CHAPTER 9
INFORMATION SECURITY

Management Information Systems, 10th edition,
By Raymond McLeod, Jr. and George P. Schell

PEARSON
Prentice
Hall

Learning Objectives:

- Know that information security is concerned with securing all of the information resources, not just hardware and data.
- Know the three main objectives of information security.
- Know that management of information security consists of two areas-information security management (ISM) and business continuity management (BCM).
- See the logical relationship among threats, risks, and controls.

Learning Objectives (cont.):

- Know what the main security risks are.
- Know the process for implementing an information security policy.
- Be familiar with the more popular security controls.
- Be familiar with actions of government and industry that influence information security.
- Know the types of plans that are included in contingency planning.

Introduction

- Information security is intended to achieve confidentiality, availability, and integrity in the firm's information resources.
- The management of information security consists of:
  1. The day-to-day protection called information security management (ISM)
  2. Preparing for operating after a disaster called business continuity management (BCM)

INFORMATION SECURITY

- **Information security** describes efforts to protect computer and non computer equipment, facilities, data, and information from misuse by unauthorized parties
- This definition includes copiers, fax machines, and all types of media, including paper documents

Objectives of Information Security

- Information security is intended to achieve three main objectives:
  - **Confidentiality:** protecting a firm's data and information from disclosure to unauthorized persons
  - **Availability:** making sure that the firm's data and information is only available to those authorized to use it
  - **Integrity:** information systems should provide an accurate representation of the physical systems that they represent

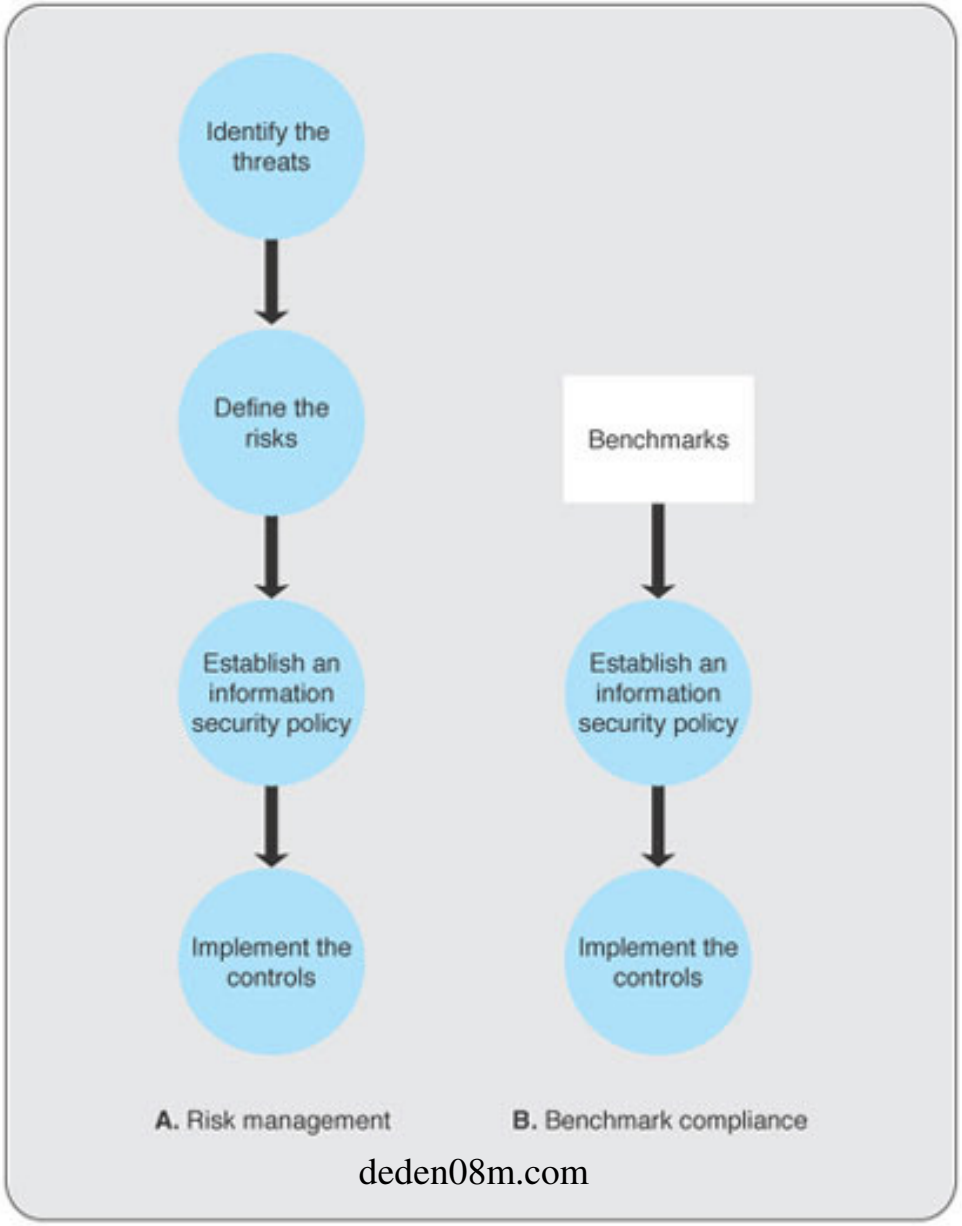
Management of Information Security

- The title **corporate information systems security officer (CISSO)** has been used for the person in the organization responsible for the firm's information systems security.
- Now there is a move to designate a **corporate information assurance officer (CIAO)** who reports to the CEO and manages an information assurance unit

INFORMATION SECURITY MANAGEMENT (ISM)

- ISM consists of four steps:
  1. Identifying the *threats* that can attack the firm's information resources
  2. Defining the *risks* that the threats can impose
  3. Establishing an information security policy
  4. Implementing *controls* that address the risks
- Figure 9.1 illustrates the risk management approach
- Benchmarks are also used to ensure the integrity of the risk management system

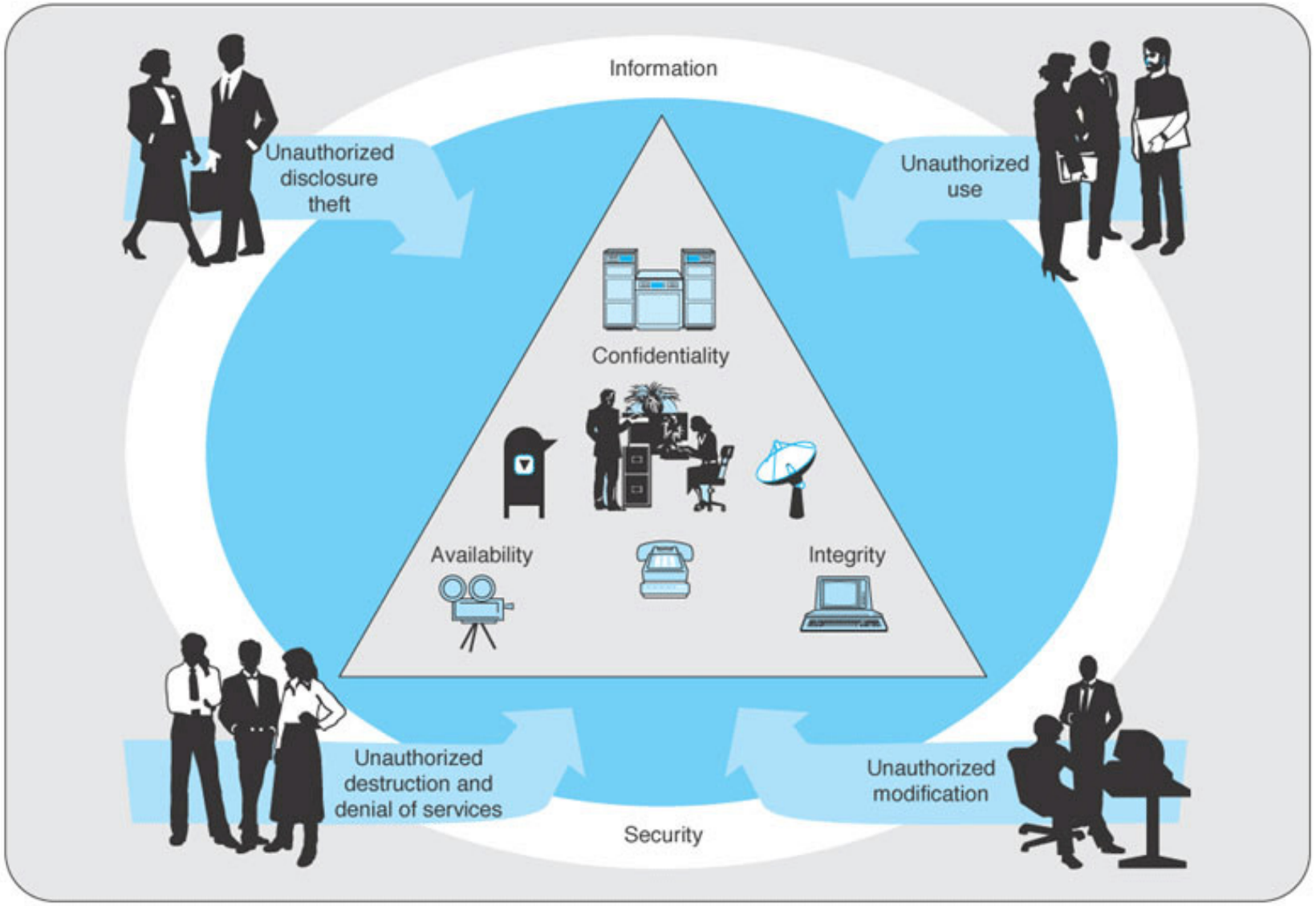
Figure 9.1 Information Security Management (ISM) Strategies



THREATS

- An information security **threat** is a person, organization, mechanism, or event that can potentially inflict harm on the firm's information resources
- Threats can be internal or external, accidental or intentional
- Figure 9.2 shows the information security objectives and how they are subjected to the four types of risks:
    - Internal and External Threats
    - Accidental and Deliberate

Figure 9.2 Unauthorized Acts Threaten System Security Objectives



RISKS

Unauthorized acts that present risks can be categorized into four types:

Unauthorized Disclosure and Theft

1. Unauthorized Use
2. Unauthorized Destruction and Denial of Service
3. Unauthorized Modification

THE MOST NOTORIOUS THREAT—THE "VIRUS"

- A **virus** is a computer program that can replicate itself without the user's knowledge
- A **worm** can't replicate itself within a system but can transmit copies of itself by e-mail
- A **Trojan horse** can neither replicate nor distribute itself. Distribution is accomplished by users who distribute it as a utility that, when used, produces unwanted changes in the system's functionality

E-COMMERCE CONSIDERATIONS

- E-commerce has introduced a new security risk: credit card fraud. Both American Express and Visa have implemented programs aimed specifically at e-commerce
- American Express has announced "disposable" credit card numbers. These numbers, rather than the customer's credit card numbers, are provided to the e-commerce retailer, who submits it to American Express for repayment
- Visa has announced ten security-related practices they expect their retailers to follow plus three general practices that retailers should follow (next slide)

Visa's Security Precautions

Retailers must:

- Install and maintain a firewall
- Keep security patches up to date
- Encrypt stored data and transmitted data
- Use and update antivirus software
- Restrict data access to those with a need to know
- Assign unique IDs to persons with data access privileges
- Track data access with the unique ID
- Not use vendor-supplied password defaults
- Regularly test the security system

Retailers should:

- Screen employees who have access to data
- Not leave data (diskettes, paper, and so forth) or computers unsecured
- Destroy data when it is no longer needed

RISK MANAGEMENT

- The four sub steps to defining information risks are:
  1. Identify business assets to be protected from risks
  2. Recognize the risks
  3. Determine the level of impact on the firm should the risks materialize
  4. Analyze the vulnerabilities of the firm
- A systematic approach can be taken to sub steps 3 and 4 by determining the impact and analyzing the vulnerabilities
- Table 9.1 illustrates the options.

Table 9.1

Degree of Impact and Vulnerability Determine Controls

	Severe Impact	Significant Impact	Minor Impact
High Vulnerability	Conduct vulnerability analysis. Must improve controls.	Conduct vulnerability analysis. Must improve controls.	Vulnerability analysis unnecessary.
Medium Vulnerability	Conduct vulnerability analysis. Should Improve controls.	Conduct vulnerability analysis. Should Improve controls.	Vulnerability analysis unnecessary.
Low Vulnerability	Conduct vulnerability analysis. Keep controls intact.	Conduct vulnerability analysis. Keep controls intact.	Vulnerability analysis unnecessary.

Risk Analysis Report

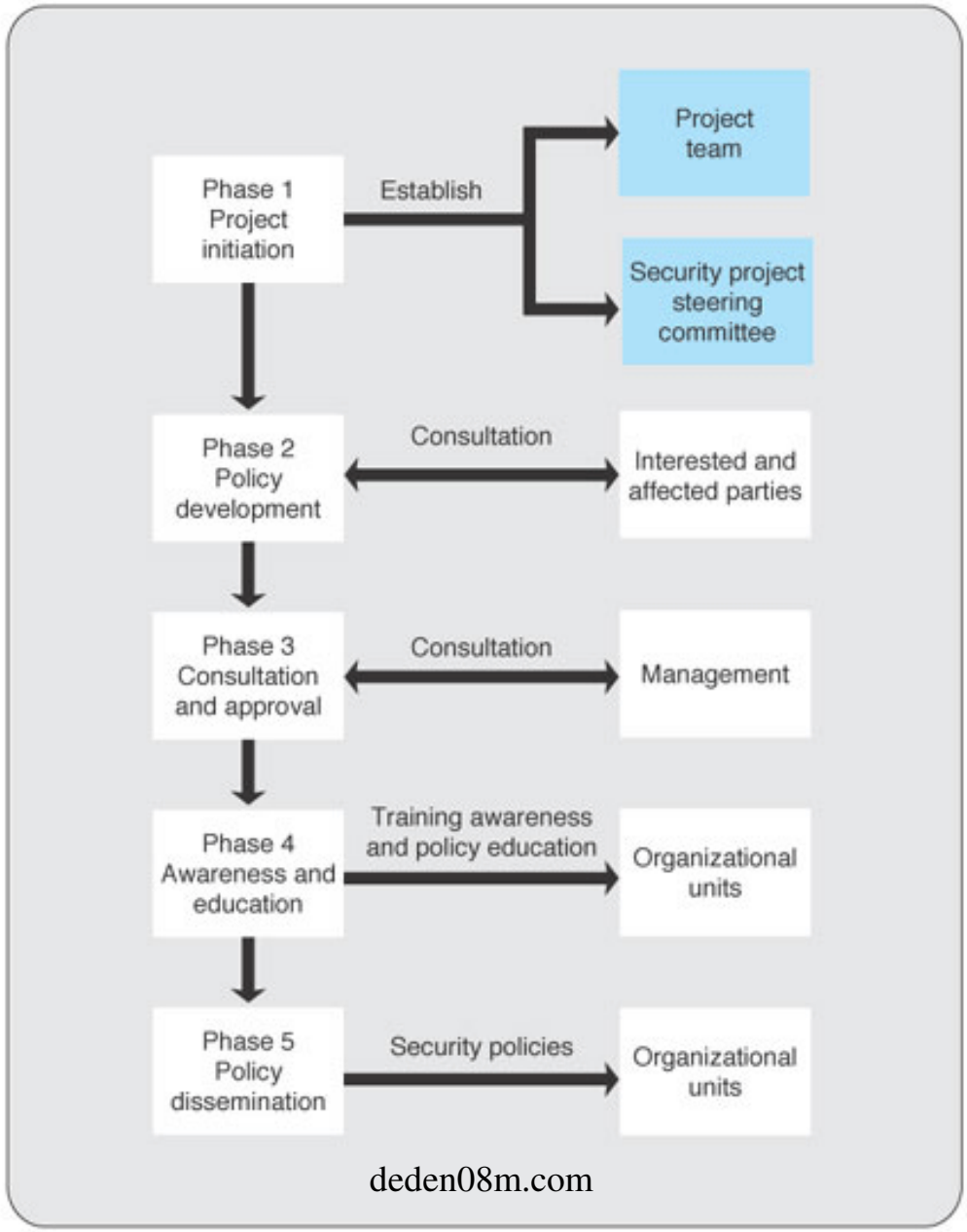
- The findings of the risk analysis should be documented in a report that contains detailed information such as the following for each risk:

1. A description of the risk
2. Source of the risk
3. Severity of the risk
4. Controls that are being applied to the risk
5. The owner(s) of the risk
6. Recommended action to address the risk
7. Recommended time frame for addressing the risk
8. **What was done to mitigate the risk**

INFORMATION SECURITY POLICY

- A security policy can be implemented using the following five phase approach (Fig. 9.3):
    - Phase 1: Project Initiation
    - Phase 2: Policy Development
    - Phase 3: Consultation and Approval
    - Phase 4:Awareness and Education
    - Phase 5: Policy Dissemination

Figure 9.3 Development of Security Policy



Separate policies are developed for:

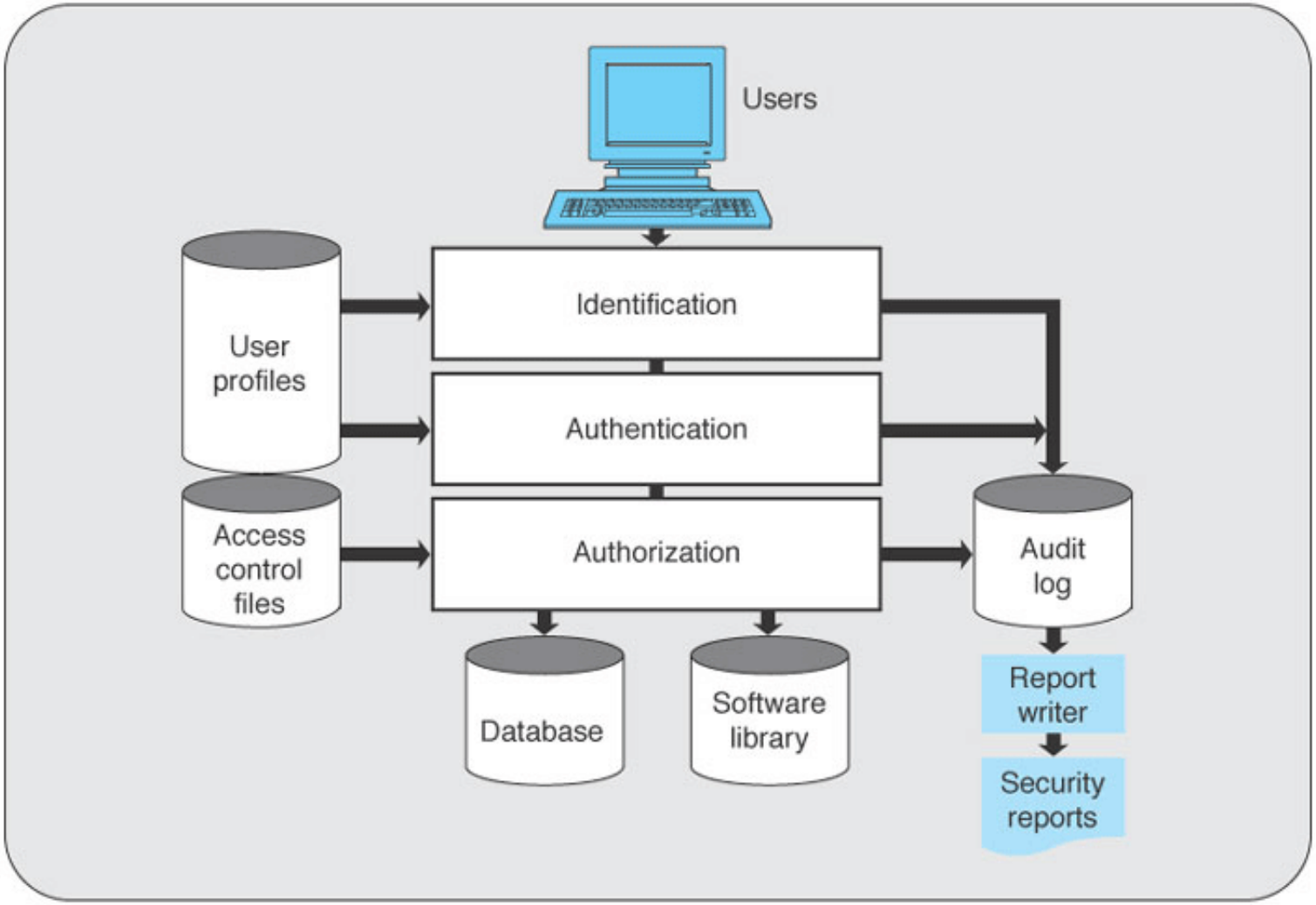
- Information systems security
- System access control
- Personnel security
- Physical and environmental security
- Telecommunications security
- Information classification
- Business continuity planning
- Management accountability

These policies are distributed to employees, preferably in writing and in educational and training programs. With the policies established, controls can be implemented

CONTROLS

- A **control** is a mechanism implemented to protect the firm from risks or minimize the impact of those risks on the firm should they occur:
  1. **Technical controls** are those built into systems by system developers during the system development life cycle
  2. **Access control** is the basis for security against threats by unauthorized persons
  3. **Intrusion detection systems** try to recognize an attempt to breach security before it has the opportunity to inflict damage

Figure 9.4 Access Control Functions



Source: Ken Cutler, "Hackers, Viruses, Thieves, and Other Threats to Your Information Assets," in Computer Security Seminar Course Material *(NY:ACM 1991)*

Access Control

1. **User identification**. Users first identify themselves by providing something that they *know*, such as a password
2. **User authentication.** Once initial identification has been accomplished, users verify their right to access by providing something that they *have*, such as a smart card or token, or an identification chip
3. **User authorization**. With the identification and authentication checks passed, a person can then be authorized certain levels or degrees of use. For example, one user might be authorized only to read from a file, whereas another might be authorized to make changes

Firewalls

- A firewall acts as a filter and barrier restricting the data flowing between the firm's network and the Internet
- There are three types of firewalls:
  - **Packet-Filters –** are routers equipped with data tables of IP addresses which reflect the filtering policy positioned between the Internet and the internal network, it can serve as a firewall
  - **Circuit-Level Firewall –** installed between the Internet and the firm's network but closer to the communications medium
  - **Application-Level Firewall –** located between the router and the computer performing the application

Cryptographic Controls

- **Cryptography** is the use of coding by means of mathematical processes
- The data and information can be encrypted as it resides in storage and or transmitted over networks
- If an unauthorized person gains access, the encryption makes the data and information unreadable and prevents its unauthorized use
- Special protocols such as **SET** (Secure Electronic Transactions) have been developed for use in e-commerce

FORMAL CONTROLS

- Formal controls include the establishment of:
  - Codes of conduct
  - Documentation of expected procedures and practices
  - Monitoring and preventing behavior that varies from the established guidelines
- The controls are formal in that management:
  - Devotes considerable time to devising them
  - They are documented in writing
  - They are expected to be in force for the long term

INFORMAL CONTROLS

Informal controls include such activities as:

- Instilling the firm's ethical beliefs in its employees;
- Ensuring an understanding of the firm's mission and objectives;
- Education and training programs; and
- Management development programs

These controls are intended to ensure that the firm's employees both understand and support the security program

ACHIEVING THE PROPER LEVEL OF CONTROLS

- As all three types of controls, technical, formal, and informal - cost money
- The idea is to establish controls at the proper level
- The control decision boils down to cost versus return, but in some industries there are other considerations
- In banking, when engaging in risk management for ATMs, controls must keep the system secure but not at the cost of diminishing customer convenience
- In health care, the system should not be so secure as to reduce the amount of necessary patient information available to hospitals and physicians

GOVERNMENT AND INDUSTRY ASSISTANCE

- Several governments and international organizations have established standards (next slide) intended to serve as guidelines for organizations seeking to achieve information security
- Some are in the form of benchmarks, sometimes referred to as a *baseline*

Government and Industry Assistance

- **United Kingdom's BS7799** The UK standards establish a set of baseline controls. Both Australia and New Zealand have instituted controls based on BS 7799
- **BSI IT Baseline Protection Manual** The baseline approach is also followed by the German Bundesamt fur Sicherheit in der Informationstechnik (BSI). The baselines are intended to provide reasonable security when normal protection requirements are intended. The baselines can also serve as the basis for higher degrees of protection when those are desired
- **COBIT** COBIT, from the Information Systems Audit and Control Association & Foundation (ISACAF), focuses on the process that a firm can follow in developing standards, paying special attention to the writing and maintaining of the document
- **GASSP** Generally Accepted System Security Principles (GASSP) is a product of the U. S. National Research Council. Emphasis is on the rationale for establishing a security policy
- **GMITS** The Guidelines for the Management of IT Security (GMITS) is a product of the International Standards Organization (ISO) Joint Technical Committee and it provides a list of the information security policy topics that should be included in an organization's standards
- **ISF Standard of Good Practice** The Information Security Forum Standard of Good Practice takes a baseline approach, devoting considerable attention to the user behavior that is expected if the program is to be successful

GOVERNMENT LEGISLATION

- Governments in both the U.S. and U.K. have established standards and passed legislation aimed at addressing the increasing importance of information security:
  - U.S. Government Computer Security Standards
  - The U.K. Anti-terrorism, Crime and Security Act (ATCSA) 2001
  - U.S. Government Internet Crime Legislation

INDUSTRY STANDARDS

- **The Center for Internet Security** (CIS) is a non profit organization dedicated to assisting computer users to make their systems more secure
- CIS Benchmarks have been established and are integrated in a software package that calculates a "security" score on a 10-point scale

PROFESSIONAL CERTIFICATION

- Beginning in the 1960s the IT profession began offering certification programs:
  - Information Systems Audit and Control Association (ISACA)
  - International Information System Security Certification Consortium (ISC)
  - SANS (SysAdmin, Audit, Network, Security) Institute

PUTTING INFORMATION SECURITY MANAGEMENT IN PERSPECTIVE

- Firms should put in place an information security management policy before putting controls in place
- The policy can be based on an identification of threats and risks or on guidelines provided by governments and industry associations
- Firms implement a combination of technical, formal, and informal controls expected to offer the desired level of security within cost parameters and in accordance with other considerations that enable the firm and its systems to function effectively

BUSINESS CONTINUITY MANAGEMENT (BCM)

- The key element in BCM is a **contingency plan**, formally detailing the actions to be taken in the event that there is a disruption, or threat of disruption, in any part of the firm's computing operation
- Rather using a single, large contingency plan, a firm's best approach is to develop several sub-plans that address specific contingencies. Such as:
    - An emergency plan
    - A backup plan
    - A vital records plan

PUTTING BUSINESS CONTINUITY MANAGEMENT IN PERSPECTIVE

- Much effort has gone into contingency planning and much information and assistance is available
- Some firms use packaged plans they can adapt to their needs
- TAMP Computer Systems markets a Disaster Recovery System (DRS) that includes a database management system, instructions and tools that can be used in preparing a recovery plan
- There are also guidelines and outlines that firms can use as starting points or benchmarks to achieve

END OF CHAPTER 9