COMPUTERS

Crimes, Clues and Controls

Prepared by the Prevention Committee
President's Council on Integrity and Efficiency
as part of its continuing effort to prevent fraud,
waste, and abuse in government programs.

SOMETHING CAN BE DONE

"I have asked myself many times if my agency could have done anything to predict that I, and people like me, would initiate fraud against its computer. The answer is yes."

SECURITY CONTROLS

"The computers were like unlocked bank vaults waiting to be invaded. Security around these machines was almost nonexistent. If the bank vault has money in it and if nobody is watching, somebody, for whatever reason, is likely to steal from it."

PERSONNEL SECURITY

"A more alert personnel security system might have flagged me or someone like me as a risk...I had personal problems because I was $20,000 in debt...They passed me over for a promotion. I was good and deserved more. I decided to get back at them."

SECURITY ATTITUDE

"The problem is also one of attitude. The attitude that security is important seems to be lacking."

Former Government Employee
Convicted of Computer Crime

108970

COMPUTERS: CRIMES, CLUES AND CONTROLS

A Management Guide

Prepared by the Prevention Committee
President's Council on Integrity and Efficiency
as part of its continuing effort to prevent fraud,
waste, and abuse in government programs.

March 1986

PREFACE

Computer crime causes significant financial losses. But of at least equal concern is the computer-related waste and abuse caused unintentionally as a result of not knowing how to safeguard information resources.

This document is designed to heighten your information security awareness and increase your information security knowledge. It is concerned with preventing unauthorized access, disclosure, delay, alteration, destruction or other misuse of automated, unclassified sensitive data.

This document is specifically addressed to you:

- If you are an end user of automated information;

- If this information is sensitive (i.e., information whose improper use or disclosure could affect adversely the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act); and

- If you are a manager.

Regardless of whether you are the target audience or whether you have responsibility for all of the vulnerable areas or suggested controls, you will find this document of assistance in protecting information resources if you use a word processor or computer in carrying out your job responsibilities.

The controls and techniques in this document are for information purposes and should be used to supplement your agency's information security program. Although the securing of classified information is beyond the scope of this document, many security concerns are the same and the controls presented herein may be appropriate.

These controls and techniques are not mandatory and are not the only information security measures which can be taken. Following these measures will not ensure that misuse of information will be prevented, but it will limit the possibility.

Security issues are addressed in three areas: **information security, physical security, and personnel security**. In each area, **crimes, clues** and **controls** are discussed. This document concludes with a **plan of action** and **sources for assistance.**

The Prevention Committee, President's Council on Integrity and Efficiency, is pleased to make *Computers: Crimes, Clues and Controls* available. Your awareness of the wide spectrum of vulnerabilities and available safeguards is invaluable to the success of a total information security program.

Joseph H. Sherick
Inspector General, Department of Defense
Chairman, Prevention Committee
President's Council on Integrity and Efficiency

ACKNOWLEDGEMENTS

The Prevention Committee of the President's Council on Integrity and Efficiency would like to acknowledge the generous contribution to *Computers: Crimes, Clues and Controls* by the Inspector General at the Department of Defense whose office initiated and directed this project, and by the Inspectors General at the Departments of Energy, General Services Administration, and Health and Human Services, taskforce members.

During the developmental phase, offices with expertise in information security policies and practices, computer fraud and abuse detection and prevention, and management helped shape this document. These offices include: Office of the Deputy Assistant Secretary for Information Systems, Department of the Treasury; Office of Information Regulatory Affairs and Division of Management Improvement, Office of Management and Budget; Office of Inspector General, Small Business Administration; and several offices within the Department of Defense (DoD) including the Office of the Assistant Secretary of Defense (Comptroller); the DoD Computer Institute (DoDCI), National Defense University; and Computer Crime Division, Office of Special Investigations, U.S. Air Force.

The Prevention Committee is especially grateful for the technical expertise ably provided by these offices: Institute for Computer Science and Technology, National Bureau of Standards, Department of Commerce; Office of Information Technology, Department of Justice; and offices at DoD including DoDCI, the National Center for Computer Security, National Security Agency, and Office of Information Systems, Office of the Assistant Secretary for Defense (Command, Control and Communications Intelligence).

In the past, users of automated information and computers assumed that security was a technical problem and not their concern. That has changed, and managers and users recognize the opportunity to further safeguard valuable government resources by making security information available and understandable to nontechnical users.

COMPUTERS: CRIMES, CLUES AND CONTROLS

A Management Guide

TABLE OF CONTENTS

1. COMPUTERS: CRIMES, CLUES, AND CONTROLS

Introduction

The Information Age has brought about dramatic improvements in the way the Federal government does its job. For making decisions, more and better information is available more quickly to more people than ever before. Statistical computations that once took weeks now take minutes. And analyses that once required numerous programmers, a computer operator, and a large computer facility may now need only a nontechnical staff using software packages on desktop computers in their office.

The General Services Administration estimates that Federal agencies will acquire half a million small computers by 1990. In FY 1984, Federal expenditures for micro and desktop computers totaled $137 million. The comparable figure in FY 1983 was $34 million. And these statistics do not include computer terminals that are part of a large computer system or word processors --many of which can be used to store and manipulate data, as well as create graphics. **The Office of Management and Budget (OMB) estimates that $13.9 billion was spent in FY 1985 to acquire, operate, and maintain Federal information technology systems.**

New management problems have accompanied the increased use of computers and automated technology. Terminals, often connected to computers that are networked together, can access vast quantities and different types of data. There are publicly voiced concerns about privacy of information and the risks associated with automating and making more accessible personal, proprietary, or other sensitive data. There are serious concerns about increased computer crime, waste, and abuse which result in such costly problems as improper payments from government benefit programs and unnecessary equipment purchases. And there is the clear recognition that information is a resource to be protected.

The responsibility for protecting information resides with the end user manager. This responsibility is acknowledged in OMB Circular A-130, *Management of Federal Information Resources*:

> *"Agencies shall make the official whose program an information system supports responsible and accountable for the products of that system....*
>
> *"Because end user computing places management of information in the hands of individual agency personnel rather than in a central automatic data processing organization, the Circular requires that agencies train end users in their responsibilities for safeguarding information."*

This document is designed to provide information security awareness training for the end user manager. Security awareness training acquaints end user managers with the vulnerabilities of automated information systems, controls, and techniques that enhance information security and with resources available for additional information.

"YOU'VE GOT TO CONSIDER YIELD. IT'S $19,000 PER BANK ROBBERY AND $560,000 PER COMPUTER CRIME!"

Computer crime is a growth industry --and so are computer waste and abuse. Some estimates peg the increase of computer crime at 35 percent annually and the cost at $3.5 billion. One obvious reason is the potential payoff: the average computer crime yields an estimated $560,000; the typical bank robbery, $19,000.

The computer criminal is less likely to get caught than the bank robber --and less likely to get convicted, if caught. Estimates of detected computer crimes are as low as 1 percent. And the likelihood of a criminal conviction for computer fraud is less than 1 in 10.

Deliberate computer crime is a significant part of the picture. But wasteful and abusive practices, accidents and errors are an even larger part. In the succinct words of one noted expert, "*We bumble away far more computer dollars than we could ever steal.*" Those bumbled dollars -- combined with the estimated $3.5 billion annual cost of computer crime-- underscore the scope and seriousness of computer-related losses.

A major contributor to computer-related losses is the lack of security awareness. Security awareness can stop accidents and errors, promote adequate information security controls, and prevent and detect the would-be computer criminal. End user awareness of security controls provides four levels of protection for computers and information resources:

SECURITY CONTROLS: FOUR LEVELS OF PROTECTION

Prevention -- *Restricts access to information and technology to authorized personnel who perform only authorized functions;*

Detection -- *Provides for early discovery of crimes and abuses if prevention mechanisms are circumvented;*

Limitation -- *Restricts losses if crime occurs despite prevention and detection controls; and*

Recovery -- *Provides for efficient information recovery through fully documented and tested contingency plans.*

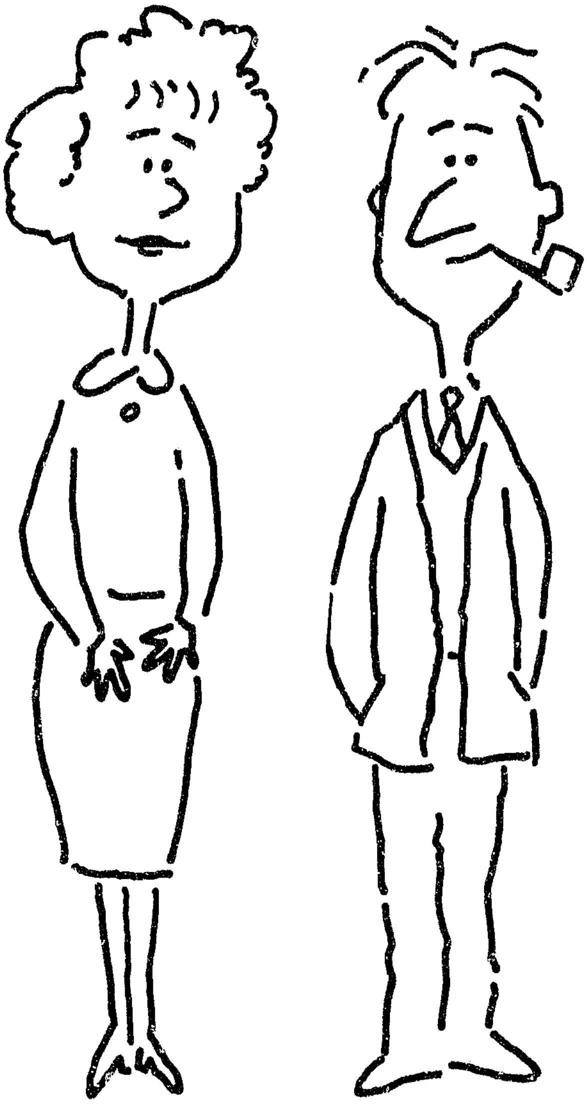
Yesterday, **managing technology** was the **technical manager's** concern. Today, **managing information is every nontechnical end user manager's** concern. Managing information requires new knowledge and new awareness by a new group of nontechnical employees. Good information management requires recognizing opportunities for computer crime and waste so that steps can be taken to prevent their occurrence.

When computers were first introduced, few were available and only a small number of persons were trained to use them. Computers were usually housed in separate, large areas far removed from program managers, analysts, economists, and statisticians. Today that is changed. Word processors, computer terminals, and desktop computers are common equipment. This electronic equipment is rapidly becoming increasingly user-friendly so that many people quickly and easily learn to use it.

Employees with access to computer equipment and automated information are greatly increasing throughout the organizational hierarchy. The GS-4 secretary, the GS-9 budget analyst, the GS-12 program analyst, the GS-13 statistician, the GM-14 economist, and the Senior Executive Service manager may all have access to a computer terminal or word processor and the information it contains.

No longer is information restricted to a select few at the highest levels of an organization. This phenomenon has led computer crime to be called the "*democratization of crime.*" **As more people gain access to automated information and equipment, the opportunities for crime, waste, and abuse likewise increase.**

It's Difficult to Generalize, But....



-- Functional end user, not the technical type and not a hacker

-- Holds a non-supervisory position

-- No previous criminal record

-- Bright, motivated, desirable employee

-- Works long hours; may take few vacations

-- Not sophisticated in computer use

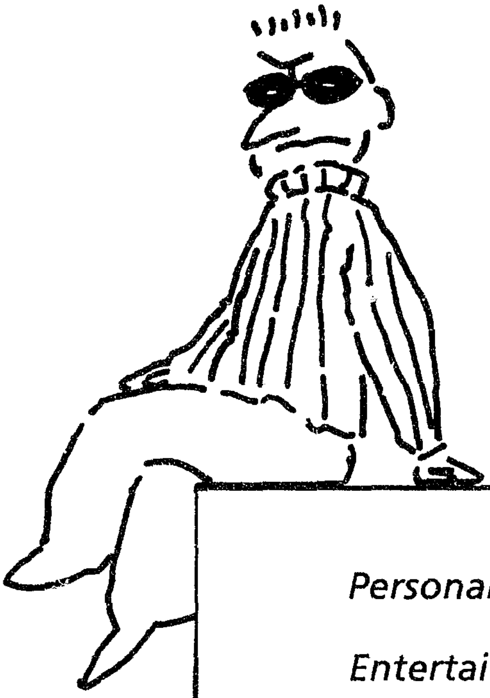
-- The last person you would suspect

-- Just the person you would want to hire.

THE COMPUTER CROOK CAN BE ANYONE

The typical computer crook is not the precocious hacker who uses a telephone and home computer to gain access to major computer systems. The typical computer crook is an employee who is a legitimate and nontechnical end user of the system. Nationally, employee-committed crime, waste, and abuse account for an estimated 70 to 80 percent of the annual loss related to computers. Dishonest and disgruntled employees cause an estimated 20 percent of the total computer-related loss. And they do so for a variety of reasons.

WHY PEOPLE COMMIT COMPUTER CRIME



Personal or Financial Gain

Entertainment

Revenge

Personal Favor

Beat the System, Challenge

Accident

Vandalism

But a significantly larger dollar amount, about 60 percent of the total computer-related loss, is caused by employees through human errors and accidents. Preventing computer losses, whether the result of deliberately committed crimes or unknowingly caused waste, requires security knowledge and security awareness. A recent survey reported that observant employees were the primary means of detecting computer crime.

CLUES TO COMPUTER CRIME AND ABUSE

BE ON THE LOOKOUT FOR....

- Unauthorized use of computer time
- Unauthorized use of or attempts to access data files
- Theft of computer supplies
- Theft of computer software
- Theft of computer hardware
- Physical damage to hardware
- Data or software destruction
- Unauthorized possession of computer disks, tapes or printouts

This is a beginning list of the kinds of clues to look for in detecting computer crime, waste and abuse. Sometimes clues suggest that a crime has been committed or an abusive practice has occurred. Clues can also highlight system vulnerabilities --identify where loopholes exist-- and help identify changes which should be made. Whereas clues can help detect crime and abuse, controls can help prevent them.

Controls are management-initiated safeguards --policies or administrative procedures, hardware devices or software additions-- the primary mission of which is to prevent crime and abuse by not allowing them to occur. Controls can also serve a limitation function by restricting the losses should a crime or abuse occur.

This document addresses information security in three areas: ***information security, physical security, and personnel security.*** *In each area,* ***crimes, clues, and controls*** *are discussed. In these areas not only frauds, but abuses and waste are addressed. The final chapters provide* ***a plan of action*** *and cite* ***available security resources.***

2. INFORMATION SECURITY

What was called computer security in the 1960s and data security in the 1970s is today more accurately called information security. Information security underscores the value of information in today's society --the recognition that information is a valuable resource, that it is more than discrete data elements.

Information security refers to the controls that protect information from unauthorized access, destruction, modification, disclosure, and delay. Information security addresses safeguards in the processes of data origination, input, processing, and output. The goal of information security is to safeguard the system's assets, to protect and ensure the accuracy and integrity of information, and to minimize the damage that does occur if the information is modified or destroyed. Information security requires accountability for all events that create, modify, provide access to, or disseminate information.

Information security provides assurances that the following are achieved:

- ***Confidentiality*** of sensitive information;
- ***Integrity*** of information and the related processes (origination, input, processing, and output);
- ***Availability*** of information when needed; and
- ***Accountability*** of the related information processes.

Some techniques to protect the system and provide accountability can be built into the computer. Others can be built into the software. Still others are dependent upon management policies to define appropriate procedures to be followed. Deciding upon the level of sophistication of accountability techniques for a system requires identifying the sensitivity of the information and then determining the appropriate level of security.

This document addresses sensitive data as defined in OMB Circular A-130, *Management of Federal Information Resources:*

> *The term "sensitive data" means data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.*

CRIMES, ABUSES, AND WASTE

A survey of government agencies identified techniques used in committing computer-related fraud and abuse. Few of these frauds and abuses involved destruction of computer equipment or data. Only 3 percent of the frauds and 8 percent of the abuses involved willful damage or destruction of equipment, software or data. Most of the fraud and abuse cases involved information --manipulating it, creating it, and using it.

THE FIVE MOST COMMON TECHNIQUES* USED TO COMMIT COMPUTER-RELATED FRAUD AND ABUSE

Computer-Related Fraud

1. Entering unauthorized information
2. Manipulating authorized input information
3. Manipulating or improperly using information files and records
4. Creating unauthorized files and records
5. Overriding internal controls

Computer-Related Abuse

1. Stealing computer time, software, information, or equipment
2. Entering unauthorized information
3. Creating unauthorized information files and records
4. Developing computer programs for nonwork purposes
5. Manipulating or improperly using computer processing

*These techniques are often used in combination and are identified in *Computer-Related Fraud and Abuse in Government Agencies*, Department of Health and Human Services, Office of Inspector General, 1983.

Another way of looking at computer-related crime is to examine the types of crimes and abuses, and the methods used to commit them. These include:

"Data Diddling" Probably the most common method used to commit computer crime because it does not require sophisticated technical knowledge and is relatively safe. Information is changed at the time of input to the computer or during output. For example, at input, documents may be forged, valid disks exchanged, and data falsified.

"Browsing" Another common method of obtaining information which can lead to crime. Employees looking in others' files have discovered personal information about coworkers. Ways to gain access to computer files or to alter them have been found in trash containers by persons looking for such information. Disks left on desks have been read, copied and stolen. The very sophisticated browser may even be able to look for residual information left in the computer or on storage media after the completion of a job.

"Trojan Horse" This method assumes that no one will notice that a computer program was altered to include another function before it was ever used. A computer program with a valid, useful function is written to contain additional hidden functions that exploit the security features of the system.

"Trap Door" This method relies on a hidden software or hardware mechanism that permits system protection methods to be circumvented. The mechanism is activated in some nonapparent manner. Sometimes the program is written so that a specific event, e.g., number of transactions processed or a certain calendar date, will cause the unauthorized mechanism to function.

"Salami Technique" So named because this technique relies on taking slices so small that the whole is not obviously affected. This technique is usually accomplished by altering a computer program. For example, benefit payments may be rounded down a few cents and these funds, which can be considerable in the aggregate, diverted to a fraudulent account.

"Superzapping" Named after the program used in many computer centers which bypasses all system controls and is designed to be used in time of an emergency. Possession of this "master key" gives the holder opportunity to access, at any time, the computer and its information.

Examples of computer-related crimes, abuses, and waste include:

- *A payroll clerk, notified of a beneficiary's death, opened a bank account using the beneficiary's name and social security number. The beneficiary was not removed from the computer eligibility lists, but a computer input form changed the address and requested direct deposit of benefits to the payroll clerk's new bank account.*

- *A major loss occurred with the diversion of government equipment. Fictitious requisitions were prepared for routine ordering at a major purchasing center. The requisitions directed shipment of communications equipment to legitimate private corporations holding government contracts. Just prior to the delivery date, one of the conspirators would call the corporation* *to alert them to the "error" and arrange "proper" delivery of the equipment to the conspirators.*

- *Three data clerks, using a remote terminal, entered phony claims into the computer to receive over $150,000 in benefits and then deleted records of these transactions to avoid being caught.*

- *Thefts of information commonly involve selling either personnel information, contract negotiation information (e.g., contract bids), and company proprietary information (e.g., product engineering information) for outside commercial use, or copying or using software programs for personal or personal business use.*

CLUES

The following clues can indicate information security vulnerabilities:

1. Security policies and practices are nonexistent or not followed. No one is assigned responsibility for information security.

2. Passwords are posted next to computer terminals, written in obvious places, shared with others, or appear on the computer screen when they are entered.

"HERE, USE MY PASSWORD. IT'S 1234."

3. Remote terminals, microcomputers, and word processors are left on and unattended during work or nonwork hours. Data is displayed on unattended computer screens.

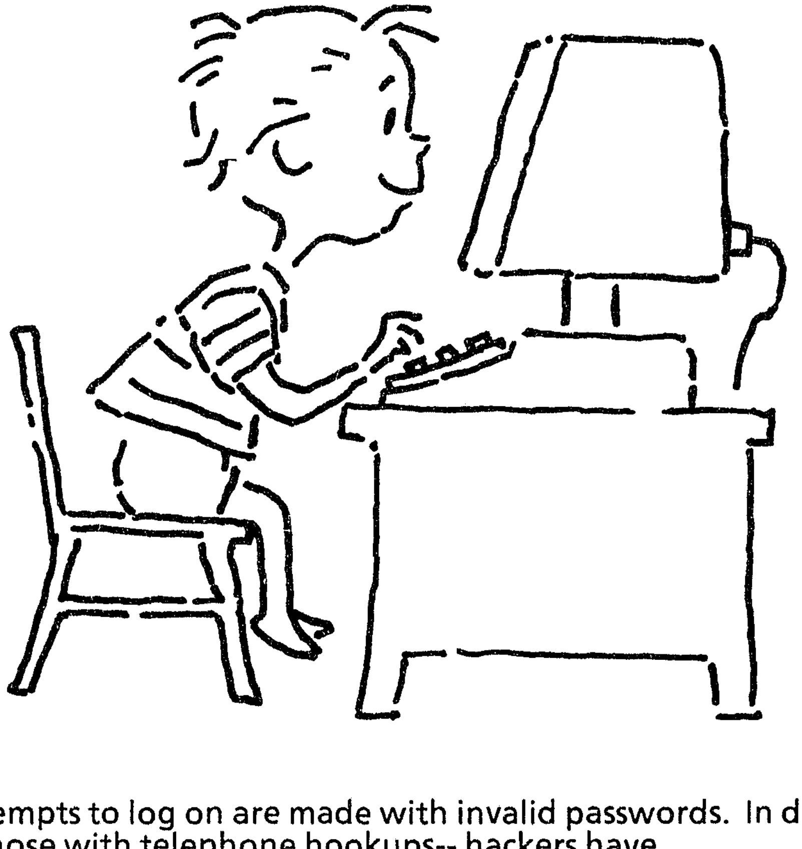
4. There are no restrictions on users of the information, or on the application they can use. All users can access all information and use all the system functions.

5. There are no audit trails, and no logs are kept of who uses the computer for which operations.

6. Programming changes can be made without going through a review and approval process.

7. Documentation is nonexistent or inadequate to do any of the following: understand report definitions and calculations; modify programs; prepare data input; correct errors; evaluate system controls; and understand the data base itself --its sources, records, layout and data relationships.

"WOW! IT'S THE FEDERAL GOVERNMENT!"



8. Numerous attempts to log on are made with invalid passwords. In dial-up systems --those with telephone hookups-- hackers have programmed computers to do this "trial and error" guessing for them.

9. Input data is not subject to any verification or accuracy checks, or, when input data is checked:

   -- *more data is rejected;*
   -- *more data adjustments are made to force reconciliation; or*
   -- *there is no record of rejected transactions.*

10. There are excessive system crashes.

11. No reviews are made of computer information to determine the level of security required.

12. Little attention is paid to information security. Even if an information policy exists, there is a prevailing view that it really is not needed.

INFORMATION SECURITY CONTROLS

1. ***Control access to both computer information and computer applications. Ensure only authorized users have access.***

   User Identification:

   Require users to log on to the computer as a means of initial identification. To effectively control a microcomputer, it may be most cost-effective to use it as a single user system. Typically, a microcomputer has no log-on procedures; authority to use the system is granted by simply turning on the computer.

   User Authentication:

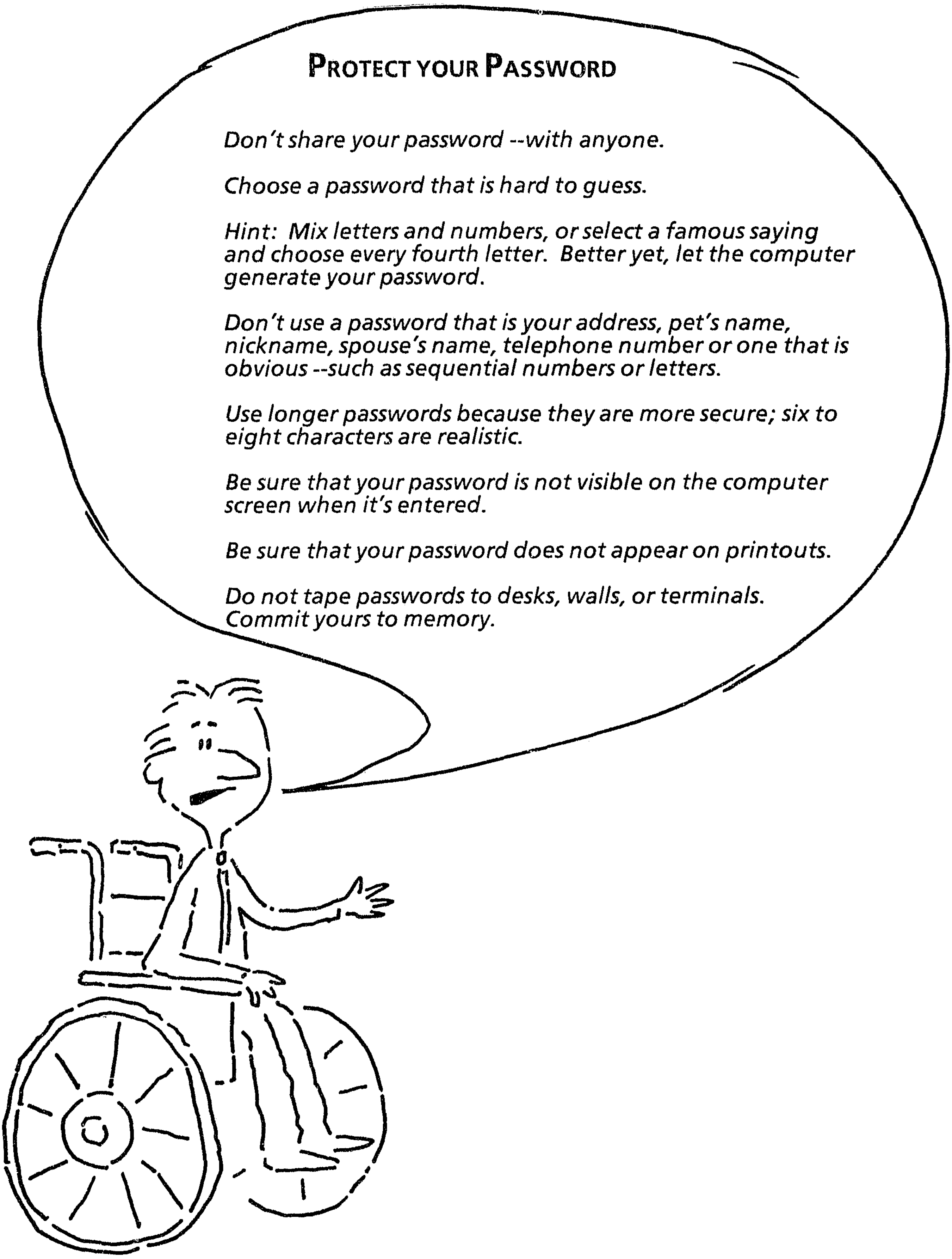
   Use nontransferable passwords, avoiding traceable personal data, to authenticate the identity of users. Establish password management protection controls, and educate users to common problems.

   Other Controls:

   Passwords are one type of identification --something the user knows. Two other types of identification which are effective are something the user has --such as a magnetic coded card-- or a distinguishing user characteristic --such as a voice print.

   If the computer has a built-in default password (a password that comes built into the computer software and overrides all access controls) be sure it gets changed.

   Consider having the computer programmed so that when users log on, they are told the last time of its use and the number of invalid log-on attempts since then. This makes the user an important part of the audit trail.



Protect your Password

Don't share your password --with anyone.

Choose a password that is hard to guess.

Hint: Mix letters and numbers, or select a famous saying and choose every fourth letter. Better yet, let the computer generate your password.

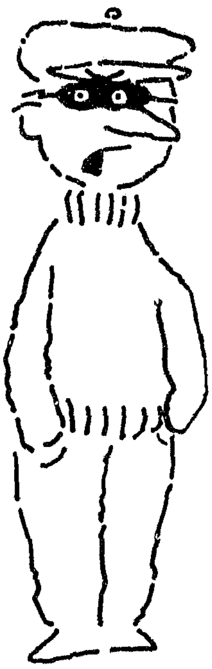
Don't use a password that is your address, pet's name, nickname, spouse's name, telephone number or one that is obvious --such as sequential numbers or letters.

Use longer passwords because they are more secure; six to eight characters are realistic.

Be sure that your password is not visible on the computer screen when it's entered.

Be sure that your password does not appear on printouts.

Do not tape passwords to desks, walls, or terminals. Commit yours to memory.



MANAGE PASSWORDS CAREFULLY

Change passwords periodically and on an irregular schedule.

Encrypt or otherwise protect from unauthorized access the computer-stored password file.

Assign password administration to only the most trusted officials.

Do not use a common password for everyone in an area.

Invalidate their passwords when individuals leave the organization.

Have individuals sign for their passwords.

Establish and enforce password rules --and be sure everyone knows them.

Authorization Procedures:

Develop authorization procedures that identify which users have access to which information and which applications --and use appropriate controls.

Establish procedures to require management approval to use computer resources, gain authorization to specific information and applications, and receive a password.

File Protection:

In addition to user identification and authorization procedures, develop procedures to restrict access to data files:

-- *Use external file and internal file labels to identify the type of information contained and the required security level;*

-- *Restrict access to related areas that contain data files such as off-site backup facilities, on-site file libraries, and off-line files; and*

-- *Use software, hardware, and procedural controls to restrict access to on-line files to authorized users.*

System Protection:

Take precautions to prevent system access:

-- *Turn off idle terminals;*

-- *Lock rooms where terminals are located;*

-- *Position computer screens away from doorways, windows, and heavily trafficked areas;*

-- *Install security equipment, such as devices that limit the number of unsuccessful log-on attempts or that dial back would-be users who use telephones to access the computer;*

-- *Program the terminal to shut down after a specific time of non-use; and*

-- *If feasible, shut down the system during nonbusiness hours.*

2. ***Protect the integrity of information. Input information should be authorized, complete, accurate, and subject to error checks.***

Information Integrity:

Verify information accuracy by using procedures that compare what was processed against what was supposed to have been processed. For example, controls can compare totals or check sequence numbers.

Check input accuracy by installing checks on data validation and verification, such as:

character checks that compare input characters against the expected type of character (e.g., numeric or alpha);

range checks that check input data against predetermined upper and lower limits;

relationship checks that compare input data to data on a master record file;

reasonableness checks that compare input data to an expected standard; and

transaction limits that check input data against administratively set ceilings on specified transactions.

Trace transactions through the system using transaction lists.

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

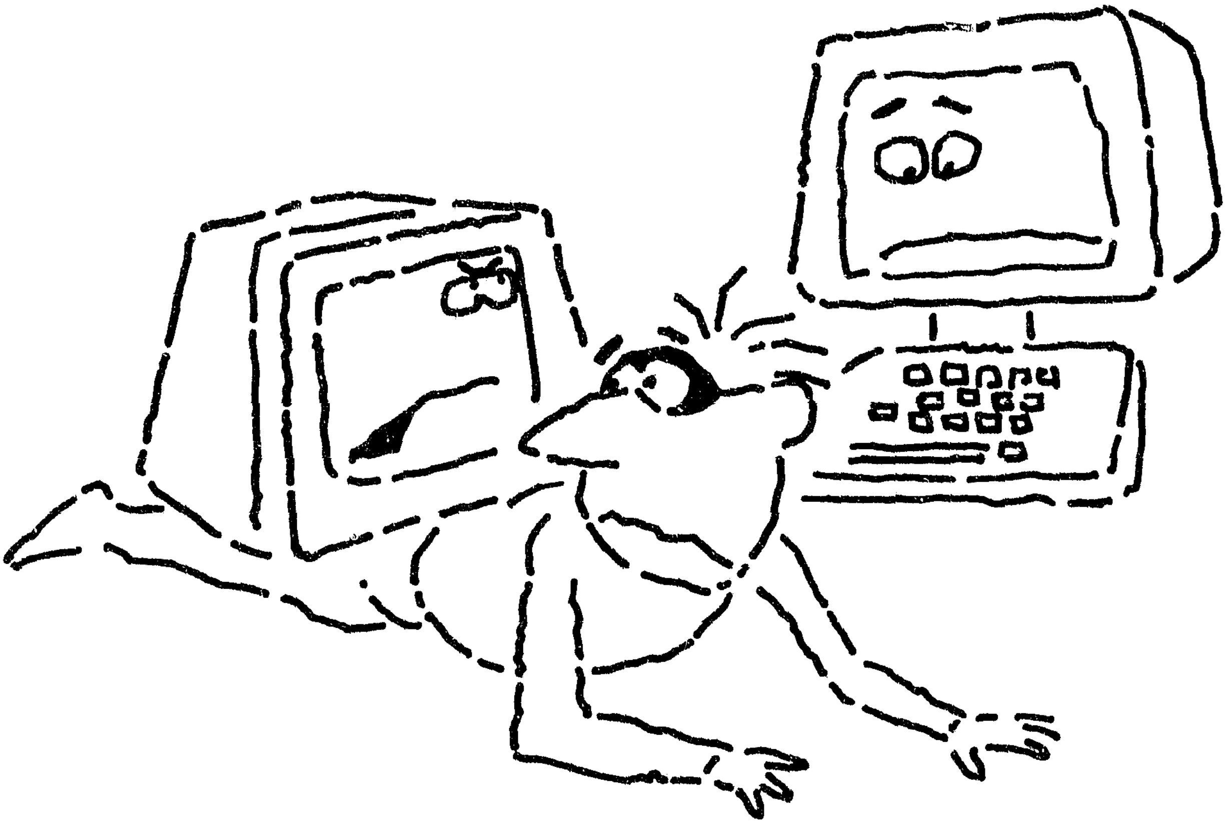
3. ***Protect system software. If software is shared, protect it from undetected modification by ensuring that policies, developmental controls and life cycle controls are in place, and that users are educated to security policies.***

   Software developmental controls and policies should include procedures for changing, accepting and testing software prior to implementation. Policies should require management approval for software changes, limit who can make software changes, and address maintaining documentation.

   An inventory of software applications should be developed and maintained.

   Controls should be installed that prevent unauthorized persons from obtaining, altering, or adding programs via remote terminals.

4. ***Enhance the adequacy of security controls by involving ADP auditors in evaluating applications program controls and consulting them to determine needed tests and checks in handling sensitive data. Audit trails built into computer programs can both deter and detect computer fraud and abuse.***



"WHY DON'T __WE__ EVER GET THE CREDIT?"

Security audit trails should be available to track the identity of users who update sensitive information files.

If the sensitivity of information stored on microcomputers requires audit trails, then both physical and access controls are essential.

In a computer network, the host computer, not the terminal, is where audit trails should be located.

Audit trails should not be switched off to improve processing speed.

Audit trail printouts should be reviewed regularly and frequently.

5. ***Consider the need for communications security. Data transmitted over unprotected lines can be intercepted or passive eavesdropping can occur.***

3. PHYSICAL SECURITY

Traditional Security: Locks, Fences, and Guards

Physical security once meant keeping a computer and its information from physical harm by surrounding the computer facility with locks, fences, and guards. But physical security has changed to accommodate the realities of today's computer environment --an environment that is often a typical office setting with many small computers, word processors, and portable terminals.

Physical security is concerned with controls that protect against natural disasters (e.g., fires, floods, or earthquakes), intruders or vandals, environmental hazards (e.g., power fluctuations), and accidents. Physical security controls regulate the environment surrounding the computer, the data input, and the information products. In addition to the site where computer equipment is housed, the environment includes program libraries, logs, records, magnetic media, backup storage areas, and utility rooms.

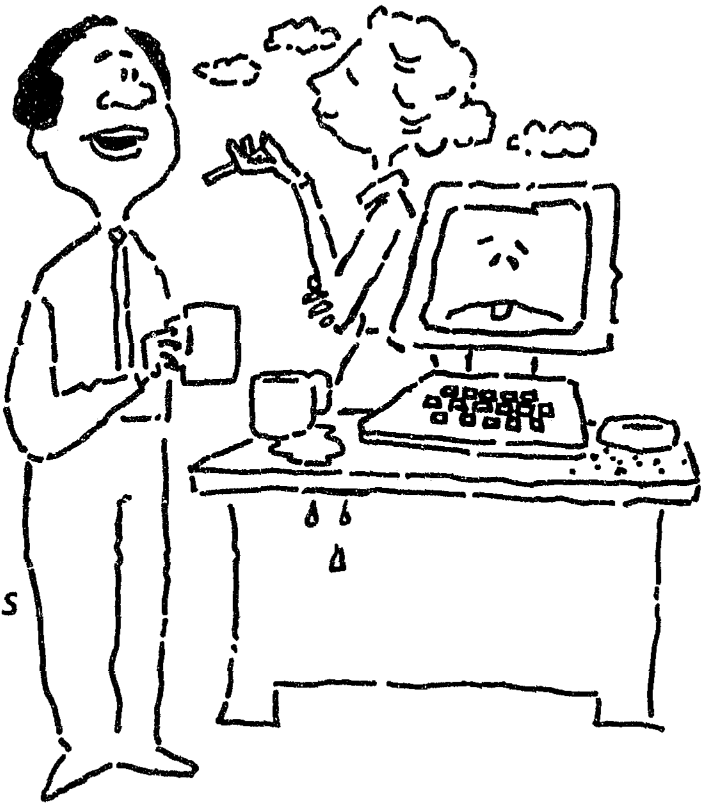
Whether physical security controls are called environment controls, installation controls, or technical controls, they must be responsive to today's environment and they must be cost-effective. For example, installing costly fire suppression systems may be essential to protect a large computer that processes sensitive data but may not be justifiable to protect a single microcomputer.

CRIMES, ABUSES, AND WASTE

Computers have been shot, stabbed, stolen, and intentionally electrically shorted out. Disks and tapes have been destroyed by spilled beverages, and computers have been harmed by water leaks. Computers have been seriously damaged by temperature extremes, fire, electric power surges, natural disasters, and a host of accidents. Information has been intercepted, stolen, sold, and used for the personal gain of an individual or for the benefit of a company.

- *Small computers are an especially attractive target for thieves.*
- *During a fire, disks stored in nonfireproof cabinets and floppy disks left next to computer terminals were destroyed by a sprinkler system. Thousands of dollars were spent reconstructing the information they contained.*

But accidents and ordinary contaminants are probably the major cause of damage to computers and related equipment.



COMPUTER GERMS:

SPILLS, SMOKE, AND CRUMBS
HEAT AND HUMIDITY

CLUES

The following clues can indicate physical security vulnerabilities:

1. Smoking, eating, and drinking are permitted in the computer work area.

2. Computer equipment is left unattended in unlocked rooms or is otherwise unsecured.

3. There is no fire alert or fire protection system.

4. Disks are left in desk drawers; there are no backup copies of disks.

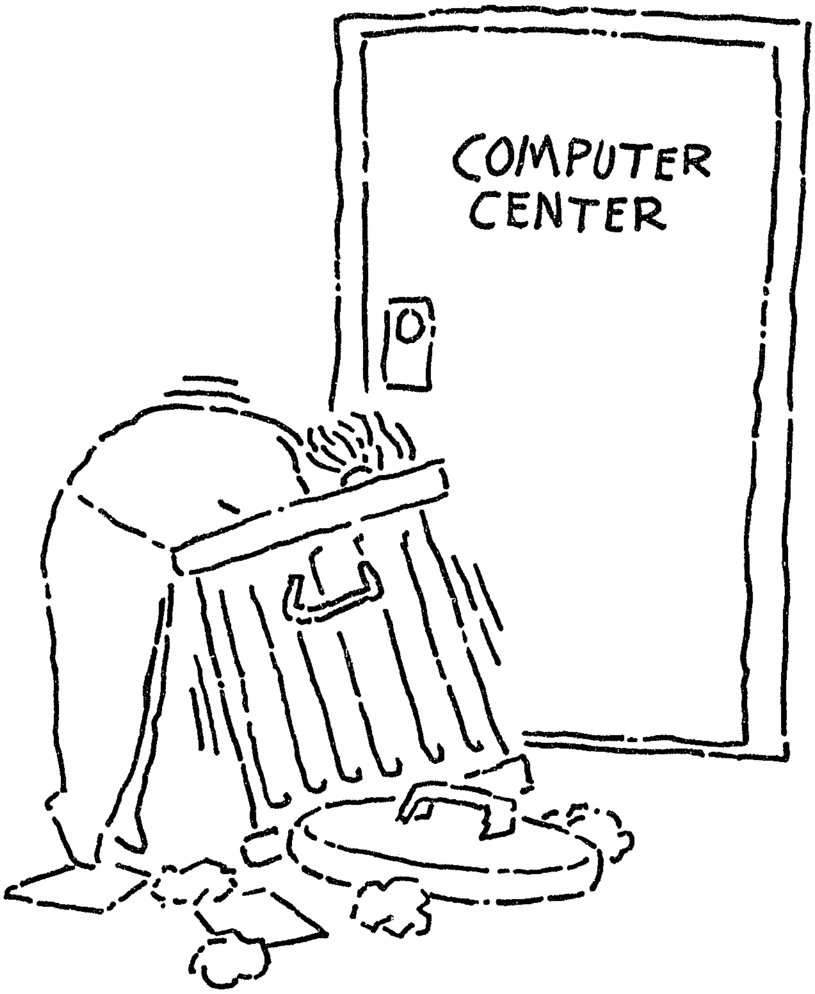
5. Strangers are not questioned about being in the computer area.

6. An inventory of computer equipment or software is nonexistent, incomplete, never updated, or not verified after it is completed. Inventory shortages occur frequently.

7. Printouts, microfiche, or disks containing sensitive information are discarded as normal trash.

8. Locks which secure computer equipment or provide access to computer equipment are never changed.

9. No assessment is made of the computer site, i.e., how vulnerable it is to access by unauthorized persons, to fire or water damage, or to other disasters.



"THIS PRINTOUT IS WORTH $$$S! IT WILL GET ME INTO THE SYSTEM."

PHYSICAL SECURITY CONTROLS

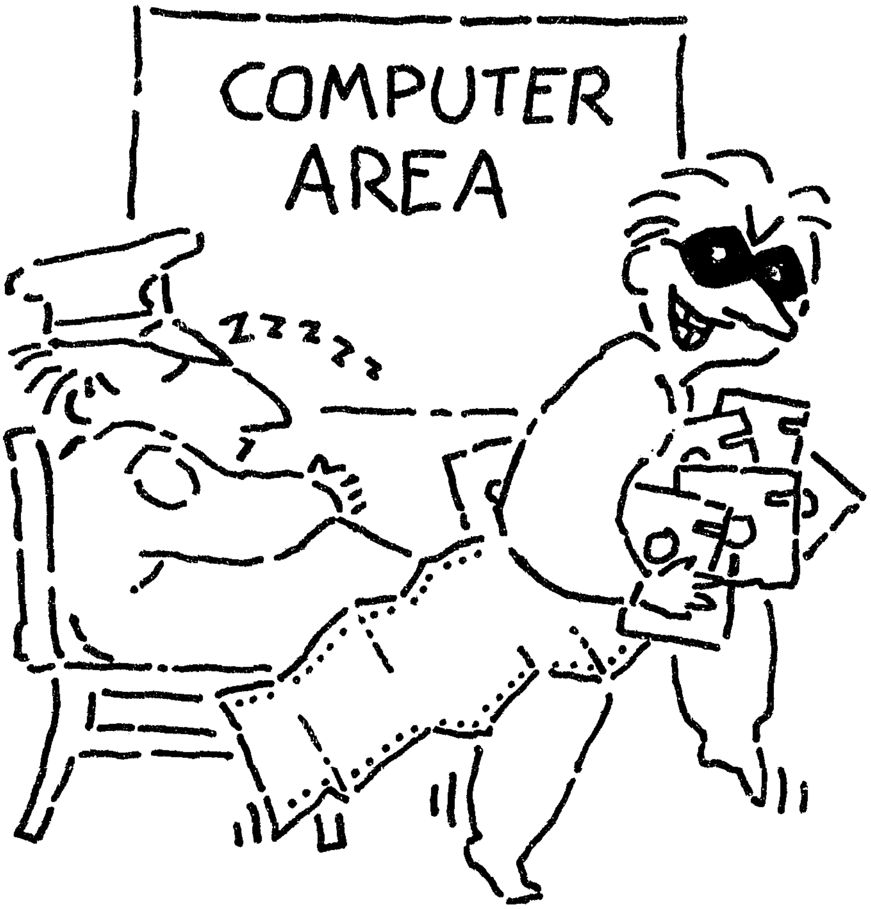
1. ***Prevent intentional damage, unauthorized use, and theft.***

   Small computers can be locked or bolted to work stations and access to them limited by equipment cover locks. Lock offices where they are located. Ensure individuals are responsible and accountable for the small computers they use.

   If the information used by a government program is processed by a major computer facility, check to see how physical access to the facility and to related locations are controlled. Methods such as logs, locks, identifiers (such as badges), and guards may be appropriate.

   The input of sensitive information requires proper handling of source documents. Proper handling means giving the same security considerations to these documents whether they provide input to automated or nonautomated systems. Considerations may involve securing the input area, logging the documents, ensuring that only appropriately cleared persons see these documents, and using burn bags or other approved disposal methods.

   Carefully consider computer location. Is it too accessible to unauthorized persons or susceptible to hazards?



"OUR INFORMATION IS SAFE. SOMEONE IS ALWAYS THERE."

Alert staff:

Be aware of common access-gaining schemes, such as "piggy-backing," where an authorized worker is followed into the computer area by a stranger carrying an armload of computer printouts or by persons without credentials claiming to be maintenance workers.

Know persons with authorized access to the computer area and challenge strangers.

Many people believe that locked and guarded doors provide total physical protection. But electromagnetic emanations from computers can be intercepted and automated information read. Recommended protections (e.g., equipment modification and shielding) must take into account the level of security required by the automated information and the fact that such interception is rare, but may occur.

An inexpensive precautionary measure is making sure that telephone and computer transmission lines are not labeled as to their function and that their location is secured. In a network system, dedicated transmission lines --which perform no other function-- may be required. In an increasing number of situations, dedicating a small computer to a single application may be the most cost-effective protection device.

Each of the four technologies used to transmit automated information can be intercepted: cable (wiretapping), microwave (interception), satellite (satellite receiving antenna), and radio frequency (interception).

Protection technologies which may be called for include encryption of information, dedicated lines, security modems, and the alteration of voice communications by scrambling the signal, converting it to digital form, and using encryption.

2. ***Environmental hazards can wreak havoc with large and small computers alike.***

Take measures to prevent, detect, and minimize the effects of hazards such as fire, water damage, air contaminants, excessive heat, and electricity brownouts.

Protect against **fire damage** with a regularly tested fire alert systems, and fire suppression devices. Protect small computers with covers to prevent damage from sprinkler systems. Do not store combustibles in the area.

Static electricity can erase memory in small computers. Antistatic pads and sprays can help control this. Users can be reminded to discharge static electricity by touching a grounded object.

Power surges can erase memory, alter programs, and destroy microcircuits. An uninterrupted power source allows enough time to shut down a computer without losing data. Prevent momentary power surges from damaging computers by using voltage regulators. In a thunderstorm, unprotected small computers can be turned off and unplugged.

Excessive heat can be controlled by air-conditioning systems and fans, and by ensuring that air can circulate freely. A common problem is stacking peripheral equipment or blocking air vents on terminals or small computers.

Air filters can remove the **airborne contaminants** that harm equipment and disks. Consider banning **smoking** near small computers.

Locate computers away from potential **water hazards**, such as plumbing pipes, areas known to flood, or even sprinkler systems if other fire protection devices are available.

Keep **food, beverages,** and **ashtrays** away from the computer.

Keep equipment in good working order. Monitor and record hardware maintenance. This provides both an audit trail of persons who have had access to the system and a record of contract fulfillment. Remember that maintenance personnel must carry proper identification.

3. ***Protect and secure storage media (source documents, tapes, cartridges, disks, printouts).***

-- Maintain, control, and audit storage media inventories.

-- Educate users to the proper methods for erasing or destroying storage media.

-- Label storage media to reflect the sensitivity level of the information they contain.

-- Destroy storage media in accordance with the agency's security provisions.

-- Ensure that access for storing, transmitting, marking, handling, and destroying storage media is granted only to authorized persons.

-- Publicize procedures and policies to staff.

Consider posting the following reminders --**Disks are Fragile** and **Good Management Practices Provide Protection**-- where everyone can see them.

DISKS ARE FRAGILE

- *Store in protective jackets.*
- *Don't write on jackets.*
- *Protect from bending.*
- *Don't touch disks directly.*
- *Insert carefully into the computer.*
- *Protect from coffee and soda spills.*
- *Maintain acceptable temperatures (50°-125°).*
- *Prevent erasures by keeping disks away from magnetic sources such as radios and telephones.*
- *Store in areas, such as metal cabinets, protected from fire and water damage.*
- *Handle disks in accord with their sensitivity marking.*

Good Management Practices Provide Protection

- *Lock disks and tapes when not in use.*

- *Use a filing system to keep track of disks and tapes.*

- *Don't lend storage media with sensitive information to unauthorized persons.*

- *Return damaged or defective disks with sensitive information only after degaussing or after using a similar procedure.*

- *Dispose of disks with sensitive information by degaussing, shredding, and following agency security procedures.*

- *Dispose of printouts and printer ribbons with sensitive information by following agency security procedures.*

- *Secure printouts of passwords and other access information.*

4. ***Be sure that adequate plans are made for contingencies.*** Remember that the intent of contingency plans is to ensure that users can continue to perform essential functions in the event that information technology support is interrupted. End users of information technology applications, as well as computer installations that process these applications, are required to have contingency plans.

   Contingency plans must be written, tested, and regularly communicated to staff.

   Contingency plans must take into account backup operations, i.e., how information will be processed when the usual computers cannot be used, and the recovery of any information which is lost or destroyed.

   With small computers and word processors especially, the contingency plan should address selected equipment breakdowns, such as a single printer servicing many stations.

   Procedures and equipment should be adequate for handling emergency situations (fires, floods, etc.).

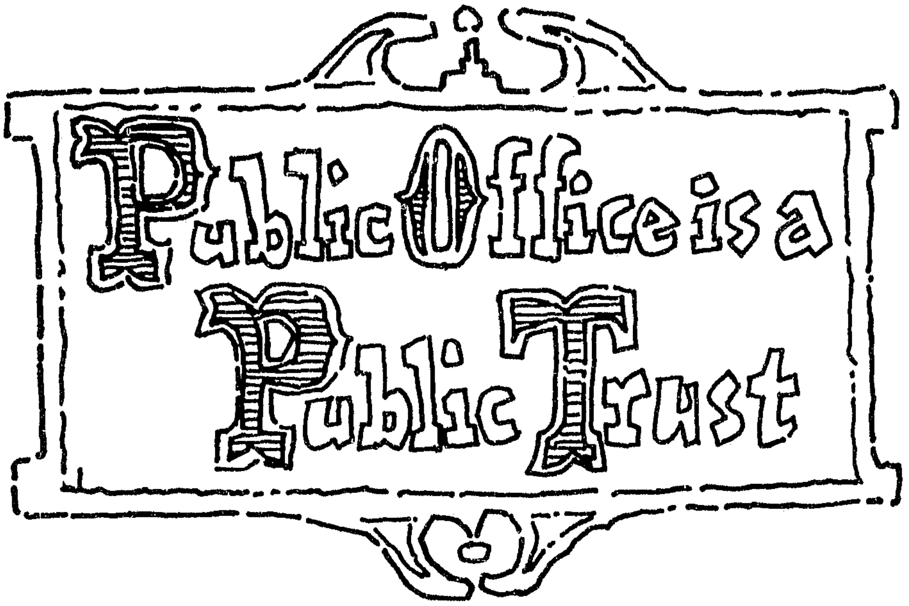
   Store backup materials, including the contingency plan, in a secure and safe location away from the computer site.

   Contingency procedures must be adequate for the security level and criticality of the information.

   Know what to do in case of an emergency and be familiar with the contingency plan.

   Remember that the contingency plan may be operating at a time of great stress and without key personnel. Training of staff is vital.

4. PERSONNEL SECURITY



People are the most serious threat to computers and automated information. The unintentional errors people commit occur more frequently and cause more costly damage than do deliberate acts of sabotage. Unknowingly, people destroy or damage computers, related equipment, and software. Unwittingly, people enter incorrect data into the computer or erroneously alter data.

But people also deliberately damage computers, intentionally steal small computers, and knowingly use automated information for their own gain. It is important to remember that all security measures are vulnerable to users who have legitimate access.

Personnel security as used in this document refers to ensuring that employees know information security requirements and are aware of their responsibilities. Personnel security is also concerned with issues of ethics and personal integrity. The primary mission of personnel security is establishing and maintaining an ethical, technically proficient, informed, and trusted workforce.

CRIMES, ABUSES, AND WASTE

The computer crimes that people commit typically involve entering false data or manipulating data; altering personnel data to get a raise or to delete leave taken; keeping funds returned to the agency; and issuing funds to themselves.

- *A government claims representative embezzled more than $100,000 by creating many fictitious beneficiaries and diverting their payment checks to his personal bank account.*

- *A government employee redirected program funds returned to a government program to a personal bank account.*

Thefts may occur unintentionally. People may copy licensed software to use on their home computer without realizing it is a violation.

Typically, thefts are intentional. Personnel lists have been stolen and sold for commercial use. Computer supplies --disks, printer ribbons, paper-- are attractive items for theft. The most popular theft item is probably the small computer itself. But the largest losses have occurred when people diverted materials and funds to themselves --as in the case of the government employee who created fictitious beneficiaries and directed their benefit payments to his personal bank account.

"THIS NEW OFFICE SPREADSHEET PACKAGE IS PERFECT FOR TRACKING MY HOME EXPENSES."

Common abuses include using the computer for personal business; browsing; preparing personal-use software programs; and creating team rosters, scores, and handicaps.

- *An engineer used his agency's computer to maintain records of his after-hours business and to transmit messages to customers. These records were either deleted or encrypted, which prevented determining the full extent of this abuse.*

Personal ethics play a vital role in protecting computers and information. Ethics provide protection not only against the most serious and costly crimes but against noncriminal abuses that can undermine an organization's integrity.

" LOOK AT THAT SUPERVISOR'S RATING!"

CLUES

The following clues can indicate personnel security vulnerabilities:

1. Information security vulnerabilities are not taken very seriously; it is assumed that these problems will occur elsewhere.

2. Employees have little motivation and low morale. Relationships with management are poor.

3. There is evidence of unusual employee behavior or problems, such as gambling, alcoholism, or drug abuse.

4. Employees seldom take vacations, often choose to be secluded from other employees, and may use their home computers to conduct official work.

5. Employees being terminated are not automatically prevented access to the computer system.

6. Employees are unaware of information security concerns and requirements to protect information.

7. Unauthorized computer products --computer art, games, sports, handicap reports-- appear in the work area.

8. The same technical employees work in all phases of the system -- data entry, data analysis, and data output.

9. Unscheduled programs are run on a recurring basis, particularly during hours of low computer usage.

10. The level of background clearance required by employees has not been considered.

PERSONNEL SECURITY CONTROLS

1. ***Personnel must have a current, working knowledge of information security procedures and practices, and their responsibilities to protect information.***

   Consider offering information security training courses, preparing specialized pamphlets or other training material, and distributing pertinent literature.

   Alert employees to the agency's policy on use of at-home computers for agency work.

   Include both the organization's information security policies and the individual's responsibilities in information security training.

   Publicize procedures to report security violations and irregularities. Inform staff that unauthorized duplication and use of licensed software violate the law.

   Conduct periodic security briefings for all personnel dealing with sensitive information.

   Indoctrinate new employees to their ethical responsibilities.

   Ensure program managers are aware that they are responsible and accountable for the products of information systems that support their programs.

   Ensure that personnel know who their agency security officials are and how to communicate with them.

2. ***Personnel policies must address information security requirements and concerns.***

Personnel security policies must require screening of all individuals (including contractors) participating in the design, operation, and maintenance of computer systems or having access to the data in these systems, commensurate with the sensitivity of information being handled.

Position descriptions of technical staff must provide for adequate separation of duties; for example, systems programming should be separate from data base administration, and data input should be distinct from data auditing functions.

Regular reassignment of data processing duties and required taking of leave are often recommended as further controls.

Personnel policies should include checkout procedures that deny access to the computer system to departing employees. Standard debriefing procedures should be followed.

3. ***Through its administrative personnel-related practices, management must encourage and, where appropriate (as with small computers), take the lead in promoting information security.***

Consider instituting personnel practices designed to promote information security:

-- *After annual security training, require personnel to sign a statement that they understand their information security responsibilities.*

-- *Assign responsibility to small computer users for their equipment and their computer transactions on it.*

-- *Develop a remote terminal user's agreement that delineates the user's responsibilities.*

-- *Encourage personnel to be involved in risk analyses and contingency planning. Especially with microprocessors, promote broad personnel participation in identifying the risks involved should the information be destroyed or accessed by unauthorized individuals.*

-- *Develop a software integrity policy that cautions against "softlifting" (illegal copying of licensed software for personal use) and "software piracy" (software copying) and that describes the circumstances in which vendor-developed software can be reproduced and distributed.*

-- *Encourage the establishment of an information security steering committee within the organization to highlight security issues and to identify solutions to security problems.*

Demonstrate to staff that information security is a serious responsibility by keeping informed of current policies, providing training to staff, and paying attention to and taking action on identified vulnerabilities.

Be alert to unusual employee behavior --low morale, refusal to take vacations, or personal problems that may indicate vulnerabilities which could lead to information security problems.

Be aware of computer output and whether unauthorized items (e.g., mailing labels and printouts) are being produced.

Stress to staff the importance of personal integrity and ethics, and encourage the reporting of suspected security violations.

5. A PLAN OF ACTION

While the preceding chapters explored the various types of security, this chapter is a planning primer that provides a basic framework in which to develop the necessary security measures for your situation.

1. ***Establish an information security policy.***

   -- Identify the level of information in the system and the types of information requiring protection.

   -- Determine the required user clearance level and identify who can access which information.

   -- Specify the control measures that apply.

   -- Assign appropriate responsibility to users.

   -- Identify the individual who is responsible for information security.

2. ***Develop an inventory of applications.***

   Include these factors: system identification and location; responsible user; other users; general categories of sensitive information handled; specific, identifiable applications; general description of access controls; and other security measures currently in place.

3. ***Conduct a risk analysis.***

   A risk analysis is a periodic, formal assessment of threats and risks to information and equipment. It should be conducted to ensure that appropriate, cost-effective safeguards are in place.

   The objective of a risk analysis is to provide a measure of the relative vulnerabilities and threats to the system so that security resources can be effectively distributed to minimize potential loss.

   Risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large-scale computer system.

   Three elements should be reviewed: value of assets being protected; nature and likelihood of threats facing those assets; and the cost-effective use of existing or potential safeguards.

   In thinking about threats and system vulnerabilities, a review of the *Clues* previously listed under *Information Security, Physical Security,* and *Personnel Security* may be helpful.

The following list can be a starting point to identify the threats to your system and the issues your security program should address.

1. *Fire*
2. *Flood*
3. *Computer equipment failure*
4. *Stolen software*
5. *Theft of information*
6. *Unauthorized manipulation of input information*
7. *Unauthorized access to information*
8. *Loss of small computers*
9. *Explosion caused by a bomb*
10. *Loss of heat*
11. *Loss of air conditioning*
12. *Power interruption*
13. *Sabotage of equipment*
14. *Sabotage of information*
15. *Loss of back-up files*
16. *Loss of program documentation*
17. *Tornado or hurricane*
18. *Unauthorized distribution of information*
19. *Unauthorized changes to written procedures*
20. *Damage to floppy disks*
21. *On-line interception*
22. *Unauthorized program changes*
23. *Explosion caused by gas*
24. *Loss of key personnel*
25. *Theft of sensitive or classified information*
26. *Inadequate equipment maintenance*
27. *Addition of fraudulent data records*
28. *Mismanagement of data input forms*
29. *Open media storage items (e.g., disks, tapes, printouts) on open shelves*
30. *Lack of audit trails on information access and use*
31. *Security clearances not required*
32. *Terminating employees allowed computer access*
33. *Loss of critical supplies*
34. *Contingency plan stored on-site*
35. *No employee computer security training*
36. *No back-up computer facility*
37. *Employees unaware of contingency plan provisions*
38. *Printouts discarded in regular trash*
39. *Temporary loss of many employees (e.g., due to an epidemic)*
40. *Small computers left on all night*

4. ***Select control measures.***

   Where risks are unacceptable, implement additional controls.

5. ***Audit and monitor the results.***

   Make sure the controls are in place and still appropriate.

6. ***Plan for contingencies.***

   Include significant applications. Prepare a documented plan. Test it and communicate it to appropriate personnel. Determine emergency responses. Ensure backup for equipment, information, programs, and documentation. Store a copy of the contingency plan in the backup location.

7. ***Emphasize the importance of information security.***

   Educate computer users. Correct identified security violations. Add security reviews to audits of the computer system. Demonstrate a commitment to information security at the highest organizational levels. Encourage security awareness and support.

6. SOURCES FOR ASSISTANCE

- The problems of information security can often be addressed through an agency's own resources, such as a data security group, ADP auditors, and the agency individual charged with information security responsibilities. Many agencies have published documents on information security.

- Other sources for assistance include professional organizations, trade organizations, and professional literature.

- The **Department of Commerce, National Bureau of Standards, Institute for Computer Services and Technology** provides guidance on a broad range of information security issues. They issue Federal Information Processing Standards (FIPS) and guidelines on information security topics, prepare special research publications, and undertake cooperative efforts with government agencies.

- The **Office of Management and Budget** issued OMB Circular A-130, *Management of Federal Information Resources*, December 12, 1985, that establishes policy for the management of Federal information resources.

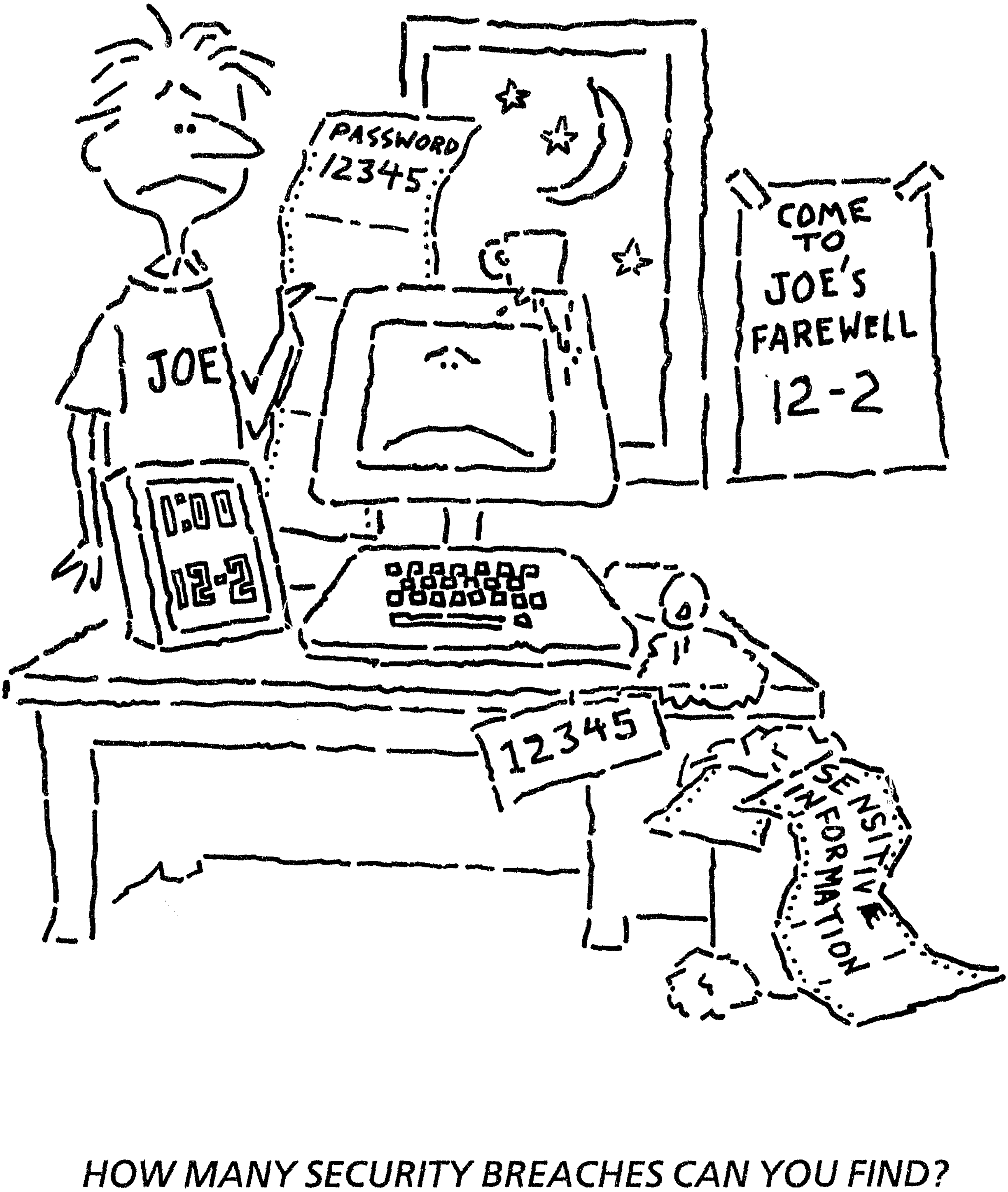
- The **Office of Management and Budget**, in January I985, published an annotated bibliography of laws, policies, regulations, and associated documents entitled *Automatic Data Processing and Telecommunications in the Federal Government.*

- The **Department of Defense** is responsible for the **National Computer Security Center** whose mission is to encourage the widespread availability and use of trusted computer systems throughout the government. It provides technical support in computer security, develops technical criteria, evaluates commercial systems, conducts and sponsors research in computer and network security technology, develops and provides access to verification and analysis tools, conducts training, and disseminates computer security information.

- The **Department of Defense** is responsible for the **DoD Computer Institute (DoDCI), National Defense University,** whose mission, in part, is to provide information resource protection and security training to DoD civilian and military service personnel. DoDCI offers courses in information security that are available to personnel from other government agencies on an availability basis. DoDCI also provides information security management advisory services.

- The **Department of Justice** publishes documents on computer crime and computer security that include references to the laws and regulations requiring and implementing information security.

THESE PREMISES ARE PROTECTED BY A FALSE SENSE OF SECURITY



HOW MANY SECURITY BREACHES CAN YOU FIND?

MICROCOMPUTERS REQUIRE SPECIAL PROTECTION

- *Guard microcomputers from power surges.*
- *Use antistatic pads, mats, or carpets.*
- *Prevent theft with anchor pads or locking devices.*
- *Backup information and store copies in a safe place.*
- *Consider limiting the microcomputer to a single user. It may be the most inexpensive way to secure information.*
- *Determine which information needs to be secured, and implement security policies.*
- *Ensure that users are aware of their ethical responsibilities, as well as information security precautions.*

12 COMMON DON'TS

- *Don't share your password with anyone.*
- *Don't tape your password to desks, walls, or terminals --commit yours to memory.*
- *Don't smoke or have food or beverages near the computer.*
- *Don't leave the computer on and unattended.*
- *Don't use the computer for personal business.*
- *Don't have automated information in only one place --back it up.*
- *Don't forget to secure printouts containing sensitive information.*
- *Don't copy licensed software packages and don't use copies someone else has made.*
- *Don't treat all automated information the same. Know what needs to be secured and do what needs to be done.*
- *Don't assume that your automated information and equipment are always protected. Plan for contingencies.*
- *Don't assume information security just happens. Do your part.*
- *Don't go it alone. Seek help when you need it.*

REPORT FRAUD, WASTE OR MISMANAGEMENT

- Information is Confidential
- Callers can Remain Anonymous

Offices of Inspector General and Hotline Numbers

Department of Agriculture	(800) 424-9121
Agency for International Development	(FTS) 235-3528
Department of Commerce	(800) 424-5197 (202) 377-2495
Department of Defense	(800) 424-9098 (202) 693-5080 (AV) 223-5080
Department of Education	(800) 646-8005 (202) 755-2770
Department of Energy	(FTS) 252-4073 (202) 252-4073
Environmental Protection Agency	(800) 424-4000 (202) 382-4977
General Services Administration	(800) 424-5210 (FTS) 566-1780 (202) 566-1780
Department of Health and Human Services	(800) 368-5779 (800) 638-3986 (Maryland only) (301) 597-0724
Department of Housing and Urban Development	(FTS) 472-4200 (202) 472-4200
Department of the Interior	(800) 424-5081 (202) 343-2424
Department of Justice	(202) 633-3365
Department of Labor	(800) 424-5409 (202) 357-0227
National Aeronautics and Space Administration	(800) 424-9183 (202) 755-3402
Office of Personnel Management	(FTS) 632-4423 (202) 632-4423
Small Business Administration	(FTS) 653-7557 (202) 653-7557
Department of State	(202) 632-3220
Department of Transportation	(800) 424-9071 (202) 755-1855
Department of the Treasury	(800) 826-8407 (202) 566-7901
Veterans Administration	(800) 368-5899 (FTS) 389-5394 (202) 389-5394
General Accounting Office	(800) 424-5454 (202) 633-6987
Merit Systems Protection Board	(800) 872-9855

Or call the Office of Inspector General at your agency.

You are the first line
of defense in protecting government
information resources.