of the following:

Information assets	Personnel Assets
_____	_____
_____	_____

3. Take the individual data items listed below and make a meaningful item of information.

   Y C U E S I R T

   While most assets can be easily be distinguished, it is hard to differentiate between data and information assets.

Vulnerabilities

A *vulnerability* is a weakness that can endanger or harm any of the assets mentioned earlier. It is a:

> *flaw or weakness in the environment that can cause harm to computer assets such as hardware, software, data, communications, personnel or physical resources.*

Every information system is comprised of the people who operate it, the life cycle of its hardware and software, the facilities it occupies, and the communication network it uses. Most of these have *inherent* weaknesses or vulnerabilities. Below are a few examples of vulnerabilities and the assets they can endanger.

Assets	Examples of Vulnerabilities
Hardware	Computer hardware is vulnerable if the operational environment is not secure. The location of the facilities can frequently affect their vulnerabilities. How effective are the access controls? Can anyone walk in the front door? How susceptible is the facility to natural disasters such as fires, water damage, and lightning? Malfunctioning of equipment, incorrect operational procedures, lack of maintenance and controls are other examples of hardware vulnerabilities.
Software	Vulnerabilities include known program errors, unauthorized automated routines, and inadequacies in system software that permit unauthorized access to hardware, data or programs.
Data	Data is subject to both *accidental and deliberate* compromise. Lack of effective controls on personnel, software, or hardware can cause data to be accessed by unauthorized persons. There are several ways this could happen: photocopying, browsing, negligence in handling sensitive trash, exploiting a system flaw, etc.

Administrative	Standard operating procedures are essential in ensuring the consistent and efficient operation of an automated environment. Failure to establish these procedures can result in costly disasters. Examples of administrative vulnerabilities include lack of procedures to control changes to a system's software structure, inadequate operational procedures, lack of on or off site locations to store backup tapes or disks, and ineffective accountability techniques.
Personnel	If users are not adequately trained, they represent a considerable vulnerability to the system. Poor work habits, lack of communication between management and employees, and disgruntled employees are examples of personnel vulnerabilities.
Communications	Open and easy access to phone lines, microwave, and satellite communications facilitate the movement of data from place to place. All of these systems are vulnerable to compromise.

EXERCISE

3. From your experience, give one additional example for each of the following:

   a. Administrative vulnerability?

   _____

   b. Personnel vulnerability?

   _____

   c. Communication vulnerability?

   _____

Understanding Threats

A threat is defined as:

> *any activity, deliberate or unintentional, with the potential for causing harm to an automated system.*

In other words, a threat is someone or something capable of exploiting a weakness or vulnerability in the automated environment.

Threats can originate from a variety of sources. Hackers can get into the system electronically, disgruntled employees can gain unauthorized access to sensitive information, and even natural occurrences, such as storms, floods, and power surges, can completely destroy computer assets.

Threats can be grouped under three major categories as follows:

- External/Internal threats
- Environmental threats
- Technical threats

As you will notice in the examples discussed later, there is a lot of overlap between the various categories of threats.

Any of these threats can cause tremendous damage to an automated environment both in terms of cost as well as time. They can cause denial of service to software, data, hardware, administrative, physical, communication and personnel resources.

External/Internal Threats

External threats are deliberate and frequently malicious acts of behavior committed by *outsiders*, while internal threats original from *within* an organization. Internal threats are usually committed by personnel who come in contact with the system on a daily basis. The primary goal of the instigators of both external and internal threats are to disrupt normal business operations and cause harm to an automated information system.

Some common external/internal threats include:

- *Theft of software, hardware or data* - Smaller computer systems such as micros and PCs are ideal targets for theft because of their compact size.
- *Sabotage* - Terminated employees (or others) can gain unauthorized access to a facility and modify data or cause damage to other computer resources.
- *Espionage* - a former or current employee can use their password to gain access to sensitive information.
- *Vandalism* - Vandals and other intruders, such as hackers[2], can cause immense damage by closing down accounts, altering data, crashing electronic bulletin boards and even totally destroying computer systems. Such people are usually motivated by mischief, challenge, the urge to cause destruction, or a desire to steal data and application software.
- *Improper handling of media* - This can lead to damage or destruction of crucial data. The problem could stem from a lack of proper training in the handling of storage media, such as tapes, disks, cartridges and printouts.
- *Eating, drinking and smoking* - In the computer work area these can cause problems. For example, smoke particles can damage magnetic heads of floppy diskettes and destroy the data.
- *Compromise of passwords* - Sharing of passwords, or accidentally leaving them around for others to see, can be a serious threat to any information system.

---

2 As computer technology has evolved, the term hacker has taken on different meanings. In the early days of computer usage, hacker did not have negative connotations. It originally referred to an intelligent and extremely proficient programmer who could put together an elegant statement of code. Today, hacker may also mean a person who attempts to gain unauthorized access to large system by using PCs.

- *Data alteration* - An employee can accidentally or intentionally alter crucial data, thereby reducing the integrity of the system and causing immense damage. (For example, changing numeric data or inputting false information into data files.)

- *Operational errors* - Due to lack of proper training, a user can make costly mistakes while operating the computer. For example, in attempting to format a floppy disk, a user could wipeout information on the hard disk by entering an incorrect command.

- *Improper disposal practices* - Throwing away unwanted materials in the trash can be a serious information security hazard. Proper disposal practices such as degaussing, shredding or using burnbags should be enforced.

Environmental Threats

Environmental threats are usually caused by natural disasters such as fires, water damage and earthquakes. They may also be caused by improper environmental controls, malfunctioning of equipment, lack of proper maintenance procedures and negligence.

A few examples of environmental threats are as follows:

- *Earthquakes* can pose a critical threat to the computer environment, depending on geographical location.
- *Fires* or explosions of any type within a facility can partially or even totally destroy computer resources.
- *Water damage* as a result of floods, thunderstorms or a burst pipe can interrupt services.
- *Airborne particles* such as smoke or dust can harm equipment and disks.
- *Improper environmental controls* such as excessive heat, humidity and an inadequate ventilation system can cause erratic operation of the information system and result in the disruption of services.
- *Power fluctuations* or interruptions in power supply can erase memory, alter programs and destroy hardware.

In addition, electromagnetic interference and static electricity charge are other environmental hazards that can damage equipment and affect other computer resources.

Technical Threats

Technical threats are man-made threats that are implanted into the computer system with the specific purpose of causing harm. They are *programming or instructional codes that are deliberately embedded* into the system to destroy, sabotage or alter computer resources. Technical threats are capable of tremendous financial and productivity losses due to damage and destruction of critical data.

A few examples of technical threats include:

- *Viruses* - a small program that contains instruction codes to attack software and provide unauthorized access into a computer system. For example, a virus attack may be able to erase data, alter programs and even display unwanted messages on the screens. The key feature of a virus is that it can replicate by attaching itself to the programs it comes in contact with, thus affecting a vast network of programs and users.

- *Trojan horses* - On the surface Trojan horses appear to be legitimate programs with a valid, useful function. However, they also have a *hidden agenda.* Skillfully embedded into such programs are additional, hidden functions that can exploit the security features of a system. An example of a Trojan Horse could be a text editor that copies every file it creates into the attacker's directory. The attacker, in turn, could use the directory to alter, or destroy data.

- *Time Bombs* - is an instructional code that is preset to cause a later malfunction after a specific time and date.

- *Logic bombs* - a computer code that is preset to cause a later malfunction when a specified set of logical conditions occur. For example, a logic bomb may be set to alter all records of employees with particular social security numbers.

All of the above are methods used to commit computer related crime. There is a more elaborate discussion of viruses in a later section.

EXERCISE

4. We just ta :ed about some of the more common threats to computer systems. Based on your personal background and experience, can you identify additional threats? Name one example from each category.

Internal _____

External _____

Environmental _____

5. Identify whether the following threats are Internal (I), External (Ex), Environmental (En) or Technical (T).

a. An employee attempting to format a floppy disk, wipes out information on a hard disk by accidentally entering an incorrect command.

b. A computer terminal has been on for a long period of time in a poorly ventilated room.

c. A terminated employee uses his password (still in operation) to gain access to classified information.

d. A program which is set to alter all records which have a social security number beginning with 999.

e. An employee regularly dumps unwanted documents and diskettes into the trash.

Impact on Computer Resources

So far, we have discussed various examples of threats and vulnerabilities. However, to understand their relevance to computer security, we need to examine how these threats affect the resources in an automated environment.

In this section we will explore the four ways in which threats and vulnerabilities can impact computer resources:

- Destruction
- Disclosure
- Modification
- Denial of Service

Destruction occurs when an asset, such as computer equipment or software is totally lost or damaged. This can occur as a result of theft, vandalism or natural disasters such as fires and floods.

Disclosure occurs when data, programs or other sensitive information is intentionally or accidentally divulged to unauthorized recipients. It occurs primarily due to external and internal threats. It basically refers to the violation of information secrecy.

Modification occurs when data or programs are altered or damaged as a result of input errors or unauthorized access. Data integrity can be violated due to malicious altering of information or when personnel handling the data are inadequately trained in operational procedures.

Denial or disruption of service results when an asset still exists, but cannot be accessed or used to perform a processing function for a prolonged period of time. Denial of service can be defined as a temporary reduction in system performance, a system crash requiring manual restart, or a major crash with permanent loss of data.

In the past, most people's idea of computer security focused primarily on the physical machine and the facilities. However, with the high incidence of security violations due to disclosure and modification of data, *information secrecy and integrity* are becoming critical security issues and will be a major focus of this seminar.

Preventive Measures

Being aware of threats and their consequences is important in order to take remedial actions. But what about preventive measures? While the danger of threats cannot be totally eliminated, there are certain crucial preventive security measures that can be taken to minimize the damage.

1. Establish and implement security policies and procedures for maintaining a safe computer environment. This involves identifying the individuals responsible for maintaining security, deciding on the types of information requiring security, assigning responsibilities to users, and building accountability into the system.

2. Emphasize the importance of information security.

3. Educate users. Make them aware of the threats and vulnerabilities that are present in the automated environment and the control measure to prevent or remediate these threats.

4. Periodically conduct risk analysis to assess risks to information and equipment.

5. Plan for contingencies to ensure backup for equipment, information, programs and documentation.

This workshop attempts to address most of the preventive measures suggested above.

BASIC SECURITY POLICIES AND PRACTICES

So far, we have discussed problems. This section deals with solutions or *countermeasures* to deal with the threats and vulnerabilities.

Countermeasures

A countermeasures can be defined as:

> *any action, device, procedure or technique to direct, oppose or regulate a threat or vulnerability.*

This section deals with the various security countermeasures that can be adopted to safeguard and protect computer resources. They can broadly be categorized as follows:

- Physical security
- Information/software security
- Administrative/procedural security
- Communications security
- Personnel security

For each category there will be a brief description of the problem, vulnerability clues or checks, and recommended security practices and procedures. Both *preventive and remedial* security measures will be discussed.

Physical Security Measures

Physical security measures involve safeguarding *all* computer assets, including the surrounding facilities, from theft, physical damage and unauthorized access. Physical security measures also encompass protection against environmental hazards.

Some common physical security problems include:

- Theft, vandalism, arson and other physical damage
- Unauthorized access
- Improper work area practices and unethical conduct
- Improper handling of media
- Problems resulting from environmental and natural causes

Below are a set of physical security guidelines needed to safeguard A.I.D. automated systems and the information resident on them.

Security of Operational Environment

One of the most important physical security measures is controlling access to the *operational environment*. The room housing the VS or OIS - often referred to as the *Computer Room or Information Center* - as well as the distributed system, must be protected from external threats such as theft, physical damage and unauthorized access.

Additionally, there is also the danger of *internal threats* such as unrestricted access, uncleared personnel and post employment access. Disgruntled employees are also of great concern. Inadequate procedures to control access can lead to disclosure, modification, or destruction of computer resources.

Improper work area practices, and unethical conduct is another area of concern for physical security. Smoking, drinking and eating in the vicinity of computer equipment is a hardware security problem. Food and ashes that are dropped on the keyboard can work down into the mechanism and cause malfunctioning.

Security Policies and Procedures

Below are suggested procedures and policies for ensuring security of the operational environment.

Protection against theft and physical damage

1. The Computer Room or Information Center must be designated a *controlled* area and be properly secured with locking devices.

2. The Information Center door combinations must be controlled and changed at intervals of 6 months, and as necessary.

3. An inventory of all computer equipment, including software and storage media, must be maintained and updated periodically.

4. Strangers and terminated personnel entering a computer facility must be questioned and screened appropriately.

5. Users must be made responsible and accountable for the small computers they use.

6. Small information systems, such as WANG WP, small OIS, VS systems, and microcomputers, located in open work areas should be placed so that their use may be easily monitored. When necessary, room or equipment locks should be used to protect such systems against theft.

   Terminals and printers should be physically or logically disconnected after business hours, or when they cannot be monitored effectively.

7. If necessary, install external surveillance systems to prevent unauthorized users from gaining access.

Unauthorized Access

1. Access to computers should be limited to authorized users in order to prevent untrained or malicious individuals from damaging or making inappropriate use of computer resources.

   Control access with user identification techniques such as passwords, log-on procedures, and authorization procedures (discussed later).

   Maintain a list of authorized users near computers, terminals and printers and enforce the use of such a list.

2. Establish a guard force to prevent unauthorized persons from entering the facility. The guard will be responsible for verifying and admitting authorized personnel, maintaining a visitor log, and ensuring that visitors are properly escorted.

3. Visitors and other maintenance personnel should be allowed access only when authorized by the System Security Officer (SSO). Visitors should always be escorted by authorized personnel.

4. Invalidate passwords of terminated employees immediately.

5. Extended Hours - A plan should be formulated to allow authorized personnel entry into the area after duty hours and in case of emergencies.

Hardware Security

1. Establish audit trails or logs to monitor hardware access.

2. Restrict hardware modifications to authorized personnel such as system engineers and maintenance personnel.

3. Develop and implement policies for preventive hardware maintenance.

   Ensure that equipment is kept in good working order. Monitor and record hardware maintenance. Make sure that maintenance personnel carry proper identification.

4. Establish proper work area practices and ethics. If necessary, prohibit smoking, eating and drinking on or near terminals.

Security of Storage Media

Equally important as physical security for computer equipment is security for *storage media* such as source documents, tapes, cartridges, disks and printouts. If storage media are not maintained, controlled, or audited, they become vulnerable to theft, misuse and unauthorized access.

Improper handling of magnetic media is yet another serious physical security concern. If floppy diskettes and tapes are not labelled, stored, or handled correctly, critical data can be altered or destroyed.

Security Practices and Procedures

1. Magnetic media must be stored in secure storage areas or filing cabinets. When not in use, tapes, disks and other operational records should be securely locked away.

2. Physical access to tapes or disks should be restricted to avoid deliberate or inadvertent removal.

3. Employees should be trained in the proper handling of magnetic media.

4. Establish appropriate procedures for disposal of unwanted and outdated materials such as degaussing, shredding and the use of burn bags.

5. Maintain, control, and audit storage media inventories. All magnetic storage media should be accounted for and labelled correctly, with the owner's identification and the proper classification of data.

6. Back-up material critical to the organization's functioning must be stored completely away from the main computer room. This decreases the potential of loss from fire or flood.

7. Employees must be cautioned against lending storage media to unauthorized persons.

8. Whenever demountable magnetic media are moved to another location, the Systems Manager should record their removal and subsequent return in an appropriate log.

Environmental Controls

The automated system's environment is a security concern, because an improper or a *hazardous* environment can cause severe damage to the system. Hence special attention should be given to minimize the natural and man-made hazards to which computer resources are exposed.

Security Practices and Procedures

1. Fire and water sensors should be strategically placed in the Computer Center, and users should practice fire prevention rules. The fire alert system and suppression devices should also be tested regularly.

2. Ensure that equipment is located away from potential water hazards, such as plumbing pipes, sprinkler systems and areas known to flood.

3. Ensure that the humidity controls functions properly. Adequate air-conditioning and ventilation is necessary to ensure continuing operation and accessibility of computer resources. Depending on local conditions, backup air conditioning should be available.

4. If local power is not dependable, consider the use of a UPS (uninterrupted power supply), or other means of avoiding power fluctuations. Use of voltage stabilizers also helps prevent momentary power surges.

5. Dust and smoke infiltration can seriously damage equipment. Keep equipment in a *dust-free* environment. If necessary, use plastic covers to protect computer equipment and resources from dust and other airborne contaminants, food and cigarette ashes.

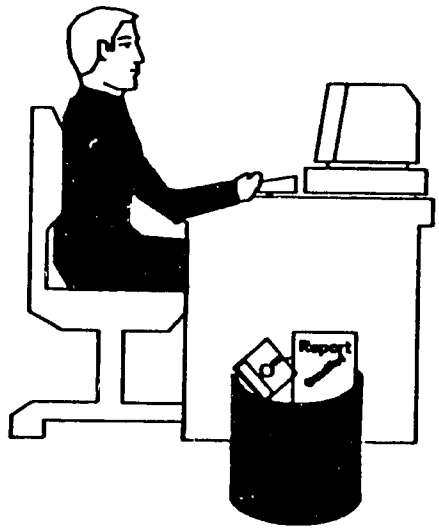
6. Use anti-static pads, carpets, and sprays to control static electricity.

7. Contingency and recovery plans for fire disasters should be established. As part of the overall fire plan, an emergency team must be prepared to respond to a fire alarm and help evacuate the building, shut down the system, and protect storage cabinets and other appropriate fire procedures.

   Note: In case of building emergencies - fire, earthquake, bomb threat, etc. - systems personnel should exercise judgement in powering down the equipment and evacuating the area. To avoid uncontrolled access during the emergency, users should be logged off and the system powered down normally if time permits.

EXERCISE

1. Examine the illustration and answer the questions given below:



a. Identify the threat being described in the illustration.

b. What might be the consequences of the threat?

c. What countermeasures can you take to safeguard yourself.

2. Which of the following are effective disposal techniques:

   a. Use of burn bags
   b. Shredders
   c. Degaussing devices
   d. All of the above

3. Indicate whether the following statements are True (T) or False (F).

____ a. One of the most important physical security measures is controlling access to the operational environment.

____ b. Without appropriate temperature and humidity conditions, computer systems can crash.

____ c. Passwords of terminated employees can safely be assigned to other incoming employees.

____ d. All backup materials should be stored in the vicinity of the computer room.

____ f. Frequent power fluctuations may cause a system to become inoperable or may destroy or change data being stored or written.

____ g. Computers should share electrical power sources with appliances and office equipment.

4. What remedial measures would you take to counteract the following security breaches:

   a. External theft of hardware, software and data

   b. Post-employment access

Data/Information and Software Security

The following story indicates the *susceptibility* of information:

A stealthy figure dressed in black shines a penlight around your darkened, deserted office. Slinking over to your desk, he pries open the locked top drawer and rummages through the debris to find his booty - the disk with your top secret financial information. He steals over to your PC and attempts to open the disk by selecting common passwords. He tries your birth date, then your initials with no luck. Success comes on the third try when he enters your company name. Now he can steal your data.

Excerpt from Joel Mcnamara's
For Your Eyes Only, MacUser, Sept 1988.

Over time, we have gone from recording history on cave walls to paper, and now to disks. Though the medium may change, the susceptibility of information remains the same. *Information* is perhaps an organization's most valuable resource. If compromised, it can result in significant financial losses and embarrassment.

This section will discuss security measures pertaining to the following:

- Information Security
- Data Security and Integrity
- Software Security

The heart of data security is how and where you store information, who gets access and what type of access, and what are the accidental vulnerabilities the data is prone to.

Information Security Measures

Information security refers to the controls that *protect* sensitive information from unauthorized access, destruction, modification or disclosure.

As more employees get access to computers, information is no longer restricted to a select *few*. As a result, opportunities for crime, waste, abuse and unauthorized access increase. Significant steps towards protecting information include:

- *Controlling access* through user identification techniques such as passwords, authorization and log-on procedures.
- *Restricting the activities* performed with information. For example, most employees in the payroll department might need to view the data, but only a select few may require the capability to make changes to it.
- *Preventing accidental damage* due to human errors, improper media handling or system malfunctioning. Examples include coffee spilling on a diskette, fingerprint smudges on the magnetic surface of a floppy, or even an operating system error causing classified information to be included as unclassified output.

Below are a set of guidelines that will help you protect your information. They are categorized broadly into general security measures and password security measures.

Keeping Backups

1. The first step in information security is to backup all your files, disks and other magnetic media.
2. Have a *daily and weekly* backup policy. Such routine backup of files allow users to continue operations with little or no delay if they incur problems such as hardware failure, power loss, etc.
3. Keep backup files in a separate location from the original disks, ideally, locked in a fireproof container.

Preventing Unauthorized Access

1. Use passwords and other authorization procedures (discussed later) to prevent unauthorized access.
2. Establish an audit trail or log to monitor computer usage.

3. Restrict activities performed with information. There should be restrictions on the type of information, applications or systems that users can access.

4. Turn off idle terminals and word processors when not in use.

5. Keep all disks locked and out of sight. Restrict access to related areas that contain data files such as off-site backup facilities, and on-site file libraries.

6. Maintain and update an inventory of all files. Know what data you have. Periodically check the inventory to make sure that all files are accounted for.

7. Enforce all the physical security measures (discussed earlier) for dealing with uncleared personnel and post employee access.

Preventing Accidental Disclosure

1. Ensure that all employees know how to identify sensitive information. Use external and internal file labels to clearly indicate the type and sensitivity of information they contain.

2. Train all employees in the use, maintenance, and disposal of magnetic media.

3. Any system malfunction or peculiarity should be reported *immediately*.

EXERCISE

5. An important *preventive* measure in protecting data from power failures, hackers and improper media handling is:

   a. Establishing audit trails
   b. Backing up files on a regular basis
   c. Maintaining an inventory of all files and programs
   d. Enforcing logon and authorization procedures

Password Security Procedures

Passwords have been part of security systems since the first millennium B.C., when they were used to control access to various parts of Solomon's Temple.

The computer world has been using passwords for a while now, and it has proved to be a common and effective technique for ensuring system and information security. Today, passwords serve to protect databases and spreadsheets, encrypt data, and limit network and file access.

What is a password?

A password identifies a user to access computer resources. When a user wishes to access a computer system and its resources, she is required to identify herself. By providing the correct password, a system is able to authenticate an individual's identity and authorize access to the computer system.

How do you generate effective passwords?

A password is only as secure as you make it. The key to generating effective passwords is to make them *difficult to guess*.

If you were trying to break into a system, think about some of the passwords you would use:

_____, _____, _____, _____.

Make sure you *avoid* some of these common, and thereby easily guessed, passwords. Don't use passwords like the name of your spouse, pet, or child, your first or last name, or initials, your birthday or wedding anniversary, your social security number, a word relating to a personal interest, your company's name or some derivation, your job function or department, single letters of the alphabet or sequential numbers.

Suggested methods for generating secure passwords include: combining two dissimilar words (taco and sushi to make tacosushi), using foreign words (luotuo - Chinese for camel), mixing significant words, dates, and initials (AEOz1934), or selecting a word and adding a few random characters to it (slugxa).

Thus, the golden rule for effective passwords is: select them *consciously*, make them unique to each person and change them frequently.

Making passwords difficult to guess but at the same time *easy to remember* is certainly a tricky issue. Although it is recommended that you don't write down your password, this goes against what we know about human thinking and remembering. One way out of this tricky situation is to *cleverly conceal* the password (encrypting, use of special coding schemes, etc.) so that it is difficult for the password pilferer to find.

Despite its popularity, the success of using passwords is directly linked to the discretion of the user and the security policies of the agency. A password in the hands of the wrong person can lead to disclosure and modification.

Note: Whatever password combination you choose, be sure to commit the password to *memory*. Otherwise, it is of little use.

Password Protocols

The following passwords protocols should be strictly adhered to.

1. Each user must have a unique ID and password. Group passwords are not allowed.

2. Passwords should be selected randomly and should not be names, initials or traceable personal data. Variable passwords are permitted as long as they are within an 8 character limit (Wang VS restriction).

3. Whenever possible, generate passwords by an automatic generation program in a system that has been approved by the proper authority.

4. Invalidate the passwords of those leaving the organization.

6. Commit passwords to memory. Do not post them in visible areas such as desks, or walls. Whenever possible, store passwords in encrypted form.

7. Be sure that a password is not visible on the computer screen when it is entered. Also ensure that passwords do not appear on printouts.

8. Change passwords at regular intervals. The recommended time between password changes is 3 months.

9. If you have even the slightest inkling that it has been compromised, notify your representative and change it immediately.

Establish and enforce the above password rules. Be sure to educate users to common problems.

While password protecting files, *where should the protection be?* Should it be at the operating system level or should it be at the software level? It is less vulnerable at the operating system level, since denying access to the system itself precludes unauthorized users from ever attempting to access the files. Having it at the software level means that they have already accessed the system and can now start exploring alternative methods to gain *unauthorized access* to the files.

When protecting files, it is a good idea that one person be designated the *keeper of passwords*. Otherwise, if employees leave the organization without divulging the passwords, it may become very difficult to gain access to critical information. It becomes a crucial personnel security issue, particularly with disgruntled employees.

EXERCISE

6. Examine the illustration and answer the questions listed below:

a. What is the vulnerability being described in the illustration above?

b. What will the consequences be?

c. What countermeasures would you take to protect your information?

7. Bill keeps forgetting things, so when he was assigned a password by the SSO, he immediately wrote it down on a piece of paper and posted it next to his desk drawer. What is the vulnerability being described here? What steps should he take to prevent disclosure of sensitive information?

8. Which of the following conditions may lead to unauthorized disclosure of sensitive information:

a) System malfunction
b) Labelling data incorrectly
c) Compromise of a password
d) All of the above

9. Indicate whether the following statements are true (T) or false (F).

____ a. It is good practice to change passwords once every year.
____ b. If you can't remember your password, then chances are that it is too long or too cryptic and you should change it to something simpler.
____ c. Effective passwords are selected consciously, are unique to each person and changed frequently.
____ d. It is good practice to post passwords in visible areas. It helps jog your memory.
____ e. If you use passwords for a variety of purposes, it is a good idea to use the same one for everything.

10. Under which of the following conditions should passwords be changed and new passwords issued:

a. Immediately following any suspected security compromise
b. When an individual goes on a two-week vacation
c. When files are being backed up
d. At least every 3 months
f. All of the above
g. Options a and d

Data Security and Integrity

Data integrity addresses safeguards in the processes of data origination, input, processing and output. The goal is to protect the system's data from malicious or accidental alterations, and to ensure its accuracy and completeness.

If processed information is not accurate and complete, it can cause inestimable damage to the functioning of an organization. For example, a personnel information system which stores and processes confidential employee data (such as payroll and health records), if tampered with can cause a great deal of financial loss to the organization and personal embarrassment to the individuals.

Other factors affecting data integrity are input or *data entry errors*, and operational errors. Hence input data should be subject to scrupulous verification and accuracy checks. Otherwise, bad data can lead to serious processing errors, job halts, output errors, and even compromise the confidentiality of sensitive information.

Security Procedures and Practices

1. Personnel should be trained adequately to operate a system and enter data correctly.

2. Operators should follow standard operating procedures and there should be built-in checks to detect operator errors.

3. Implement any of the following validation and editing techriques to ensure that data is being processed properly.

   Key Verification - a second person reads the same document and keys data into a verifier.

   Editing - Individual fields and combinations of fields are checked for valid content, format, size and sign.

   Data Validation: Transaction values (or dates) are compared automatically with a table of valid values (dates) stored in the system.

4. Cross-check the contents of files by doing a records count or controlling the total.

5. Create backup copies of all data files and documents.

EXERCISE

11. It is a good idea to distribute responsibility for sensitive data entry and processing to several people within the group. Do you agree with this statement? Give reasons for your answer.

12. Data integrity can be compromised if:

    a. Proper disposal practices are not enforced
    b. Data is entered incorrectly
    c. Operators do not follow standard operating procedures
    d. Both b and c are correct
    e. All of the above

Software Security

If software is *not* protected, it can be altered, modified or destroyed. This, in turn, can adversely affect the data being processed or even result in system failure and denial of computer services. Hence, efforts should be made to establish procedures and policies for:

- *Use and maintenance of software*

  Software should be documented thoroughly to ensure its proper use and maintenance. Any program that is modified should undergo operational testing and validation.

- *Software sharing*

  In situations where software is shared, there should be well established policies for accepting and checking software prior to its installation. New packages should be tested extensively for errors, peculiarities, or unexpected functions. Many packages are not what they seem and could contain viruses or hidden program codes that can damage or corrupt the equipment or data.

- *Safeguarding license software*

  Employees should be cautioned against unauthorized copying of proprietary software which can be a significant financial liability for the organization.

Security Practices and Policies

1. Document and maintain software thoroughly to ensure its proper use and maintenance.

2. Maintain and update an inventory of all existing software. Unlimited copies of protected commercial software should not be made and installed randomly.

3. Test new software on test data before installing. New software should be subject to extensive and critical review and error checking. Any software that is known to have inherent security weakness should not be implemented.

4. Never use the original software diskettes. Always work from copies.

5. Software from *unrecognized sources* and bulletin boards should not be accepted without undergoing a comprehensive review for errors and peculiarities.

6. As users work with various software, stress the importance of reporting anything out of the ordinary. Errors or unauthorized program codes are often discovered only by accident. Frequently, program errors can become the entry point for dishonest system users.

7. Establish audit trails and monitor log-on attempts to detect unauthorized access to software resources.

Administrative/Procedural Security

Administrative security involves establishing *operational and accountability* procedures to ensure that all personnel who install, operate and maintain computer resources know their responsibilities for system security.

It establishes methods for detecting, reporting, investigating or *resolving security violations* and abuses. In addition, it establishes procedures for controlling changes to system hardware, software, applications, passwords and central facility and terminal access.

Administrative security measures provide managers with *guidelines* for the management and supervision of information resources, including data processing, storage media, system and application development, and telecommunications.

Two critical administrative security procedures include:

- Dividing functions and duties based on the employee's need to know.

- Tailoring access controls to ensure that data and files are available only to authorized personnel.

Access controls are determined by:

* The type of work to be performed
* The interval of time for which access is required
* The location from which the data will be accessed: remote, local or microcomputer
* How the data will be used
* Who will use the information

Administrative Security Policies

1. Develop and establish policies and controls for the effective operation and maintenance of computer resources.

2. Computer systems should be audited or reviewed regularly for errors in operations, software, and data processing.

3. Establish audit trails and procedures to check the accuracy and completeness of processing operations.

4. Develop and establish measures for the disposal of outdated and unwanted materials.

5. Establish procedures for the proper labelling and inventory of storage media.

6. Make frequent backups of information processed by a system and the programs used to process it.

7. Maintain the required logs and registers of visitors, system users, etc.

8. Conduct risk analysis periodically to identify risks and vulnerabilities.

9. Develop contingency plans, disaster recover plans or continuity of operation plans to handle disasters such as fire, water damage and system breakdowns.

A.I.D. specific administrative controls will be discussed in the next section.

EXERCISE

13. Users of a network terminal, which accesses sensitive information, are ignoring the sign-on log placed next to the keyboard.

    a. What type of vulnerability is being described?

    b. How would you rectify this problem?

Communications Security

As more and more personal computers are networked and able to communicate with each other, protection of transmitted data and the physical security of the connecting lines and links becomes a critical issue.

Without *communications security,* information can be intercepted or manipulated by people masquerading as authorized users, or even routed to unauthorized terminals. Another example of a communication security violation is intrusion by hackers and others who could use techniques to browse through critical information, and even examine the user's communication package for dial-up phone numbers, access codes, and passwords.

Recommended Security Practices

1. Implement password usage to control access to a system.

2. Disconnect communications devices when they are not in use.

3. Configure systems to allow only a very small number of invalid log-on attempts before lock out.

4. Check audit trails for communication intrusion attempts.

5. If dial-up access is used, change telephone numbers periodically. If suspected of compromise, change phone number immediately. Caution all employees about the sensitivity of dial-up access telephone numbers. If necessary, install protection devices for dial-up access of computer systems.

6. Communications systems should have alternative or backup paths to accommodate breakdowns of lines or links.

International Communications System (ICS)

The International Communications System (ICS) provides for interchange of documents and data between A.I.D. overseas Mission and A.I.D./W, using the A.I.D./W main computer as central switch and mailbox.

The use of the communications facility is restricted to unclassified documents and data only. Overseas posts and Regional Bureaus should coordinate what documents can be transmitted via ICS. However, no classified or LOU (Limited Official Use) material should be transmitted via this network.

Personnel Security

In the past, personnel security was not an issue at all. But with so many people using computers today, *people* have become a significant threat to computers. The threat of poor personnel security is greater due to the inherent vulnerability of computer systems. Employees, knowingly or unknowingly can cause modification, damage, destruction or denial of use of computer resources.

The four most serious areas of personnel vulnerabilities are as follows:

- *Inadequate training on security policies and procedures*

  It has been estimated that 50 to 80 percent of the problems occurring within automated environments are due to lack of employee training and development skills. In today's technical and complex environment, a well-trained employee is one of the most effective safeguards against any threat.

- *Poor communication channels between management and staff*

  Poor management attitudes and policy can lead to low employee morale, low motivation and a decrease in work productivity. This, is turn, can result in computer abuses, damages and violations.

- *Low motivation, morale and personnel problems*

  Personal problems such as drinking, drug abuse, financial difficulties and poor work attitudes can also affect the quality of an employee's work. If employees with such problems are allowed to continue working, they have the potential to be compromised, posing a threat to the systems and information with which they work.

- *Failure to comprehend the confidentiality of the information*

  Frequently, unauthorized disclosure occurs when personnel fail to comprehend the confidentiality and sensitivity of information. Such ignorance leads to information being downgraded without adequate review, and being incorrectly classified or labelled.

Security Practices

Personnel security refers to ensuring that employees are well trained, highly motivated and ethical. If they are not, there is a great potential for serious computer errors, abuse and violations.

1. Screen potential employees for personal integrity and stability.

2. Ensure that all personnel are well trained on the following issues:

   * the need to protect information.
   * effective security practices and procedures.
   * security roles and responsibilities within the organization.
   * correct procedures for operations and data input.
   * able to identify the levels of information in a system and the types of information to be protected.

3. All employees should be familiar with the security officials and how to communicate with them.

4. Publicize procedures to report security violations and irregularities.

5. All terminated and transferred employees should be prevented access to the automated system.

6. Observe the work habits of employees to detect poor work habits that may compromise computer security.

7. Include computer security compliance in job performance standards.

8. Frequently update their knowledge about security by distributing flyers, checklists etc.

9. Ensure that all employees know the organization's policy regarding the use of Bulletin Board Systems (BBS), and other information utilities such as CompuServe etc.

Note: Take immediate action against personnel who display the above vulnerabilities. Don't leave a disgruntled employee with extensive access rights while you decide how to deal with the situation.

A.I.D. SPECIFIC SECURITY PROCEDURES AND POLICIES

So far we have discussed general security measures that will help protect your information resources. This section focuses on security policies that are more specific to A.I.D. operations.

Roles and Responsibilities of Security Personnel

Whom do you contact when there is a problem?

The intent of this section is to discuss the roles and responsibilities of persons associated with maintaining effective security practices at A.I.D. Security responsibilities can be divided into the following categories:

- Management
- Operations
- User

A brief discussion of the responsibilities in each category, and the personnel associated with discharging them follows. It is important to recognize that some responsibilities may vary depending on installations and that one individual may hold more than one designation, depending on local conditions.

Management Responsibilities

The role of management is to facilitate the *development, administration, monitoring and enforcement* of computer security policies and procedures. Their principle responsibilities include:

- Establishing security policies and procedures
- Assigning accountability and responsibility for resources and security
- Minimizing risks and ensuring the continuity of agency operations
- Coordinating investigations of system security violations
- Performing risk analysis and contingency planning

Regional, Post and Unit Security Officers

The following A.I.D. personnel are responsible for the above management responsibilities.

At overseas posts, the Department of State, Regional Security Officer (RSO) is responsible for maintaining overall security. Depending on local conditions, there may be Post and Unit Security officers to assist the RSO in the discharge of his/her duties.

At A.I.D./W, a Principal Unit Security Officer is designated by the head of each major functional area to assist in carrying out the area's overall security responsibilities.

> **Note: Overall responsibility for all information system hardware and software within their jurisdiction still lies with Mission, Bureau and Office Directors.**

Operational Responsibilities

Operational responsibility for the security of A.I.D.'s information resources rests with the following personnel:

Systems Security Officer (SSO)

Both overseas and at A.I.D./W, the primary responsibility of the SSO is to assure that automated information systems are installed and operated in a manner consistent with A.I.D.'s security standards and requirements.

Following is a checklist of the SSO's specific responsibilities:

___ Take appropriate measures to protect all system resources from damage, destruction, or misappropriation.

___ Ensure effective implementation of security procedures by (a) educating users, (b) disseminating standards, and (c) providing periodic briefings.

___ Develop additional security procedures to supplement the general standards, as needed for local operating conditions.

___ Monitor the activities of all employees with access to the system resources.

___ Issue and maintain permanent records of access authorizations to facilities and equipment.

___ Monitor the issuance and control of all user IDs and passwords.

___ Browse through word processing documents periodically to ensure that sensitive material is not widely disseminated.

___ Coordinate with the Personnel Office to establish procedures to promptly notify the SSO of changes in status of employees (e.g., termination, transfer).

___ Conduct periodic compliance surveys and security evaluation reviews.

___ Evaluate, at least semiannually, threats and vulnerabilities to the automated information system.

___ Suspend operations, partially or fully, as soon as any compromise to system security is detected.

___ Report system failure, or other security violations to the appropriate A.I.D. officer.

___ Conduct risk analysis and develop appropriate contingency plans.

Systems Manager (SM)

The Systems Manager (SM) is responsible for *overseeing the day-to-day operations* of the automated system. This individual assists the SSO in the maintenance and compliance of security practices.

The specific duties of the System Manager include:

- Establish software, hardware and physical security controls
- With guidance from the SSO, develop procedures for establishing access to system applications, programs and data files
- Maintain an on-going log of access control data such as user IDs, passwords, data file access limits
- Report security violations and abnormal system operations to the SSO
- Back up and restore data files, as needed
- Arrange for data storage, both on and off-site

In some locations, the Systems Manager (if an American direct-hire employee) may also be designated as the System Security Officer. Depending on local circumstances, an Assistant Systems Manager may be available to assist the Systems Manager in his/her duties.

EXERCISE

1. In case of the following security breaches, whom would you notify?

   - A suspected password compromise
   - Theft of magnetic media
   - Unescorted visitor access
   - Non compliance with security practices

   a. RSO
   b. SSO
   c. Your immediate supervisor
   d. Personnel Department

User Responsibilities

Since *users* are a critical part of any automated environment, their responsibility in maintaining security procedures cannot be overstated. User responsibilities include:

- Complying with security guidelines
- Monitoring access to workstations located in their work areas
- Immediately reporting any abnormal occurrences to the relevant authority
- Protecting passwords
- Notifying the SSO in case of suspected security compromise
- Logging off idle terminals
- Ensuring that all storage media is properly secured and periodically reviewed
- Maintaining the integrity of data
- Protecting computer resources from physical or environmental hazards
- Following appropriate practices for disposing of sensitive information

EXERCISE

2. Which of the following are *not* user responsibilities.

   a. Reporting security violations to the SSO or SM
   b. Following correct operational procedures
   c. Protecting passwords
   d. Conducting risk analysis

A.I.D. Specific Administrative Controls

The administrative controls listed below will be helpful in monitoring workflow and in detecting and correcting security violations.

Log and Record Keeping

The following logs and records should be maintained by the SSO or SM:

a. Loan or Removal of Automation Equipment from A.I.D. premises

b. System User List

The SSO should maintain a list of all authorized system users. Such a list should contain name, user ID, access level, and the date the user was added and/or deleted from the system. The SSO should periodically review access levels, particularly for sensitive applications, with the user's supervisor.

c. Operations Area Access List

The SSO should maintain a list of all persons who have *unescorted access privileges* to sensitive areas including the central computing facilities and remote disk tape and disk storage areas.

d. Visitors Log

A record should be maintained of all visitors who require escorted access to the locked facility.

e. After-Hours Use Log

A record of requests for system use outside of normal work hours.

IDs For Visitors

When approved by the SSO, the SM can assign temporary system access IDs to visitors at the written request of the visitor's control officer. The request should include effective dates of *access validity* and should permit minimum access. A log of temporary IDs issued should be maintained, and the SM should periodically review the list and delete all expired visitor IDs.

System Maintenance Procedures

The SM should be notified before maintenance personnel or other vendor service personnel are allowed to access a system. In dealing with maintenance personnel, the following precautions should be enforced:

1. Maintenance personnel should be closely supervised.

2. Any magnetic media, circuit boards or other equipment brought into or removed from the facility, should be logged and monitored by the SM.

3. Certain Wang diagnostics allow for reading, and modification of data on magnetic storage devices mounted on the system. Care must be taken to prohibit maintenance personnel from using diagnostics or other methods to randomly browse through documents stored on the system.

4. Passwords issued to Customer Service Engineers should be *changed* at the end of each service call.

Systems Operations Log - A log should be kept of all normal daily operations, including the installation and removal of software, storage media usage, system problems reported, repairs conducted, parts replaced or removed for repairs, etc.

Extended Operations

If a computer facility is in operation beyond business hours, the following minimum standards should be enforced:

- The system must not be used after hours unless an authorized member of the system staff is present. The SM must be notified by the intended user when the system is needed for after-hours use.

- All after-hours usage should be noted in a log maintained by the SM and submitted to the SSO for periodic review.

- System maintenance personnel are prohibited access to the computer facility after normal business hours, unless escorted by an authorized employee.

Processing of Classified and Limited Official Use (LOU) Material

Confidential, secret and top secret material will not be prepared, processed or stored on non-TEMPEST information systems.

LOU materials are defined as "certain sensitive information which is not national security information and therefore, is not classifiable, but nevertheless warrants a degree of protection."

In A.I.D./W, employees may process LOU material on non-TEMPEST information systems provided it is: (a) password protected, and (b) stored in tapes or floppies which are appropriately secured at the close of each working day.

At overseas Missions, the processing of LOU material is dependent upon the Mission's classification as a high or low technical threat post.

Microcomputer Security

This section addresses A.I.D.'s security guidelines regarding the use of *microcomputers*. Microcomputers afford almost unlimited opportunity for intrusion into the system itself. For example, the entire system can very easily be removed, or data and even operating systems can be modified without your knowledge.

The following security practices should be strictly enforced:

- Users must be made aware of their responsibility to protect their data and equipment, including the necessity for making periodic backups of files.
- Locks must be used to protect information resources at all times. For example, microcomputers left in open office areas should be physically secured to a desk or wall.
- Data files containing sensitive information should not be identifiable by name. A separate printed index of the files can be maintained in a locked and secured area.
- When not in use, PCs should be turned off or disconnected. Limit access to micros and store diskettes in a secure location.
- Removable hard disks which have been evaluated and approved by the IRM can be used as backups for storing information that should be controlled.

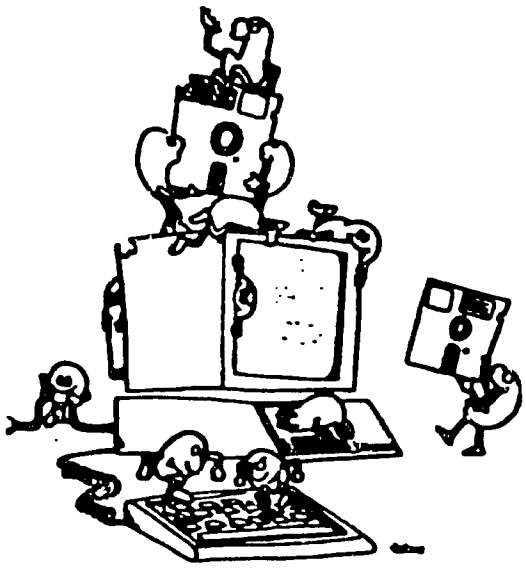
- Microcomputers removed from A.I.D. premises should be subject to standard property passes procedures.

Personally-owned Microcomputers

To avoid inhibiting the productivity of employees after hours or while on tours, A.I.D. policy *authorizes* employees to use personally-owned microcomputers for business purposes provided:

- Neither classified nor LOU information is processed on the equipment.
- Reasonable precautions are taken to avoid the misuse of information that should not be widely distributed.
- Projects are not designed for internal A.I.D. use through hardware or software that is inconsistent with A.I.D.'s equipment/systems standards.

COMPUTER RELATED CRIME AND ABUSE - STRATEGIES FOR PROTECTION



"Is today the day? I know there's something important I must do if the time is right. I have to reproduce myself fifty times. Let's look at the system files. Is there one of me already? If there isn't, I can copy myself. No, I am already in that program; let's check out this computer's program files. Surely there's at least one where I haven't been yet; Yes, there's one, but it is marked read-only; that's OK, I'll just change that marking so I can change the file. This feels good; I'm copying myself into that program; now I change the program just a bit, a little jump here and a return there, after my copy. Oh, yes, I forgot to cover my tracks - I must change the file back to read-only. Will anyone know I was there? Let's see, all the attributes are the same as when I got here; the length hasn't changed since I found some empty space to copy myself into. I must remember to change the creation date back to what it was when I got here, too. No point making it easy to see where I've been. Am I finished yet? No; I need to go through the same process on the diskette drives, if there are any, and see if I can reach through a network too. Am I finished now? I wonder what FORMAT C: means. Maybe I will do that the next time."

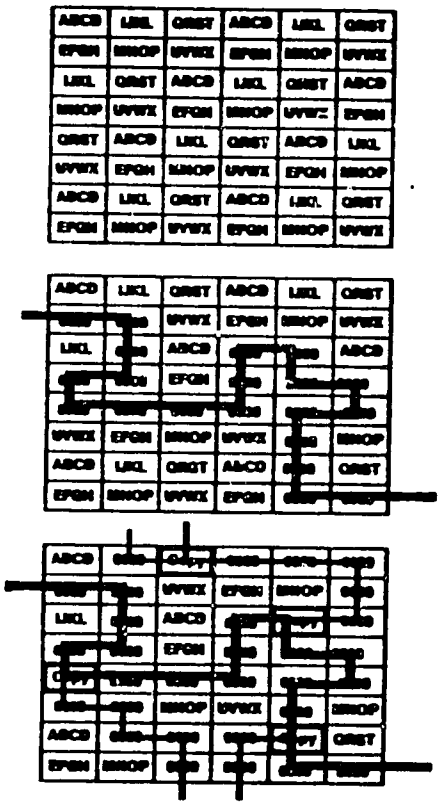
Computer Virus Crisis
Fites, et. al.

The above imaginary conversation reflects the "reasoning" of a computer virus. There have been many viruses that have worked in *exactly* this manner. You will not even know that you were affected by a virus until something goes wrong. Then you not only have to fix the damage, but also find any place the virus might have made *copies* of itself.

What is a Computer Virus?

Virus is a name for a class of programs that contain instructions to attack software and provide unauthorized access into a computer system. The key feature about a virus is that it can *replicate* by attaching itself to the programs it comes in contact with, thus *infecting* a vast network of programs and users. It is called virus because many of the characteristics of these programs mimic the characteristics of disease viruses.

The illustration below shows a *simulated computer memory* in three states. The first depicts the *ideal* state, the second displays *worm* or virus tracks and the third illustrates *virus damage* as its reproduces itself.



Memory, Worm Tracks and Virus Damage

The virus moves around randomly into any space it can reach. As it moves, it copies itself into the new space replacing the useful data with **0000** (zeros). As you can see in the third part of the figure, the virus starts to *replicate itself*, and each new copy of the virus starts on its own path through memory or disks, destroying data and programs.

When a virus attacks a system, the program or data file you were using suddenly stops working, probably when it finds zeros instead of some instruction or control information. It can be very difficult to figure out what happened. Even if you are able to figure out what is happening, you have to find and get rid of all the copies before you are safe; otherwise, the whole problem starts over.

What can a Virus do to your System?

Below are examples of ways in which viruses have affected computer resources:

* Fill up a computer with garbageware
* Corrupt executable files, such as system and program files
* Corrupt data files
* Reset a computer
* Format a hard disk and even physically damage the hardware
* Disrupt the boot sector[3], thereby disabling the computer
* Lock or redefine the keyboard
* Slow the system down
* Copy data files to unauthorized user directories

EXERCISE

Which of the following are typical characteristics of computer viruses?

a. Small and hard to find
b. Leaves no traces
c. Hides and replicates
d. Spreads very quickly
e. Both a and d
f. All of the above

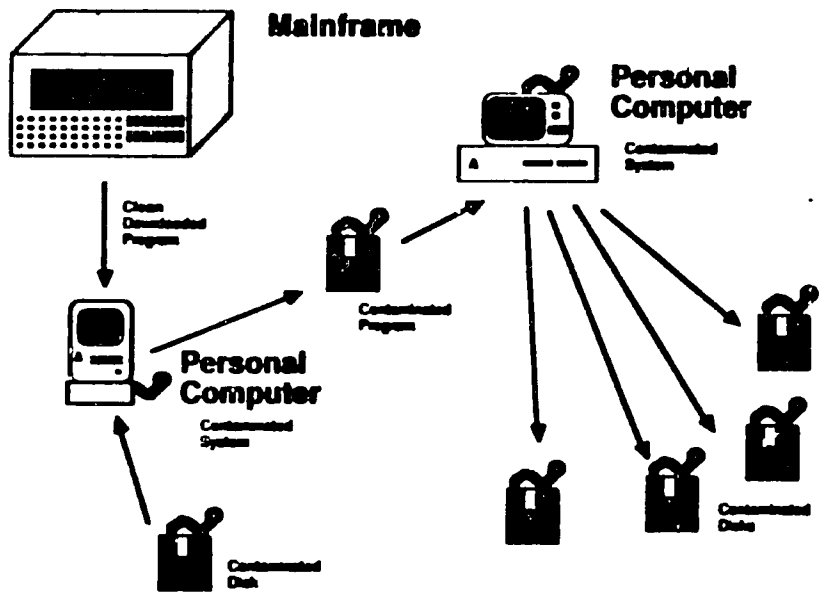
---

3 Three of the most vital sections of any computer disk are the boot sector, the FAT, and the root directory track. Unfortunately, these three areas are most vulnerable to a virus attack. The FAT (File Allocation Table) contains information about where files are stored on the disk, as well as keeps track of available storage areas.

How Does a Virus Spread?

Unlike disease viruses, computer viruses do not spread through the air. They must be put into your computer inadvertently by you, or deliberately by someone else. This leaves an enormous number of possible *infection pathways*. For example, any time you download a program from another computer, or copy new software from a friend, you increase your exposure.

The real reason why computer viruses are becoming a serious problem, and could be catastrophic in the near future, is linked to *connectivity*. Connectivity means people can share data, programs and computers. Unfortunately, it also means that vandals can attack everyone with the same computer virus program. The figure below illustrates how a virus spreads, eventually infecting a variety of systems including mainframes, minis and as well as micros.



The increasing compatibility of computers and communications have made it possible for a virus to spread much farther, faster and easier than was possible in the past.

Refer to the appendix for examples of some famous viruses and how they spread.

Trojan Horses and Other Methods of Spreading Viruses

A *Trojan Horse* is a common method for spreading computer viruses.

In the Homeric legend, the Greeks gained entry into Troy by concealing troops in a wooden horse that the Trojans took inside the city walls. In computer security, a Trojan Horse is *an apparently useful program that does things in addition to what it is advertised to do*. For example, it might be advertised as a disk compression utility, and it may indeed compress data on your disk. However, it might also copy a virus into your COMMAND.COM file.

Trojan Horses appear to be legitimate programs, but have a *hidden agenda*. They can put up nasty messages, bomb programs, erase information, and shuffle data. Harmful as Trojan Horses have proven to be, they do not reproduce themselves and cannot contaminate other programs. The damage is *localized*, and deleting the offending program usually solves the problem.

In the section on technical threats, we talked about some examples of viruses, such as Logic Bomb, Trap Door etc. Others variations include:

A Flying Dutchman is a feature of most Trojan horses that erases all traces of its existence from memory, thus eluding detection.

Salami technique is a program alteration technique which relies on altering such small slices of data, that the whole is not obviously affected. (e.g., benefit payments may be rounded down a few cents, and these funds (which can be considerable in the aggregate) are diverted to a fraudulent account.

How Great Is Your Exposure?

You increase your exposure to viruses if you use:

- *Pirated software*

  If you accept pirate copies of software from unrecognized and unreliable sources, your risk could be fairly high.

- *Freeware and shareware programs downloaded from bulletin boards*

  Public bulletin boards present the greatest exposure to viruses. Most of them have freeware and shareware programs available for downloading. Such programs pose a significant threat for viruses.

- *Disk compression utilities*

  Disk compression utilities downloaded from Bulletin Board Systems are very popular and useful, particularly while transferring data. However, these compression programs are frequently carriers of viruses and can infect the data being compressed.

- *Games from BBS*

  Games have been notorious for spreading diseased software. Typically, people download a new game and then run it immediately. Since you are concentrating on the game, you might not notice that it is doing other things as well.

A virus could also be inserted into a network. If carefully constructed, the virus could replicate and spread for quite awhile before it is detected.

EXERCISE

1. A colleague gave you a copy of a computer game, which in addition to being a game also has a secret mission to format your hard disk. Can you name the type of virus being described?

   _____ _____

Strategies for Protection

Virus protection measures include three steps:

- Avoiding viruses
- Detecting and getting rid of them
- Repairing the damage

Avoiding Viruses

Most computer viruses can be avoided by the following common-sense measures:

1. Practice the safety precautions listed below:

   * Never accept pirate copies of software.

   * Be *wary* about what you download from public domain bulletin boards, particularly games.

   * Use only programs that come from reliable and recognized sources.

2. Before installing, always test new software in a *test* environment. Check extensively for errors, peculiarities, and unexpected functions.

   Keep logs of every new program installed. Record the source, length, date and time installed.

3. On DOS computers, take a look at the .BAT files and CONFIG.SYS files regularly, perhaps monthly, and also every time you load or test a new program.

   Since viruses have to be run to make copies or do damage, they will sometimes insert lines into an AUTOEXEC.BAT or CONFIG.SYS file. If you find new lines, or changes to ones you already have, suspect a virus.

4. Keep backups of all important files. Even if your files get infected, you can replace them with the original uninfected copy. Use write-protect tabs on the backup diskettes for added protection.

5. Ensure that all users know the importance of reporting anything out of the ordinary as they use various software.

   Be wary of program size changes, amount of free space left on a diskette, and changes in last-modified dates or times.

If you think you have been exposed to a virus, report it immediately to the SSO or the SM. Available to the SSO as possible remedies, are antiviral packages such as Disk Watcher, Vaccine, Antidote, etc.

EXERCISE

3. Suggest three ways by which you can minimize your exposure to viruses.

a. _____

b. _____

c. _____

Detecting Viruses

How do you know you have a virus?

For most users, there are just two ways to discover a virus: through antiviral software which will help you detect suspicious activity, or when you see your computer do strange things for no reason.

The following *abnormalities* could indicate viral activity:

* The system slows down dramatically
* The program you are working on displays unusual error messages
* The number and size of files change without reason
* Directory updates take noticeably longer
* The keyboard suddenly starts to do odd things, or does not function
* During downloading of programs, unusual amount of free space is available
* Available RAM decreases for no apparent reason
* Last update for directory is identical to most recent update of files
* A previously-existing file suddenly disappears
* The COMMAND.COM file suddenly changes in size

Of course, any of these things can be caused by program bugs, or incorrect keystrokes. These symptoms do not necessarily mean that you have a virus. However, they should serve as *alerts* to indicate that all is not well within the system.

Be particularly *wary* of changes to system files. They *usually* indicate viral activity.

Getting Rid of Viruses

One of the planks of a security program should be *policy* on prevention, detection, reporting and remediating viruses. Without detailed technical knowledge and special tools, there are only a *few* things that can be done to get rid of viruses. Most experts in the field suggest that, in the absence of the technical knowledge, seek *professional advice*.

Other than seeking outside help, you only can recover from a virus by:

GETTING RID OF EVERYTHING THE VIRUS MAY HAVE AFFECTED AND RE-CREATING THE SYSTEM FROM CLEAN BACKUPS.

If you have kept backups (as suggested as a first line of defense security measure), and they are uninfected, you will lose whatever you have done since the backups, but you will be *operational* again. Ideally, you should always have an *original write-protected backup* copy of your operating system on a diskette. Then if you are affected by a virus, you can boot your system from the original system diskette, format the hard disk and start over from backups. This system works if you have clean backups, but it is quite *drastic* and takes a lot of your time.

Decisions regarding professional assistance (whom and when) must be established in policy. It might be less expensive to hire a professional who will be able get rid of the virus and repair some of the damage without having to rebuild the system. However, this is a critical decision which is best made before the fact and not in the heat of the moment.

If you have *not* kept backups, there is not much you can do. Remember, once a virus has struck, you cannot trust anything the virus could have infected or changed. That includes any non-write protected diskette that was in a drive while the virus was around, even before you discovered the virus.

EXERCISE

1. _____ procedures are the most important preventive action you can take to protect yourself from a viral attack. This is also the least expensive.

2. An employee regularly installs new software and games given to him by a friend. What is the vulnerability here? When installing new software, what security measures would you recommend.

RISK ANALYSIS AND CONTINGENCY PLANNING

FIRE DAMAGE! How would you like to walk in some morning and find this? It would be catastrophic unless you have some kind of recovery plan to cope with such disasters.

Performance of *risk analysis* and development of a *contingency plan* is a critical component of maintaining information security. It assumes greater importance in overseas missions and is, in fact, one of the most important responsibility of the System Security Officer.

Analyzing Risks

The risk analysis or assessment process involves the following steps:

- Identifying assets
- Impact analysis
- Identifying threats and vulnerabilities

The risk analysis process starts with *asset identification*, i.e., identifying the assets present in the automated environment. This includes not only the physical assets, but also any software, data, administrative or personnel resources within the information system.

The next step is to perform an *impact analysis*. What might happen to your operations if the asset is lost or severely impaired?

The third step is to *identify the threats and vulnerabilities* that might endanger the assets. Is the system vulnerable? Who or what is there to fear?

The SSO and SM should examine the automated environment to determine what risks would be faced in case of an emergency. The various categories of threats (discussed earlier) and their consequences should be thoroughly examined.

A *cost-benefit* analysis should then be done, comparing the value of each information resource that is threatened, with the cost of protecting it. This analysis should not only take into consideration the amount of money involved, but also the impact of the loss on the people concerned, and the operations of the Agency.

For example, if the cost of an interrupted computer service is estimated at $100,000, but the cost of preventing the interruption is $1,000,000, should you spend the million? The qualitative response would be no. However, there are other factors that must be *carefully considered* before making that decision.

Making Contingency Plans

Once the risk analysis has been performed, the SSO should develop a step-by-step contingency plan and recovery process.

A *contingency plan* is a set of procedures to ensure that users can continue to perform essential functions, in case there is a disruption of service. The plan should address the various levels of threats, and contain specific actions to be taken in each case.

An effective contingency plan should address the following areas:

- *Backup of critical material* including hard copies of processing agreements with other agencies, etc. Where appropriate, off-site storage areas for information assets, such as disks, data, operating and production libraries, should be considered. Such resources may also be stored at banks or other secured sites through mutual agreements.

- *Precise and detailed documentation* of emergency procedures. The planned emergency responses must be documented very precisely. Specific responsibilities for executing the plan should be identified.

- *Prioritize each activity*. Based on time available for response during an emergency, certain activities will become critical. For example, it may only be possible to hit the emergency power control switch before evacuating the facility, rather than calmly logging off users and powering off the system.

- *Procedures for notifying key personnel*. In case of after hours emergency, the facility guards need to know *whom* to contact (the SSO and SM) and *how* they can be reached.

It is not sufficient to simply have plans. The procedures outlined must be *practiced*. People should know what to do in the case of emergency and be well prepared to do it.

In summary, a contingency plan should include the following:

What must be done: A detailed step-by-step plan about the exact steps to be followed in each of the identified threats or disasters.

In what sequence: Establish the proper sequence. If a deadline is required, or if step is a prerequisite to some other action, specify these requirements.

Who must do it: Assign roles and responsibilities. Each major operation should be assigned to a responsible individual (designated by position), with backups identified. Normally, the SSO or SM should be in overall charge of the recovery effort.

How it should be done: The methods to be followed must be clearly described, especially if nontechnical people are to perform any of the operations.

What is needed to do the job: Determine the amount of money, people and other resources that must be applied to the task. If specific resources (fire extinguishers, alarm systems, etc.) are required, action should be initiated to procure them.

Contingency plans should be *reviewed* at least yearly, and when there is a substantial change in the threat situation.

Both the risk analysis and contingency plans should take into account the overall emergency plans of the Mission (or A.I.D./W), and should be coordinated with the Regional, Post, or Unit Security Officer.

EXERCISE

Using the chart below as a model, perform a risk analysis. The steps in their proper sequence is listed below:

a) Identify 3 assets critical to the functioning of your day-to-day operations.

b) Describe the impact of asset loss or impairment.

c) Is the asset vulnerable to deliberate or accidental attack. If so, by whom or by what?

d) What countermeasures would you take to eliminate or limit the effect of the damage.

ASSETS	IMPACT	THREATS	COUNTERMEASURES
1.			
2.			
3.			

KEY POINTS TO REMEMBER

PROTECT YOUR EQUIPMENT

Keep your equipment in a secure environment. Safeguard from food, drink and other hazards.

PROTECT YOUR FACILITIES

Prevent unauthorized access.

PROTECT YOUR PASSWORD

Don't reveal your passwords to others. Use passwords that are difficult to guess, yet easy to remember.

PROTECT YOUR FILES

Always prevent unauthorized access to files and data.

PROTECT AGAINST COMPUTER VIRUSES

Never use software from unrecognized or unreliable sources.

KEEP STORAGE MEDIA SAFE

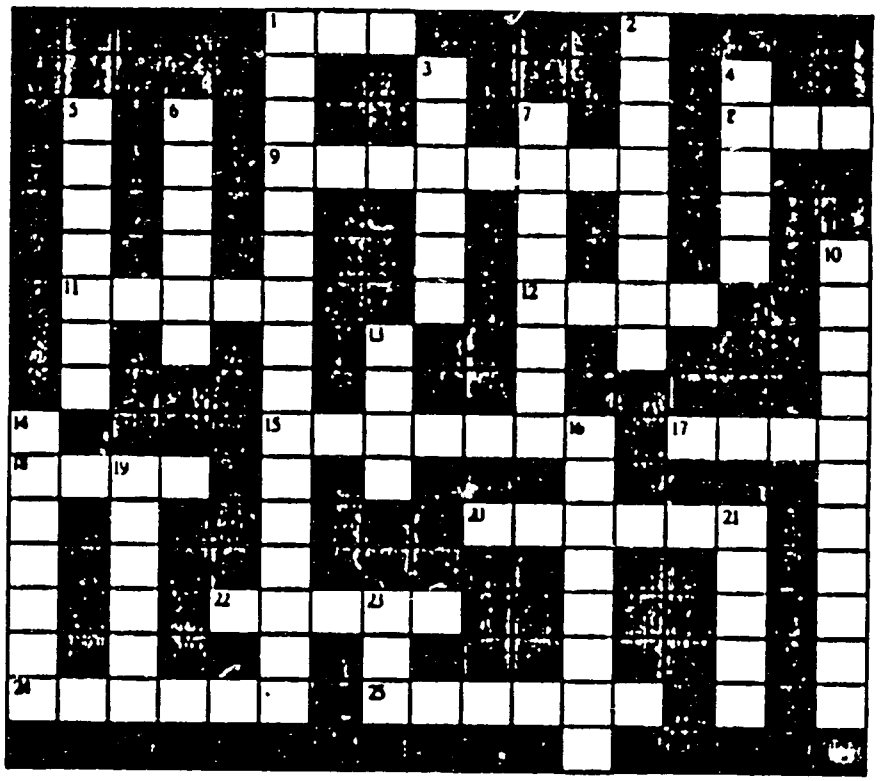
MAKE BACK-UPS OF ALL CRITICAL INFORMATION

Follow a daily or weekly backup policy. Keep back-ups in a secure location.

COMPUTER SECURITY CROSSWORD PUZZLE

ACROSS
1. Monitor
8. Execute
9. Protected word
11. Degauss
12. Electronic intruder
15. Operator
17. Information
18. Cost
20. Download
22. Vulnerability
24. Storage
25. Lock

DOWN
1. Awareness of (2 words)
2. CPU
3. Software, hardware, data
4. Deception
5. Make safe
6. Harm
7. WordPerfect
10. "Beware of hackers bearing gifts!" (2 words)
13. Password
14. Sequence of instructions
16. Backup utility function
19. Interacting elements
21. To remove
23. Uninterrupted power supply (acronym)



What is Wrong With This Office?

Can You Spot at Least 5 Security Hazards?

APPENDIX

Glossary

Access. The ability and the means necessary to approach, store, or retrieve data; to communicate with, or to make use of any resource in an automated environment.

Access Control. The process of limiting access to the resources of the automated system to authorized users, programs, and processes. Synonymous with controlled access, controlled accessibility.

Administrative Security. Operational and accountability procedures to ensure that all personnel who install, operate and maintain computer resources know their responsibilities for system security.

Archiving Workstation. A workstation that has a floppy disk drive onto which information can be copied.

Asset. Any software, data, hardware, administrative, physical, communication or personnel resource within an information system or activity.

Assistant Systems Manager. Performs systems duties under the supervision of the Systems Manager, and may assume the responsibilities of the Systems Manager in his/her absence.

Backup. The process of copying files from one volume to another to protect them from accidental loss.

Bulletin Board System (BBS). A computer that is run as an electronic "bulletin board." People can access the computer and put "notes" on the bulletin board, which anyone else with access can read. A BBS can be anything from someone's hobby to an international commercial BBS like CompuServe. The BBS concept is key to the increasing connectivity available to people with computers and also to the spread of useful programs, information and, unfortunately, viruses.

Bug. An error in a program. Bug refers to unintentional errors, not to things like viruses and logic bombs.

Communications Security. Protection of transmitted data and the physical security of the connecting lines and links.

Contingency Planning. Plan to minimize disruption caused to an organization in case of accidental or deliberate loss of computer resources.

CUE (Controlled User Environment). A security software system developed by the Department of State.

Countermeasures. Any action, device, procedure or technique to direct, oppose or regulate a threat or vulnerability.

Data Integrity. Ensuring accuracy and completeness of data. It addresses the safeguards in the processes of data origination, input, processing and output.

Degauss. To apply an alternating current (AC) field for the purpose of demagnetizing magnetic recording media, and thereby erasing any information it contained thereon.

DES. (Data Encryption Standard) An encryption technique developed by IBM and the National Bureau of Standards for encrypting data.

Encryption. Scrambling data so it becomes unreadable.

Decryption. Processing of unscrambling encrypted data so it is readable.

Enciphering. See Encryption. Process of changing information (plaintext) so that it becomes unreadable. There are many ways to do this; one involves using the Data Encryption Standard (DES). The resulting ciphertext is very difficult or impossible to read without the key used to encrypt it.

FAT (File Allocation Table). Three of the most vital sections of any computer disk are the boot sector, the FAT, and the root directory track. Unfortunately, these three areas are most vulnerable to a virus attack. The FAT contains information about where files are stored on the disk, and keeps track of available storage areas.

FIPS Pubs. Federal Information Processing Standards Publication.

Freeware. Programs distributed on bulletin boards without a charge. (If there is a registration fee, it is called **shareware**). Many software manufactures distribute upgrades for their programs in this way.

Garbageware. Coined term used to refer to diseased programs (software) that contain and spread computer viruses.

Group Access. Common (shared) file access for a group of users.

Hacker. As computer technology has evolved, the term hacker has taken on different meanings. In the early days of computer usage, hacker did not have negative connotations. It originally referred to an intelligent and extremely proficient programmer who could put together an elegant statement of code. Today, a hacker is thought of as a person who attempts to gain unauthorized access to large systems by using PCs.

Halon System. A fire suppression system using Halon gas. Halon is especially suited for computer facilities because it does not damage electronic equipment.

Information Security. Refers to the controls that protect sensitive information from unauthorized access, destruction, modification or disclosure.

LAN (Local Area Network). A data communication facility providing high-speed, switched connections between processors, peripherals, and terminals within a small geographic area.

LOU (Limited Official Use). Certain sensitive official information which is not national security information, but which nevertheless requires a degree of protection.

Logic bomb. Programming code that is preset to cause a later malfunction when a specified set of logical conditions (or activity) occur. For example, a logic bomb may be set to alter all employee records if a specific employee status is changed. A virus can be a type of logic bomb.

MACS. Mission Accounting and Control Systems. The A.I.D. automated accounting system developed for overseas use.

Magnetic Media. Devices on which information is recorded in digital form, such as magnetic tapes, diskettes, and hard disks.

Networks. Associated components interconnected for such functions as communications and resource sharing.

OIS. Wang's Office Information System. Designed primarily for word processing, but also supports list processing, BASIC programming and limited data processing applications.

Orange Book. Department of Defense Trusted Computer System Evaluation Criteria (CSC-STD-001-B3, August, 15, 1983).

Password. A protected word or string of characters that identifies or authenticates a user, specific resource, or access type.

Physical Security. Physical security involve safeguaring *all* computer assets, including the surrounding facilities from theft, physical damage, and unauthorized access. Physical security also encompasses protection against environmental hazards.

Personnel Security. Policies and practices to ensure that employees are well trained, aware of security practices, highly motivated and ethical. If they are not, there is a great potential for serious computer errors, abuse and violations.

Risk Analysis. Formal process of analyzing risks and vulnerabilities, determining how likely they are to occur, and coming up with some probabilities figures that are used as part of the process for formatting a protection strategy.

Security Policies and Procedures. The rules and practices that regulate how an organization manages, protects, and distributes automated information resources.

Shareware. Programs distributed on bulletin boards for a small charge or fee.

System. An assembly of hardware and software configured for the purpose of processing, transmitting and receiving, storing and retrieving data.

Systems Manager (SM). The individual responsible for the day-to-day operations of the automated system.

System Users. Individuals who use the system in the performance of their work.

Systems Operator. An individual, normally on the systems staff, whose job it is to perform the routine operational functions of the automated system.

Systems Security Officer (SSO). An Officer designated to manage information system security in each Agency element.

Systems Programmer. Software developer responsible for the design, development, installation and documentation of the operation system, peripheral utility programs and modifications.

Threat. Any activity, deliberate or unintentional, with the potential for causing harm to an automated information system.

TEMPEST. Term used to refer to automated information system components that use approved emanation suppression/containment systems for the processing and storage of classified national security information.

Time Bomb. Programming code that is preset to cause a later malfunction after a specific time and date. A virus can be a type of time bomb.

Trojan Horse. In Homeric legend, the Greeks gained entry into Troy by concealing troops in a wooden horse that the Trojans took inside the city walls. In computer security, a Trojan Horse is an apparently useful program that does things in addition to what it is advertised to do. For example, it might be advertised as a disk compression utility, and it may indeed compress data on your disk. It might, however also copy a virus into your COMMAND.COM file.

UPS. (Uninterruptible Power Supply). A system that maintains AC power during a temporary outage by continuing to derive DC power from batteries and converting it to AC power.

Vaccine. Program or group of programs that provide some kind of protection against computer viruses.

Virus. A small program that contains instructions to attack software and provide unauthorized access into a computer system. For example, a virus attack may be able to erase data, alter programs and even display nasty messages on the screens. The key feature of a virus is that it can replicate by attaching itself to the programs or disks, it comes in contact with, thus affecting a vast network of programs and users.

Vulnerability. A flaw or weakness in the environment that can cause harm to computer assets.

Worm. Malicious programs that *wind* their way through the memory or hard disk of a computer altering small bits of data or code or replacing them with zeros. The worm does not reproduce, but moves itself around (a kind of reproducing) each time it does something. It can be very hard to find a worm even if you know it is there and is doing damage. Many viruses are also worms.

Most of the glossary is drawn from the A.I.D. Automation Security Guidebook, and other sources referenced in the bibliography. Some definitions are quoted verbatim from the sources.

Recent Occurrences of Computer Viruses

Here are some examples of famous viruses, beginning with the much-publicized Internet incident:

- On November 2, 1988, Internet (a global computer network built around the Defence Department's Arpanet) was invaded by a worm program. In less than two days, an estimated 6,000+ Unix-based computer systems on the network were infected. The worm, written by a graduate student with no apparent intent to cause damage, used several different methods for penetrating systems and then reproducing and hiding itself. Estimates of the cost of this incident to the organizations affected (for cleanup and testing) range from $20 to $95 million.

- In March 1988, Aldus Corp., vendors of desktop publishing software, inadvertently shipped hundreds of copies of a new software product containing a virus (fortunately a relatively benign one) which had crept in from a testing site.

- On January 10, 1988, Newsday reported that thousands of computers at Hebrew University in Jerusalem were infected with a virus designed to wipe out all hard disks on the next Friday the 13th. Following an exhaustive investigation, university officials said that the virus infection (which was discovered accidentally) had spread to the point where it could have destroyed years of university research, financial information, and student files.

- On December 11, 1987, an electronic mail "Christmas card" created such a surge in mail traffic on IBM's worldwide mainframe network that it dramatically degraded the network's performance. The message automatically displayed a Christmas card on the user's screen, forwarded copies of itself to every name and address on the user's distribution lists, and then deleted itself from the user's mail directory. It was ultimately discovered that the 20-line program was created by a West German student. At its peak more than 500,000 copies of this virus-like program appeared on the network in a two-hour period.

Excerpts from A Manager's Guide to Computer Viruses
Computer Security Institute

Bibliography

This bibliography not only lists books and other documents that have formed the background material for the courseware, but also references certain general books and reports that will be useful to you in further study.

Automation Security Guidebook. (1988). Office of Information Resources Management: A.I.D.

Cohen, F. (1984). "Computer Viruses: Theory and Experiments." *Proceedings of the 7th National Computer Security Conference:* 240-263. Gaithersburg, MD: National Bureau of Standards.

Cooper, A.J. (1989). "Computer and Communications Security: Strategies for the 1990's". New York: McGraw Hill Publishing Company.

Computer. (1983). "Computer Security Technology." *Computer* 16(7).

Davies, D., ed. (1981). *The Security of Data in Networks*. Los Angeles, CA: IEEE Computer Security.

Denning, D.E. (1983). *Cryptography and Data Security*. Reading, MA: Addison-Wesley.

Executive Briefing and Computer Security Training. (1988). U.S. Office of Personnel Management.

Fites, P., Johnston, P., and Kratz, M. (1988). *The Computer Virus Crisis*, Van Nostrand Reinhold, New York.

Gasser, Morrie. (1988). *Building a Secure Computer System*. New York: Van Nostrand Reinhold Company.

Hutt, A.E., Bosworth, S and Hoyt, D.B. ed (1987). *Computer Security Handbook*. Boston, MA: Macmillan Publishing Co.

Honan, Patrick. (1989). "Avoiding Virus Hysteria." *Personal Computing*.

Landwehr, C.E. (1983). "The Best Available Technologies for Computer Security." *Advanced in Computer Security*, vol. 2, ed, R. Turn, pp. 198-22. Dedham, Mass.: Artech House (1984).

Lobel, J. (1986). *Foiling the System Breakers: Computer Security and Access Control.* New York: McGraw-Hill.

McNamara, Joel. (1988). "For Your Eyes Only". *MacUser.*

Pfleeger, Chuck. (1989). *Security Computing.* New York: Prentice Hall.

Saltzer, J.H., and Schroeder, M.D. (1975). "The Protection of Information in Computer Systems." *Advances in Computer System Security*, vol. 1, 3rd. R. Turn, pp. 105-165. Dedham, Mass.: Artech House (1981).

Seymour, Jim, and Jonathan Matzkin. (1988). "Confronting the Growing Threat of Harmful Computer Software Viruses." *PC Magazine, June 28, 1988.*

Shapiro, Neil L. (1988). "Viral Infection". *MacUser Magazine 4, No. 5.*

Turn, R., ed. 1981, (1984). *Advances in Computer System Security.* Vol. 1 and 2, Dedham, MA: Artech House.