# *Chapter* 8

# *Management Issues*

**8.1 Introduction**
**8.2 Policy Issues**
8.2.1 Acquisition Guidelines
8.2.2 EUIS Standards
**8.3 Physical Security of Hardware and Software**
8.3.1 Avoiding Damage
8.3.2 Protecting against Viruses
8.3.2.1 Trojan Horses and Worms
8.3.2.2 Procedures to Prevent Virus Damage
8.3.3 Protecting Software (Backup)
8.3.3.1 Backup Hardware and Software
8.3.3.2 Internet-Based Backup Options
8.3.3.3 Value-Added Resellers (VARs)
8.3.4 Developing Naming Conventions
8.3.5 Managing Networks
**8.4 Data Security and Confidentiality**
**8.5 Information Accuracy and Reliability (Integrity)**
8.5.1 Preparing Documentation
8.5.2 Ensuring the Accuracy of Computer Programs
8.5.3 Developing Guidelines for Information Systems Security
**8.6 Legal Issues**
8.6.1 Defining Corporate Versus Personal Data or Programs
8.6.2 Preventing Unauthorized Copying of Software
8.6.3 Developing Hardware and Software Contracts
8.6.4 Preventing Unauthorized Access to Programs and Data
**8.7 Resources, Products, and Services**
8.7.1 Auditing Procedures for EUIS

8.7.2 Hardware and Software Security Devices
8.7.2.1 Hardware Security Systems
8.7.2.2 Data Encryption
**8.8 Summary**

# Learning Objectives

*Upon completing this chapter, you should be able to:*

- Identify critical factors for managing and supporting end-user information systems.
- Discuss major policy issues for the management of desktop hardware and software.
- Describe steps managers and users can take to provide adequate security for personal computers and data.
- Explain why backup of computer data is important and how data can be protected.
- Plan strategies for protecting computers from viruses.
- Identify legal issues related to software and data.
- Discuss ways managers can ensure the accuracy and reliability of user-developed systems.
- Explain the role of auditing in protecting computer resources.

# 8.1 INTRODUCTION

Developing and managing end-user information systems (EUIS) have become high priorities for managers. Issues that were previously of concern only to managers of technical data processing departments have become general concerns in the workplace.

In today's workplace, procedures that monitored and controlled information processing in the paper-based office are no longer adequate. Likewise, control procedures used in technical data processing centers may not be practical in a decentralized office. New techniques for controlling and monitoring information processing are being developed and implemented. The solutions will vary from one situation to another, but guidelines can help.

Managers and end users alike must know about the opportunities, risks, and issues related to the effective, efficient, and safe use of desktop computers. Otherwise, they may not recognize problems until after disaster strikes. When new technologies are introduced, it takes time to understand the wide range of issues that effective use entails. These issues, related to hardware and software maintenance and management, are discussed in this chapter, and fall into five major areas:

1. *Policy issues.* What policies should managers establish, and how should these policies be communicated? How do managers integrate information systems policies into an organization's overall policy? What auditing procedures should be established to ensure compliance with corporate policies?
2. *Physical security of hardware and software.* How do managers protect computers and disks from theft and physical damage?

3. *Data security and confidentiality*. What safeguards should be taken to protect data that are stored on disks and hard disks? How can organizations protect information from unauthorized access or use?
4. *Accuracy and reliability of information.* How can managers be sure that data developed with spreadsheets, databases, and other user programs are accurate and reliable? What kind of documentation is needed, and who develops it and keeps it up to date?
5. *Legal issues.* What risks and liabilities are an organization and its managers exposed to in connection with EUIS? For example, who is liable when employees make unauthorized copies of software?

This chapter also discusses a variety of resources, products, and services that can be used in dealing with these issues. Discussion points include auditing procedures, data-protection and encryption products, hardware security products, and others. The most viable techniques, however, are practical guidelines and good management practices.

## 8.2 POLICY ISSUES

Policies established by top management are a first step toward showing employees that computer-related risks are an important corporate concern. Senior management is often too busy running the business to address these risks until a serious problem arises. Even organizations that have established security and disaster-recovery plans for their centralized computing operations may overlook the risks and issues of managing desktop computers.

Policies for EUIS vary among organizations according to their corporate cultures. Many managers have sign off authority for purchases of up to perhaps $2,000, which is enough for a complete desktop or notebook computer system. Moreover, few off-the-shelf applications packages cost more than $500. Therefore, managers and analysts generally want to stimulate creative use of EUIS, and at the same time ensure compatibility, security, and cost effectiveness. Specific goals include:

- Avoiding incompatible hardware ~td software
- Minimizing duplication of effort
- Avoiding unnecessary spending
- Coordinating EUIS with corporate information systems activities
- Coordinating EUIS with corporate strategy
- Providing adequate protection for corporate resources
- Simplifying technical support requirements[1]

The manager who wants to address these goals needs a corporate policy. The key steps for establishing a policy for EUIS include the following:

1. *Develop acquisition guidelines.* Centralize buying as much as possible; large transactions can save money and secure better maintenance terms.
2. *Take inventory.* Sudden costs must be known and evaluated before any *defacto* standards are set; the installed base will affect policy decisions and future acquisitions.

3. *Develop hardware and software standards.* Standards will facilitate the sharing of resources and the porting of development work (transferring an application developed on one computer to another).
4. *Establish return-on-investment (ROl) standards and schedules.* Some enterprises require this type of cost/benefit analysis, and return-on-investment analysis (sometimes referred to as *payback)* will assist decision makers in evaluating and justifying hardware and software investments (see chapter 9).
5. *Establish maintenance, housekeeping, and security standards and schedules.* Computers and data must be maintained, and standards must be developed that describe proper hardware and software care. Care can include how to secure the machine physically, as well as data backup schedules.
6. *Develop legal guidelines for hardware and software use.* Large sums of money may be at risk if legal issues are ignored. Novice users may be unaware of copyright restrictions on some software, and corporations have been sued for violations of these laws. These issues have become even more complex with Internet use.
7. *Establish periodic policy reviews.* Technology changes so quickly that a solution defined today may not be cost effective tomorrow.

Management can be proactive in *avoiding* problems. Preventive measures can include a written policy statement that identifies all computer and information resources as significant assets. The intent of an information policy should be to encourage care and concern by making employees accountable for unauthorized acts involving computer and information resources. The policy statement should clearly state the company's position on unauthorized copying of software and should be distributed to all employees who have access to information resources. Figure 8-1 presents a typical policy statement on the use of corporate information resources.

Organizations can help establish personal accountability by having employees sign *confidentiality covenants.* By signing such a document, employees agree not to disclose any proprietary information or to misuse corporate computer resources to which they have access. These covenants acknowledge that failure to comply with company information policies will result in disciplinary actions.

### 8.2.1 Acquisition Guidelines

Managers try to balance needs for encouraging innovative application of technology against wasteful spending, duplication of effort, or incompatible equipment. Many managers have sufficient budget control to purchase hardware and software and may be tempted to circumvent corporate procurement procedures. If the equipment meets the department's needs and the purchase can be cost justified, why not?

One reason "why not" is that such ad hoc equipment purchases may be incompatible with other corporate hardware, thereby limiting future options. Regardless of whether an organization maintains strict or flexible controls, managers should be aware of the issues relating to hardware and software acquisition. Vendors often portray personal computing to end users as effortless and immensely beneficial; they understate the risks, pitfalls, and problems. Shortcomings of products are not usually evident until the novice gains experience. Users often learn the

**Computer Software Resources**

Growing numbers of company employees and associates use computer software resources in connection with their jobs. Such resources are crucial company assets that make our tasks easier and enable us to perform our jobs with greater accuracy and efficiency Many employees are not aware of the legal duties that accompany the use of computer software, however. Often, people do not realize that unauthorized copying or disclosure of software has a costly impact.

When software has been developed here at the company, unauthorized taking or copying of that software diminishes the value of a company asset. When software is used under license from an outside supply firm, improper duplication or disclosure deprives that firm of revenue, ultimately raising costs for the customer community. More importantly, whether software resources are developed in-house or licensed from a vendor, unauthorized copying or disclosure is illegal.

Consequently, the Company has issued the following Policy Statement on Computer Software Resources. It is the responsibility of every employee and associate who uses or has access to software resources to adhere strictly to this policy.

**Policy Statement on Computer Software Resources**

The computer software resources are assets of the company that are vital to our operation. Such resources may be exclusive company property or may be proprietary products used under contractual license from program supply firms. Either way, software is a valuable commodity that the owner is entitled to protect. Consequently, whether using software owned exclusively by the company or software licensed from program supply firms, it is the responsibility of every employee and associate to prevent destruction, misuse, or misappropriation of such resources.

This policy has two components. First, the unauthorized copying or reproduction of any software program, program documentation, or related material is strictly prohibited. This policy also prohibits using any program, program documentation, or related material, or any copy thereof, for personal purposes or making such materials available to anyone outside the company.

Reproducing computer software without authorization may constitute an improper taking of a company asset or may violate the terms of a license agreement into which the company has entered. The money paid for proprietary products generally represents a license fee for the use of one copy. It does not represent an authorization to make unlimited copies. More importantly, unauthorized duplication of software violates U.S. Copyright Law. Civil damages can be as much as $50,000, and copyright infringement can qualify as a federal misdemeanor punishable by up to $10,000 in fines or up to one year's imprisonment. Consequently, this policy must be followed strictly. Second, employees and associates must make every effort to maintain and protect the integrity of confidential data contained in software programs, program documentation, and related materials. Employees and associates must not disclose these data and must take reasonable precautions to see that they are not left in the open or haphazardly discarded.

Computer software resources may constitute confidential material or trade secrets entitled to legal protection. Software 1icense agreements often require the company to treat software resources as confidential. The unauthorized disclosure of software materials could thus create legal liability Therefore, this policy also must be strictly regarded.

Violation of the above policy may result in disciplinary action, including termination, where appropriate. Employees or associates with questions concerning the policy should contact the head of the Computer Security and Contract Administration Department.

*Source:* Courtesy of Massachusetts Mutual Life Insurance Company.

**Figure 8-1** A typical policy statement on the use of corporate information resources

limitations of hardware or software too late, when they discover that if they had only bought another product, it would be able to do what they wanted.

Also, unmonitored acquisition procedures can mean higher costs because organizations usually can negotiate volume discount purchase agreements. Managers should recognize the many trade-offs in computer products in terms of price, performance, and features. Selecting appropriate hardware and software can be time consuming and fraught with problems. The immense diversity of products means that novices may select incompatible hardware or software. Incompatibility can lead to costly mistakes that preclude the transfer of data between systems or greatly increase the complexity of supporting, aiding, or training users. In-house technical resources may not support nonstandard hardware and unique software, thus forcing the department to go outside for more expensive services.

Another reason that technology should not be purchased ad hoc is that options maybe overlooked that limit or increase the equipment's use for applications other than the one for which it originally was justified. Managers can seek the advice of knowledgeable EUIS analysts when considering the purchase of computer devices for their departments. Experienced analysts, whether in-house or outside consultants, can save managers valuable time, money, and frustration. Moreover, they often can cite considerations or opportunities not apparent to managers who have limited experience with the technology.

### 8.2.2 EUIS Standards

Standards, though often looked upon as restrictive, offer benefits for both IS professionals and end users. Most large enterprises have standards that cover many aspects of their operations, including EUIS. Generally, standards are recorded in formal standards and procedures manuals, but even informal, handwritten notes about company procedures could be considered standards.

Standards provide consistency, save resources, reduce errors and problems, and, as already pointed out, provide greater compatibility among EUIS hardware and software. Most importantly, standards significantly affect productivity Software user interface standards, for example, provide greater consistency in the way applications work, which in turn makes them easier to learn and use because they are more predictable and users can benefit from previous experience with other software.

To the user, this means that standards are an important requirement for building systems that are well thought out. Standards establish a performance baseline. End users, managers, and EUIS professionals should be familiar with their firm's standards and ensure that they are followed.

## 8.3 PHYSICAL SECURITY OF HARDWARE AND SOFTWARE

Physical security involves avoiding potential threats and deterring anyone withintentions to steal or tamper with equipment or information. Managers are responsible for protecting valuable equipment and files. What should I do when two computers turn up missing on Monday morning? How did the spreadsheet software and manual disappear?

Where is the department notebook computer that has our competitive analysis worksheets?

A list of all computer hardware and software and their serial numbers should be kept in a safe location, and physical inventories should be made regularly. A signed authorization should be required for all hardware and software that is taken into and out of the office building. Devices should be insured adequately.

## 8.3.1 Avoiding Damage

Appropriate work space should be set aside to safeguard equipment. Analysts should assess possible environmental hazards such as heat from direct sunlight or rain from windows that might be left open. Proper electrical outlets and wiring should be provided. Cables and wiring should not be exposed where employees may trip over them or accidentally snag them, bringing everything crashing to the floor. Spilled liquids are a major cause of damage, and beverages and other liquids should be kept away from hardware and software. Liquids can leak into electrical circuits or damage disks. Smoking should not be allowed near computers and stored disks because smoke can deposit on sensitive drive heads, shortening their useful life and increasing the danger of losing data.

Routine computer inventories and maintenance could be assigned to one individual whose job it is to keep track of all desktop computers in the area, or this task could be assigned to various individuals for different types of peripherals. In addition, computer hardware and software need to be protected from static electricity during dry, winter months. Humidifiers, carpets that resist static buildup, and antistatic sprays and mats are resources that managers can consider.

## 8.3.2 Protecting against Viruses

While computer bugs are software glitches that are accidentally in the program code and cause computer malfunctions, viruses are malicious attempts to annoy a user or cause irreparable harm to data, programs, or operating systems. Both *bug* and *virus* are terms from the biological sciences. In 1945, Grace Hopper coined the term *bug* when she reported finding a moth in an early computer. Viruses, sometimes referred to as malware, "can't be killed by Lysol" and are capable of causing computer users and information systems managers much dismay when they attack their systems.[2]

This discussion of viruses (not bugs!) classifies recent strains of viruses as either Trojan horses or Worms, and includes a discussion of virus inoculation (antivirus) software and suggestions for how to keep desktop systems from getting virus infections.

### *8.3.2.1 Trojan Horses and Worms*

Initially, *viruses* infected files or disks on a single computer. Increasingly, their more powerful (destructive) offshoots, Trojan horses and worms, are spreading havoc among computers in a corporate network or on the Internet.

*Trojan horses* (sometimes referred to as Trojans) are true to their Greek reference. Greek soldiers hid inside a wooden horse and then launched a surprise attack on the city of Troy. In the computer sense, Trojans are viruses masquerading as something else,

such as an attachment from a friend, an attachment that offers you a free product, or simply an e-mail message that says "urgent!" Once opened, Trojan horses can wipe out the entire contents of documents, spreadsheets, and databases that are created by certain programs. At the time of this writing, Microsoft programs, particularly Outlook, Word, and Excel, are the most frequent targets.[3]
Other targets have included service providers such as AOL, where a Trojan horse created havoc in stealing users' passwords.
Worms, on the other hand, don't attach themselves to other programs. Instead, they duplicate themselves continually until your hard disk or your entire network's disk space is filled. Worms can paralyze computer operations.
Although antivirus software is useful as a cure, it isn't useful until someone has detected the virus and a cure is established. It is estimated that more than 10,000 virus types exist, and the number is increasing daily.[4] Therefore, antivirus software is a must for any user who shares data or programs with others. The current leading antivirus software providers are Symantec, producer of Norton Anti-Virus *(www.syinantec.com),* and McAfee VirusScan *(www.mcafee.com)* software. Both companies provide (for a fee) downloadable updates, and their Web sites serve as central command sites for information and cures for recently uncovered viruses, Trojans, and worms. Once installed, these antivirus programs can be set up to be updated automatically and scan e-mail attachments and other documents upon arrival at the user's system.

#### *8.3.2.2 Procedures to Prevent Virus Damage*

It is a good idea to have procedures in place to minimize the risk of damage and productivity loss from viruses. Following a few basic rules and procedures will go a long way in avoiding problems:

- Install antivirus software and keep it updated.
- Avoid using freeware or shareware acquired from friends or bulletin boards on business computers.
- If you receive a lot of e-mail, put a number of blank entries in your e-mail address folder. Some e-mail-related viruses read your address book and send messages to those at the top of your list.
- Scan all disks or CDs that are new, unfamiliar, or brought in from outside the firm *prior* to using them.
- Back up all computer files on a regular basis.

### 8.3.3 Protecting Software (Backup)

"There are only two kinds of computer users: Those who have lost data, and those who will."

—Bob Levitus, *The Houston Chronicle*

What happens when your computer gets hit by a virus? What if you accidentally hit the delete key and wipe out your contact list? What if you make an error in entering your spreadsheet formulas? What happens when the new network administrator mistakenly deletes the directory containing all the department's form letters? Data stored on the computer must be protected from modification, destruction, and disclosure. Data are also

vulnerable to accidental loss and erasure. To safeguard data, backup systems are required.

*Backup* refers to duplicate copies of electronically stored data. In computer centers, data are routinely backed up, and two or more copies of all data files are maintained in different locations. Copies of critical information often are stored in specially constructed vaults at a site separate from the computer center. These procedures serve much the same purpose as records management departments.

EUIS have greatly increased the volumes of data that are stored electronically within departments instead of in carefully managed data or records centers. Today, managers must take responsibility for establishing procedures to protect data files created and stored in their departments. Common sense is that copies should be maintained of all work stored electronically. Following are some useful guidelines:

1. Clearly assign accountability for backup. If a network is used, a system administrator can be assigned to perform backup each night. Individuals should be held accountable for backing up their own personal files. Responsibility for the backup of all departmental files, however, should be specifically assigned.
2. Store backup disks and tapes in a secured location, not at random in individual desks. Consider off-site storage.
3. Clearly label and date backup disks and tapes.
4. Maintain at least two backup copies of critical data. If a problem occurs during the backup process and both the original and the backup are damaged, a second backup copy would still be available. When multiple backup copies are maintained, they usually are updated on alternate days. For example, on Day 1, Backup Copy A is updated; on Day 2, Backup Copy B is updated; on Day 3, backup is made to Copy A again; on Day 4, to Copy B; and so on.

Because electronic storage is reliable, it is easy to become complacent about electronically stored data. In the absence of strict procedures, people tend to become careless about maintaining up-to-date copies of their work. When problems occur, however, as they invariably do, reconstructing lost information can be time consuming and expensive. Figure 8-2 presents strategies for safeguarding data through better backup procedures.

Fortunately, today a variety of tools are available to help make regular backup procedures easier and faster. In addition, other media such as magnetic tape can be used to ensure continual backup. At the simplest end, inexpensive software and zip drives can help you back up files. For Windows programs, for example, there's Microsoft Backup and Iomega software and hardware. However, for complex or critical file backup, special purpose hardware and software often are required. In other cases, a small organization may want to store its data through the Internet or even completely outsource its information systems operations through a value-added reseller (VAR). Here's a discussion of each option.

#### *8.3.3.1 Backup Hardware and Software*

In the hardware arena, the most popular choice for backup is zip drives or tape backup systems. A zip or internal tape drive may be adequate for many users.

managers must take responsibility for establishing procedures to protect data files created and stored in their departments. Common sense is that copies should be maintained of all work stored electronically. Following are some useful guidelines:

1. All new computers should include a tape or zip drive for backup purposes
2. Policies should indicate clearly what types of data and programs need (a) no backup, (b) secure on-site backup; or (c) on-site and off-site backup,
3. Every user should attend comprehensive training programs on backup procedures
4. The Data Security Office (or an assigned group under another name) should be readily available to consult on questions about whether and how to make and store backup for desktop applications desktop applications
5. Supervisors should be required to perform periodic audits on backup activities. The data security officer should perform regular checks on the supervisors' audit records

**Figure 8-2** Tactics for achieving better backup

| | | |
|---|---|---|
| OnStream, Inc. | ADR | onstream.com |
| NovaStor | NovaBackup | novastor.com |
| Veritas Software | Backup Exec | veritas.com |
| Highware | Personal Backup | highware.com |
| Dantz | Retrospect | dantz.com |

**Figure 8-3** Desktop tape backup systems vendors, sample product lines, and URLs

However, when computer users want to backup their 12-, 18-, or 36-gigabyte hard drive or when files are scattered, special hardware and software are needed.

Figure 8-3 lists backup software that may fit the needs of desktop computer users. Even the inexpensive, low-end systems typically offer features such as automatic backup. OnStream, Inc., for example, offers a tape that holds the space of about 10,000 floppy disks for less than $40. On the other hand, feature-rich, high-speed systems can cost more than $1,000.[5] Dantz's Retrospect, instead of providing full backup, takes snapshots of a disk drive as needed and can restore in a single pass.[6] Veritas Software even offers online training to its customers. Keep in mind that tape capacity is growing; at the time of this writing, storage capacities of backup systems range from 30 to 70 gigabytes. "Tape drives are like kids' sneakers—if you don't wear them out, you outgrow them. And constantly replacing tape drives quickly becomes prohibitively expensive."[7] Fortunately, most of these systems are designed to grow with the user.

#### *8.3.3.2 Internet-Based Backup Options*

Another data backup/storage option is through the Internet. For a monthly fee, organizations such as those listed in Figure 8-4 will encrypt your data, give you data transfer software, and keep your files off site in a secure location. Speed of transfer can be an issue, however, to anyone using POTS (plain old telephone service) lines to transfer data; high-speed lines are recommended.

#### *8.3.3.3 Value-Added Resellers (VAR)*

Virtual office services were described in chapter 4 as Level 1 groupware, Internet-based services that were either free when bundled with other software products or leased for a monthly fee. VARs such as CenterBeam have taken this concept one giant step further, offering virtually (no pun intended) all needed hardware, software, Internet access, backup, security, support and service components in a single package for a monthly fee.[8] In essence, this means that an organization can outsource its entire information systems department, leaving complex issues of backup and


**Figure 8-4** Internet backup data suppliers

security to other professionals. Such relatively inexpensive services are useful for organizations that want to avoid the costs associated with software and hardware and supporting IT personnel.

### 8.3.4 Developing Naming Conventions

Users and managers may need to work together to establish standards for naming data files and storing shared data. When left to the whim of individual users, it may be difficult or impossible for someone else to locate files. At the very least, hours of valuable time can be wasted finding the correct files or directories. The importance of a systematic approach to naming and storing information becomes even more apparent when departmental networks are used. All employees who create, research, and request information must talk the same language, or considerable time and effort can be wasted locating information.

### 8.3.5 Managing Networks

Networks introduce even greater risks and challenges for business managers. In one sense, protecting a network from equipment failure, power outages, natural disasters, or other problems is no different from protecting the mainframe. Even a straightforward approach of backing up the network's servers once a week or once a month, with incremental backups scheduled on a daily basis, can be time consuming and costly. A backup unit can cost as much or more than the file server itself.

As networks expand from small workgroups run from single servers to Intranets, Extranets, and Internet linkages, adequate protection becomes more complex. With so much more data, enough downtime may not be available in a day to copy an entire disk drive image for each server on the network to tape each night. Network administrators will need better hardware and backup software technologies to help them cope with large networks.

At the same time that network management issues are being addressed, analysts must address a number of other issues, such as the following: Should responsibility for backup be handled by a centralized IS resource, or should it be the responsibility of each department? Should there be only one backup service provider on the network? If

multiple providers are used, on what will the division of labor be based? Should selected enclaves of users be allowed to back up their own servers? How about their own workstations? Should workstation backup be included in the network-based backup service? If there are multiple backup providers, should they all be required to use the same backup hardware and software? How much of the data needs to be backed up and where is it located? Where should backups be stored? Is off-site storage of backup data necessary? What type of hardware and software should be used? All too often, these issues and others are not addressed until after a disaster occurs. The EUIS analyst may find it a challenge to persuade management of the importance of well-managed backup and to enforce disciplined procedures.

## 8.4 DATA SECURITY AND CONFIDENTIALITY

Data security and the confidentiality of data in computers and data banks are continuing concerns. EUIS increase these concerns because they provide wider access to data and to devices for manipulating them and easily transmitting them. Desktop computers are linked to other company computers, and, through the Internet, to the world.

EUIS present several distinct security problems. The first is protecting programs and data from unauthorized access from inside as well as outside the organization. Insiders who gain access to specific information or inadvertently damage files are perceived to be a greater threat than outside hackers. The second security issue is the problem of protecting stored or archival information. A third issue is related to safe and appropriate use of internal and external communications—e-mail.

End users may be less informed than computer professionals about the requirements of confidentiality for client and employee data. Control of databases often is separated from responsibility for their integrity and reliability. The same level of control usually is not built into desktop computer applications as is built into central systems. Yet stored information may be used and updated by novices unfamiliar with many of the software features. Moreover, the Internet enables work to be done away from the office—at home, in airplanes, in hotels, or in client offices—which increases the risk of loss, damage, or theft.

It is extremely difficult to safeguard programs and data. Data can be copied or destroyed easily, and with Internet connections, the potential for abuse has increased. Theft or misuse of sensitive data has always been a threat, even before computers. Before networks, however, it was more difficult to conceal large piles of paper or large computer tapes. It took time to hand copy, type, or even photocopy pages of information. Today, individuals can copy a wealth of information onto disks or through the Internet. Moreover, one can easily steal data by copying it and leave the original data intact.

*Intranets* are internal networks that typically have firewalls to protect their internal operations from outsiders. *Firewalls* provide a barrier for employees to transfer data out and better protect information and internal communications from those outside the organization. To improve communications and data flow between an organization and its partners, suppliers, or clients, organizations increasingly are using Extranets. An

*Extranet* is a Web-based platform that controls data exchange with specified parties, viewable through a Web browser. This minimizes software requirements[9] and allows authorized users access to the data they need to do their work.

Managers must assess the company's exposure carefully. They must identify what it is they need to protect and the possible risks. They must determine how much time and expense are warranted and establish appropriate measures. The resources invested may depend on factors such as the number of users, types of applications, corporate culture, and whether the network is connected to other networks, an Intranet, Extranet, or the Internet. For example, an Intranet that supports an important transaction processing application, critical databases, or confidential legal documents would warrant a firewall.

1. Establish a clear, organizational policy on what types of data are considered sensitive. Ensure that every sensitive data set has a designated custodian to bear responsibility for its safekeeping.
2. Establish a policy that no sensitive information may be stored in a file, either temporarily or permanently, on a hard disk when that computer also is connected to the Internet.
3. Ensure that a locked area or cabinet is available for all backup data containing sensitive information. Access should be possible only for the data custodian.
4. Encourage the use of encryption for sensitive data files.

**Figure 8.5** Tactics for better protection of sensitive computer data

This message is for the named person's use only. It may contain confidential, proprietary, or legally privileged information. No confidentiality or privilege is waived or lost by any mistransmission. If you receive this message in error, please immediately delete it and all copies of it from your system, destroy any hard copies of it, and notify the sender. You must not, directly or indirectly, use, disclose, distribute, print, or copy any part of this message if you are not the intended recipient. (Company Name) and each of its subsidiaries reserve the right to monitor all e-mail communications through its networks. Any views expressed in this message are those of the individual sender, except where the message states otherwise and the sender is authorized to state them to be the views of any such entity.

**Figure 8-6** E-mail disclosure statement

Suggested tactics for protecting sensitive computer data are presented in Figure 8-5.

Additionally, in networked, global organizations, e-mail policies are being revised constantly to protect communications for corporate confidentiality, as well as to protect the organization from legal misuse of data. Figure 8-6 is a sample disclosure statement that could appear at the bottom of users' e-mail messages.

## 8.5 INFORMATION ACCURACY AND RELIABILITY (INTEGRITY)

What does a manager do when the individual who developed a program that is used regularly is promoted to another department or leaves the company? Who is responsible when a monthly report is inaccurate because a formula was altered inadvertently? Whose figures does the executive accept when department managers show up at a meeting with three different versions of divisional sales results? These are just some of the questions and issues related to the accuracy and reliability of computer information.

Problems arise in part because of the complexities of computer programs and the difficulties involved when one person tries to figure out the logic of a program developed by someone else. These problems can be reduced significantly when computer programs are documented adequately.

### 8.5.1 Preparing Documentation

*Documentation* is a detailed, written explanation of how a computer program works. It details the programming logic, variables, formulas, processed data (and where it comes from), and any other items pertinent to the creation and use of the program. Documentation usually is contained within a program and also in supplementary reference documents (referred to as *run books).* Database and CASE tools provide support in the form of data dictionaries and other tools to help manage the onerous task of documentation.

If a spreadsheet or a program is used by someone other than the individual who created it or is intended for departmental information (rather than individual calculations), thorough documentation is essential. Without documentation, it is extremely time consuming for anyone other than the program originator to modify or correct it. Documentation also serves as a tool for verifying the correctness of a program or reconstructing it if disks containing the program are destroyed or damaged. A good technique for documenting spreadsheet programs is to print out all the formulas used to create the program. Most spreadsheet programs provide this option.

### 8.5.2 Ensuring the Accuracy of Computer Programs

Professional programmers are well aware that many errors and problems can creep into computer programs, and they realize that errors are difficult to detect. The structured design and programming methods used by technical departments are designed to minimize risks. Managers also need to be aware of potential problems and see that programs developed by their staff are tested and verified adequately.

In the rush of everyday business, it is easy for users to overlook the importance of extensive testing and verification. Managers and users must be aware of the risks and learn appropriate procedures. The Association of Computer Users recommends that before any program is put into full use, it be run concurrently with the existing manual system, if one exists. Good programming helps a user discover errors. Accounting programs with audit trails or database management systems that will reject letter input where there should be numbers (and vice versa) help keep input errors to a minimum. For number-crunching applications, users could calculate the number of entries and batch totals before data are entered in the computer. These item counts and totals can be used to verify the accuracy of the data and determine whether errors were made as the data were keyboarded into the program. Applications packages themselves can help managers and users verify and document the accuracy of spreadsheets. Excel, or example, includes an auditing function on its Tool menu. Most users, however, are unaware of its existence.

Managers could cross train personnel to do each other's jobs to prevent an operation from coming to a stop when an employee is sick or on vacation. Job rotation can help

keep skill levels up, as well as provide employees with opportunities to review each other's work. Dividing responsibility for various phases of computer operation increases the chance that one user will detect another's errors.

Managers can insist on careful testing and validation of all calculations performed on the computer. An error in a single formula or a mistyped figure easily can produce inaccurate results in computer spreadsheets—just as they do in manual calculations. Actions that a manager can take to establish controls include the following:

1. *Establish controls to verify the accuracy and integrity of spreadsheets.* Examples include independent reviews, walk-throughs, and parallel runs. (A walk-through checks the program logic by manually doing each step in the program in the programmed sequence.) The accuracy of spreadsheets can be verified by comparing results against the same calculation done manually. Old manual reports can be used for test data, or duplicate calculations can be performed.
2. *Carefully document all spreadsheets.* Documentation could include data prepared, programs used, department of origin, and other relevant information. It also is recommended that employees print out and verify the accuracy of all formulas used in the spreadsheet.
3. *Remind individuals that they are accountable for their work.* "The computer made a mistake" is not an acceptable excuse.

1. All customized programs should be validated and certified for accuracy.
2. All corporate databases, wherever they are stored, should have user-accessible date and time fields to indicate the last time the database was modified
3. All EUIS output should be marked clearly with date and time of production. If the report draws upon any external database, the report should note that database's date and time stamp.
4. All analytical data reports done on desktop computers should have independent validations of data input and embedded formulas. Analytical models are to be checked for conceptual accuracy as well as clerical accuracy. The checkers should initial the reports and note the date and time.
5. As a matter of policy, no corporate decisions shall be made on the basis of any desktop computer-based data unless they meet all the conditions set above.

**Figure 8-7** Tactics for improving the integrity of computer data

For additional recommendations on improving the integrity of computer data, see Figure 8-7.

## 8.5.3 Developing Guidelines for Information Systems Security

Major threats to information system security are shown in Figure 8-8. The types of security threats are listed in the left column, and the two right columns differentiate between intentional acts of malice and human error or naturally caused accidents.

Disasters and vandalism (Items 1 and 2 in Figure 8-8) that damage equipment or software are risks to microcomputers just as they are to large systems. Items 3 through 6 in Figure 8-8 represent cases where information is compromised either by unsystematic error or total loss. The key to solving these problems is the maintenance of adequate backups. Items 7 and 8 represent situations in which systematic error is entered into data through incompetence or criminal intent. The controls

| THREATS TO INFORMTION SYSTEM SECURITY | | |
|---|---|---|
| | **HUMAN ERROR AND NATURAL ACCIDENT** | **ACTS OF MALICIOUS INTENT** |
| Physical resource damage | 1. Disasters | 2. Vandalism |
| Random information modification | 3. Mistakes | 4. Pranks and nuisances |
| Destruction of information | 5. Erasure | 6. Sabotage |
| Systematic information modification | 7. Incompetence | 8. Fraud and embezzlement |
| Disclosure of confidential information | 9. Exposure | 10. Data theft |

**Figure 8-8** Threats to information system security

against these threats are primarily quality-assurance checks, audits, division of responsibility, and the like. Items 9 and 10 represent threats of disclosure of sensitive information. Controls involve taking care to secure information behind physical and logical locks.[10]

## 8.6 LEGAL ISSUES

Who is responsible when Marc damages a company's notebook computer in an accident while he is transporting it home? Courteney decides to market a software program she developed at home on the company's computer. She uses the program on her job, but developed it primarily on her own time at home. Preston claims that a fire in his home was started by a short circuit in his company's desktop computer, which he brought home from work. Bob's four-year-old son destroyed the program disk for the database package that the department just purchased for $500. Bob brought it home to finish a project that was due the next day. Clearly, EUIS have raised a number of legal issues and concerns for business managers.

### 8.6.1 Defining Corporate Versus Personal Data or Programs

An important measure that organizations can take is to establish clear policies on the ownership of programs or data created on company time or equipment and to require employees to sign covenants before being assigned to development projects or authorized to borrow equipment. Whether strict measures are warranted depends, of course, on how sensitive or important information is to the company.

### 8.6.2 Preventing Unauthorized Copying of Software

Software *copyrights* limit the rights of purchasers to copy or modify software programs. Making multiple copies of software to distribute in an office is a clear violation of most copyright agreements, and violation of these agreements subjects the organization to liability suits from software vendors.

The right to copyright software was established by the Software Act of 1980, which modified the federal Copyright Act. When software programmers (or others) obtain a copyright, they retain the exclusive right to reproduce or modify their software. Thus, others are prohibited from copying or modifying. A copyright grants five exclusive rights:

1. The exclusive right to make copies.
2. The exclusive right to distribute copies to the public.
3. The exclusive right to prepare derivative works.
4. The exclusive right to perform the work in public. (This applies mainly to plays, dances, and so on, but also could apply to software.)
5. The exclusive right to display the work in public (such as showing a film).

Software often is sold under licensing agreements that may be more or less stringent than the copyright laws. It is common to see a warning on a package of program disks that the purchaser read all terms and conditions carefully *before* opening the package, because opening the package constitutes acceptance of such terms and conditions. Often these agreements stipulate (among other conditions) that use of the program is restricted to one machine and often one user. The purchaser may be requested to provide the serial number of the machine when returning the software registration form (which is required for ongoing support from the manufacturer). It is not yet clear to what extent these licensing agreements are valid and under what circumstances they will stand up in a court of law. Some states have passed, or are considering, laws to make such agreements valid.

Many users object to copyright restrictions or licensing agreements on the grounds that they encumber legitimate uses of software. For example, some agreements specify no copying, which leaves it unclear whether making a copy of a software program on a hard disk violates the copyright. Even if the first copy is legal, what about copies created during routine backup of the hard disk? For example, wording, such as “Although you are encouraged to make a backup copy of the Software for your own use, you are not allowed to make unlimited copies,” still leaves the issue of multiple backup copies ambiguous. Some software manufacturers prevent the user from copying the program diskette more than once. Thus, if the hard disk fails, the user would not be able to recopy the programs onto a hard disk a second time. These restrictions also may interfere with regular backup of the hard disk. Corporations arid other large software purchasers have been pressuring manufacturers for site-licensing (discussed later in this chapter) and other agreements that would better meet their needs. EUIS analysts and managers should monitor these legal issues and keep them in mind when negotiating with software vendors.

**SPOTLIGHT ON SOLUTIONS → Technology, People, Structure, Processes**

## PUBLIC SECURITY

Imagine if hackers broke into your local health department's computer system and discovered sensitive information in your medical history. What if they compromised the 911 system or tinkered with your property tax assess-merits? The consequences of such security breaches are almost unthinkable—and that's exactly why government agencies *have* to think about them.

In October 1998, R. A. Vernon of the City of New York's Department of Investigation became the city's first chief information security officer, heading up its new security organization: Citywide Information Security, Architecture, Formulation and Enforcement (CISAFE), a unit of the Department of Investigation. CISAFE has been given the task of overseeing and coordinating security in all city agencies—more than 60 in all—covering everything from Intranets and Extranets to networks, desktop security and communications.

"Our goal is to make the City of New York a star location by creating the right security model, deploying the right technology and keeping it on the cutting edge Vernon declares

The City of New York—which has more than 350,000 employees and more than 100,000 computer systems— is moving toward an e-government model. For instance, it is enabling drivers to pay parking tickets and allowing property owners to check their property tax assessments over the Internet. At the same time, it is taking steps to employ the latest technologies to keep these systems secure.

Deploying updated security standards and tools is key to this effort. "We're working on guidelines,"
Vernon reports. "The agencies already have controls in place, and CISAFE is studying them so it can leverage the existing efforts and expertise of the city agencies to identify best practices."

Implementing standards based on these best practices will provide consistency across city agencies. "Consistency will give the city the ability to leverage its intellectual capital," Vernon explains. "If all agencies use the approved standards and tools, an individual agency can look to another for assistance when it encounters a problem. What they're trying to protect may differ from agency to agency, but standards are standards, and the controls are similar."

Once implemented, standards must be kept current. "Standards have to change rapidly or you risk exposure," Vernon explains. "It's a constant battle. As security breaches are identified or new technologies are introduced, the right measures and technologies must be deployed.

After all, security is only as good as the latest technology
Our job is to stay one step ahead of the hackers."

Vernon plans to work closely with the city agencies to see that they adhere to similar security procedures. He wants to ensure for example, that firewalls and routers throughout the city are current and configured in a similar manner, that servers aren't accessible without proper authorization and that applications are developed with proper security safeguards, such as virus protection.

Currently many city agencies use Extranets and data often moves beyond the confines of city agencies to the state government and even the federal government. Thus CISAFE is doing a formal assessment of the connections and controls m place We need to work with the state to make sure data passes in a secure way," Vernon emphasizes

Technologies such as public key infrastructure(P1(I) will also play a role. "In the future, we'd like to take advantage of PKI, which offers a set of security tools the agencies can use as they develop applications," he reports. "It will provide a single point at which everyone, including external users, must sign in."

All security technologies, he adds, depend on users to make them effective. "Security is a people issue, not an IT issue," he says. "Everyone needs to be aware of it, and education is the key. If you explain to employees why security is important and sell them on the concept, they be come your foot *soldiers."—Eileen McCooey and S. D.*

*Source:* Reprinted from an article by Sam Dickey, with permission from *Beyond* magazine, January/February 2000,  For more articles on information security go to *www.beyondcomputing.com*

Managers can take several steps to help control unauthorized copying of software. First, the organization can establish a clear policy forbidding unauthorized copying of software. The policy can establish penalties for infractions and should be published and disseminated to all employees. Second, employees can be educated regarding the rules and restrictions for copying software. Users can be reminded of the ethics of unauthorized copying and the corporation's exposure to legal action.

Some companies make software available on their network server through contractual arrangements with vendors that allow it to be used on any desktop computer connected to the server. Such agreements reduce the use of application programs on hard disks, which are copied easily.

- Specify all sales claims and promises in writing.
- Establish the time frame within which these claims should be carried out.
- Clarify the performance of the system or services the vendor will provide
- Specify the price of the product or service
- Specify how payment should be made.
- Describe the kind of product or service provided
- State any provisions that allow the purchaser to reject the product or service if it fails to perform to standard.
- Identify the forum that has jurisdiction in the event of litigation
- Spell out any penalty or cancellation clauses, and when they come into play.
- Clarify responsibility for installation and maintenance of the equipment and for training in-house personnel

**Figure 8-9** Summary of software contract terms

## 8.6.3 Developing Hardware and Software Contracts

When managers have the autonomy to sign hardware or software purchase contracts, they should be aware of possible pitfalls or problems. A well-drawn contract should specify the rights, duties, and obligations of the seller and purchaser. Managers should check with their legal departments before signing computer hardware or software contracts. Figure 8-9 lists terms that contracts should include:[11]

Some vendors offer *site-licensing* arrangements that can help organizations reduce their exposure to illegal copying. Site-licensing arrangements also can reduce the order, reorder, and program-upgrade headaches that come with buying volume copies of software. Two categories of site-licensing arrangements often are offered by vendors:

1. *Full site-licensing agreements,* which allow users to duplicate the program disk and documentation in-house.
2. *Volume-purchasing agreements,* which offer pricing discounts based on the number of copies ordered.

Site-licensing agreements may offer additional benefits, such as technical support, newsletters, or training. Some plans incorporate clauses that limit an organization's liability for unauthorized copies to the retail price of the copies duplicated.

### 8.6.4 Preventing Unauthorized Access to Programs and Data

Passwords are like underwear. Change yours often.....
Don't share yours with a friend.

— University of Michigan Guidelines

A first-line defense against unauthorized users gaining access to computer systems is the use of passwords. A password is a group of characters that a user must enter into a system to gain access to programs or data. Although computer hackers typically have little trouble getting beyond this first-line defense, passwords that are updated frequently and regularly can better ensure that the system is used only by those who are cleared to use it. Without passwords, for example, an employee could tamper with the department budget, perhaps adding some fictitious expenses and then collecting the money later. Tips for creating passwords are offered in Figure 8~1O.12

An emerging problem is how to remember all the passwords one has for various systems. We now have to develop and maintain passwords for work-based computing,

- Avoid personal information and common words
- Use at least six characters, and mix uppercase and lowercase
- Combine numbers and symbols
- Put in a spelling mistake on purpose
- Take a phrase and use only the first letters (e.g., "To be or not to be" would be TBONTB)
- Translate your password into a foreign language

**Figure 8-10** Tips for creating passwords

as well as home-based computing. A given user could have a password for an AOL account, a mutual fund, an e-mail account, and so on; it is not uncommon for a user to have more than 25 different passwords. Suggestions abound for dealing with password overload: You could use the same password for multiple applications; however, this is a security risk. You could keep all your passwords together in a single file, with a password for access (yet another security risk). High-tech remedies currently being used include smart cards and biometric devices that rely on fingerprints or retina scans.[13]

## 8.7 RESOURCES. PRODUCTS, AND SERVICES

A variety of resources, products, and services is available to help monitor hardware and software. Managers must assess the risks and determine how much effort and expense should be spent to provide adequate protection. The answer to the question of "which product to buy" depends on how much protection is needed. Managers also must assess how much convenience and accessibility they want to trade for protection and security.

### 8.7.1 Auditing Procedures for EUIS

The auditing department is an important ally in helping managers establish control procedures to ensure the proper use of information systems. Auditors can help a manager in several ways:

- Designing control systems and procedures for managing information flow.
- Stipulating specific requirements for documentation, control, and systems access.
- Developing audit trails that document personal responsibility for actions taken.
- Reviewing procedures for meeting requirements and ensuring that they are met.

One argument is that security and audit procedures should be concentrated on applications rather than hardware or systems software. The question should not be How do I protect a PC? or What security do I need on a LAN? Instead, managers and auditors should focus on requirements for specific applications)[4] The following directions and questions would be more appropriate: Describe the applications. What is the nature and value of the information? Who is involved in the process? Where does the information come from and where does it go? At what point in the process can I attest to its integrity?'[5] Organizations must make a clear statement about the importance of information security and auditing controls.

## 8.7.2 Hardware and Data Security

Several products and services that address desktop computer and peripherals security needs are available. This section provides a sampling of some of the types of products that offer solutions. A comprehensive discussion is not intended.

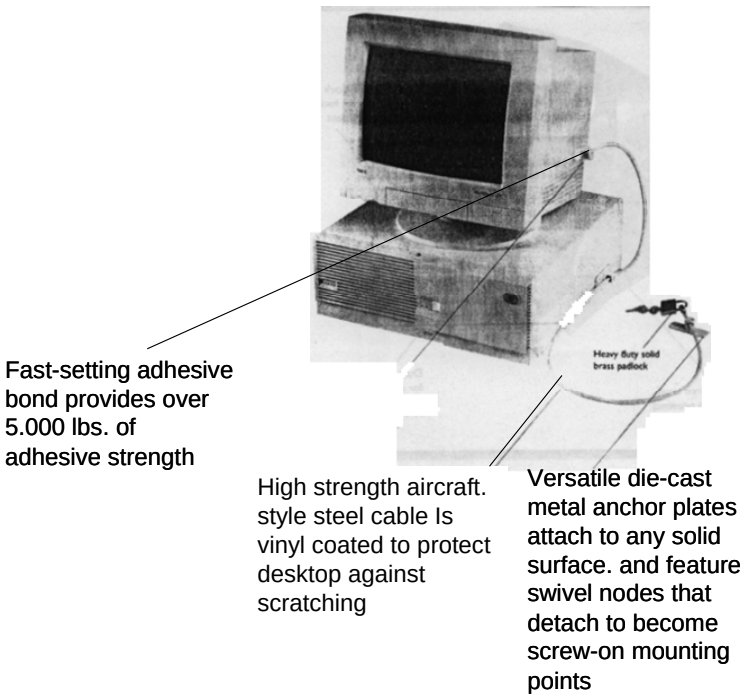


**Figure 8-11 Computer security devices a. Cable security**
*Source:* With permission from Christopher Meyer, AnchorPad Products, Cypress, CA.

### *8.7.2.1 Hardware Security Systems*

Many devices are available to secure computers to work surfaces or lock them so as to control access. AnchorPad International markets a myriad of such security products, and samples are pictured in Figure 8-11. Devices can be as simple as cables, adhesive bond, and padlocks (Figure 8-ha) or more elaborate entrapment systems that encase the computer system (Figure 8-lib). Another device protects tower computers from theft, tampering, vandalism, and damage by suspending the tower beneath the desktop, freeing space on top of the desk and at the same time keeping the tower off the floor (Figure 8-lic).

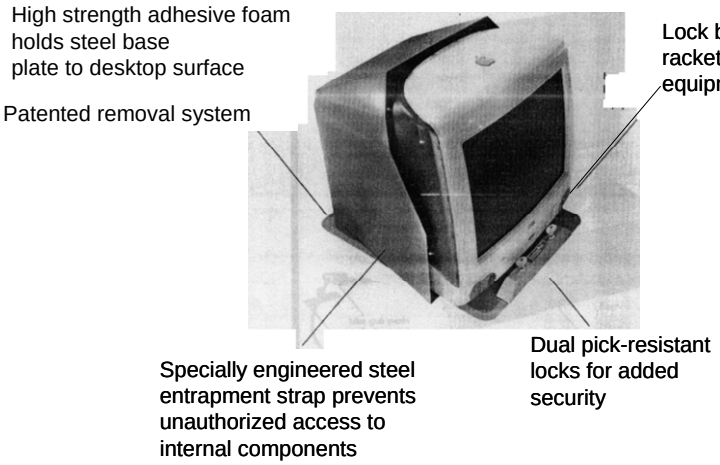


**Figure 8-11 b.**Entrapment security
*Source:* With permission from Christopher Meyer, AnchorPad Products, Cypress, CA.

The importance of security is underscored with the Computer Security Institute estimate that half of U.S. companies have notebook computers stolen every year.'[6] To counter this danger, security devices for notebook computers allow users to lock their notebook down in virtually any location (Figure 8-lid); another is an anchoring plate that can be used at a workstation (8-lie).

Another type of security system is aimed at the operability of a computer. It comes on a circuit board and is plugged into one of the computer's expansion slots. Users must provide their correct identification~ code and password. Although board-based products provide tight control, these products may work with only certain models of computers.

Some software-based products control access to the hard disk but do not prevent users from working with disks, unless the computer has no disk drive. While some of these products are designed only for specific models, other products work with almost any operating system. They are virtually hardware-independent, and some offer data encryption.

### *8.7.2.2 Data Encryption*

The products just described are designed primarily to prevent access to devices or data. Data encryption goes a step farther by making information unintelligible even if it is accessed. *Data encryption* uses a mathematical algorithm to scramble data. Two types of

data encryption are the public-key type and the Data Encryption Standard (DES). DES, developed in the early 1970s by IBM and adopted by the National Bureau of Standards in 1976, combines two operations called substitution (replacing information) and transposition (scrambling information).

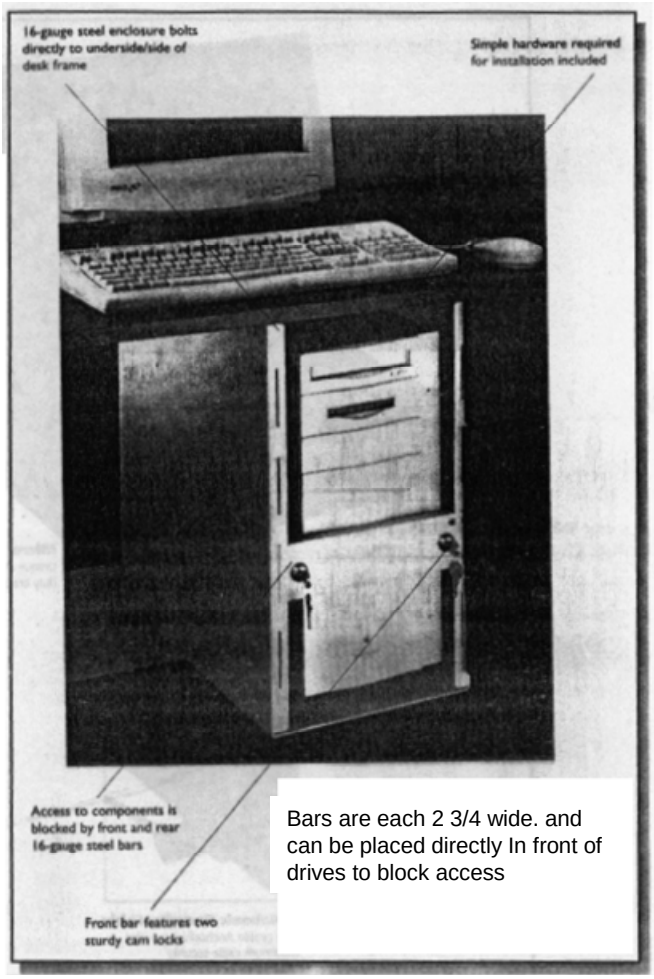


**Figure 8-11** c. Covert under desk tower security system

*Source:* With permission from Christopher Meyer, AnchorPad Products, Cypress, CA.

These two operations transform plaintext or cleartext into ciphertext. The person who deciphers the encrypted text uses the same key that encrypted the data to reverse the substitution and transposition process. The algorithm for DES encryption has 64 bits, 56 of which are active bits, and S are used to detect errors in transmission. Public-key encryption

**Micro Slot Security Cable**
Unique micro slot clip with heavy duty bass padlock

**Notebook Security Cable**
Low profile AnchorPad provides maximum cable security

**Figure 8-11** d. The sentry
*Source:* With permission from Christopher Meyer, AnchorPad Products, Cypress, CA.

works with two keys for each user: a public encryption key and a private decryption key. The user keeps the private key to decrypt messages sent by anyone who has a public encryption key. The two keys are linked mathematically, but it is not feasible in terms of time and energy to figure out from the public key what the private key is. DES-based encryption is the most widely used, although many experts favor. the public-key method and predict increased use.

Although most of us associate data encryption with government secrets and spy novels, complex systems increasingly are being used to safeguard corporate data and secure sensitive information such as credit card numbers in e-commerce transactions. For desktop users, products such as Norton Secret Stuff (Asymetrix),

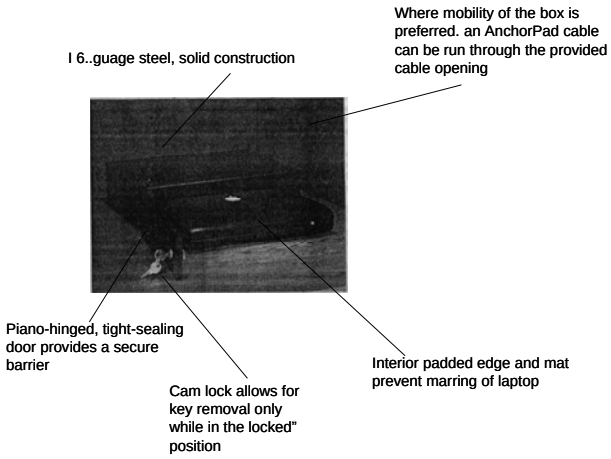


**Figure 8-11** e. Notebook cable security
***Source:*** With permission from Christopher Meyer, AnchorPad Products, Cypress, CA.
a simple encryption program that keeps e-mail messages private, works well but can be time consuming.

## 8.8 SUMMARY

Responsibility for managing safe and legal computer use falls directly on business managers. Often, in their enthusiasm for new-found opportunities, managers and users have overlooked risks and responsibilities. Unless they are informed about the issues related to managing EUIS, they may not recognize potential problems until disaster strikes.

Policies established by senior managers are an important first step toward showing employees that computer-related risks are a legitimate corporate concern.

Policies can foster an attitude of care and concern by making employees accountable for unauthorized acts involving computer and information resources. Policy statements should be distributed to all employees and should state clearly the company's positions regarding protection of information resources.

Acquisition guidelines must be established to avoid incompatible hardware and software, duplication of effort, and unnecessary spending. Equipment must be protected against damage, loss, or theft. Regular backup procedures are required to safeguard electronically stored data against accidental loss. Standard procedures for naming and storing files save time and effort. Managers also need to protect sensitive data against unauthorized access, tampering, or copying.

Viruses are malicious codes transferred to computer ifies (usually through the network) to destroy data or annoy users. Trojan horses attach themselves to specific application files, disrupting their operations. Worms attack data files by multiplying to the point where systems are shut down. All users are wise to use antivirus software to protect their valuable programs and data.

Without strict procedures in technical data processing departments, errors in end-user-developed programs may go unnoticed. A dangerous tendency is to accept detailed computer analyses without adequate verification. Managers must establish procedures to ensure that data produced and stored on departmental computers are accurate and reliable.

Among the legal issues raised by EUIS are ownership of employee-developed programs, prosecution from infringement of copyright laws, purchase and licensing arrangements, and responsibility for damage to hardware and software. Policies and guidelines are needed to minimize risks.

Several resources and services are available to help provide controls for managmg technology in the workplace. Auditors help assess risks and exposures, as well as recommend procedures to protect corporate resources and comply with corporate policies. Various products, such as locks, log-on programs, encryption programs, and security access controls, help secure hardware and software resources against unauthorized use.

Managers and employees need adequate guidelines and technical support to translate business needs into computer solutions. Along learning curve is involved as non-technical personnel gain experience in applying new computer tools. Managers must be aware of both the opportunities and the related risks of managing EUIS resources.

## KEY TERMS

- Backup
- Copyright
- Data encryption•

- Documentation
- Site license agreement
- Trojan horse
- Virus
- Volume purchase agreement
- Worm

## DISCUSSION QUESTIONS

1. What is the purpose of policy statements? Who writes them? Who follows them? Why are they important to the EUIS analyst?
2. Summarize the issue of data security in today's office environment.
3. What is meant by the term *backup?* Why are backup practices often ignored by computer users? What solutions to the problem exist?
4. Why is documentation considered a data reliability issue?
5. What options are available to the manager who wants to audit computer operations?
6. Identify legal issues related to computer software about which managers should be aware.
7. List steps a manager can take to help control unauthorized copying of software.
8. What is a computer virus? How do Trojan horses differ from worms?
9. Describe three devices that secure desktop computers from theft and two that secure notebook computers from theft.

## APPLICATION EXERCISES

1. Compose a policy statement that addresses legal concerns related to computer operations.
2. Visit the Web sites of security device makers. How do their products differ in terms of functionality and price?
3. Assume you are a manager who has hired a college student for a summer job. The job entails using an Intranet-based database. Role-play the computer orientation you will give the student, including backup policies and virus protection procedures.

## SUGGESTED READINGS

Fites, Philip; Peter Johnston; and Martin Kratz. *The Computer Virus Crisis.* (Upland, PA: Diane Publishing Company, 1999).

Kane, Pamela. *PC Security and Virus Protection Handbook: The Ongoing War Against Information Sabatoge.* (Upland, PA: Diane Publishing Company, 1999).

Spar, Debora and Jennifer Burns. *Network Associates: Securing the Web.* Harvard Business School Case Stud 799087: May 10, 1999.

Tipton, Harold F., ed. *Handbook of Information Security Management.* (Boca Raton, FL: CRC Press, Inc., 1999).

# ENDNOTES

1. Ken Michielsen, "A PC Policy Primer: A Few Basic Rules Lend Direction to MIS Departments Supporting Micros," *IBM Innovation* (1986): 4—5.
2. Mark Rowh, "Cy-Ber-Speak," *Office Systems* 16 (1999): 12.
3. Michael Gips, "Tracking Trojans," *Security Management* 43 (1999): 18.
4. Bruce Schneier, "The Trojan Horse War," *Communications of the ACM* 42 (1999): 128.
5. Todd Coopee, "Ecrix VXA-1 Launches New Tape Technology," *Info World* 21 (1999): 48—50.
6. Joseph F. Kovar, "Storage Vendors Invade Networld + Interop," *Computer Reseller News* (1999):129—130.
7. Coopee, op. cit. pp. 48—50.
8. Kelly Carroll, "A Whole New Provider," *Telephony* 237 (1999): 48.
9. Michael Mendoza, "Opening Up with Extranets," *Computer-Aided Engineering* 19 (2000): 20—26.
10. Joel S. Zimmerman, "PC Security: So What's New?" *Datamation* **(1985).**
11. August Bequai, "A Management Guide to a Good Computer Contract," *The Office* (1986): 23.
12. Gene Graber, "People Feeling Overwhelmed by Having to Recall So Many," *Denver Post*, January 10,2000.
13. lbid.
14. Harry B. DiMaio, "Who's Guarding Your PC?" *Words* (1985): 24.
15. Ibid.
16. "Hedging Hardware Heists: Quick Fix Lockdowns," *Security* 36 (1999): 89—90.