MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

TY Btech CSE (CSF) Semester (AY 2024-2025)

Computer Science and Engineering

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

CET4032B: Security Management and Cyber Laws

Examination Scheme:

Continuous Assessment: 60 Marks End Semester Examination: 40 Credit: 3+1 =4

Course Objectives:

1.Knowledge (i) To understand the basics of security management.

(ii) To introduce security management models.

2. Skills (i) To understand the importance of security planning and contingencies.

(ii) To learn about the legal frameworks.

3.Attitude (i) To explore critical understanding of cyber law for Cyber-crimes.

Course Outcomes:

After completion of this course students will be able to:

1. Describe and identify security policy framework, legal and moral implication and best practices in security management
2. Describe the need for and development of information security policies, and identify guidelines and models for writing policies
3. Design detailed enterprise wide security auditing plans and processes
4. Demonstrate a critical understanding of the Cyber law with respect to Indian IT/Act 2008

Pre-requisites

- Software Engineering
- Information and Cyber Security

Syllabus

Unit: I	**Introduction to Security Management** Basics of Security, Principles of Information Security Management, Need for Security: Threats, Attacks. Planning for Security, The role of Planning, Information Security Governance. Information Security Policy, Standards, and Practices, Planning for Information Security Implementation, Types of Information Security Policy, Guidelines for Effective Policy, Information Security Roles and Titles. Security Education, Training, and Awareness Program.	**9 Hrs**
Unit: II	**Security Management Model** Blueprints, Framework and Security Models, Access Control Models, Security Architecture Models, Security Management Models- ISO 270000 Series, NIST Security Models, SP 800-53A, COBIT, COSO, IT Infrastructure Library, Information Security Governance Framework.	**9 Hrs**
Unit: III	**Implementing Security Management** Information Security Project Management, Benchmarking, Performance Measure in Information Security Management-InfoSec Performance Measure: Management, Metrics, Building, Collecting, Implementing, Reporting, Emerging Trends in Certification and Accreditation - SP 800-37, SP 800-53, Security Management Practices and Auditing.	**9 Hrs**

Syllabus (Continue)

Unit: IV	**Legal Framework and Cyber Law** Introduction, Cybercrime and the Legal Landscape around the World, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Digital Signatures and the Indian IT Act, Amendments to the Indian IT Act.	**9 Hrs**
Unit: V	**Cyber law for Cybercrime** Need for Cyber Law, Cyber Jurisprudence at International and Indian Level, Cybercrime and Punishment, Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State, Hacking, Digital Forgery, Case studies.	**9 Hrs**
Books:- (Text)	1. Principles of Information Security, Michael E. Whitman, Herbert J. Mattord 2. Cyber Security, understanding cybercrimes, computer forensics and legal perspectives by Nina Godbole, and Sunit Belapure, WILEY Publication (2011), ISBN: 9788126521791.	
Books:- (Reference)	1. Sennewald, C., and Baillie, C. (2011). Effective Security Management. Elsevier Publication. 2. Handbook of Information Security Management, Micki Krause, Harold F. Tipton, Isc2 Press. 3. Information Security Policies, Procedures, and Standards - A Practitioner's Reference by Douglas Landoll. CRC Press, 2016 ISBN: 1482-24589-2 4. Cyber Crime Manual by Bibhas Chatterjee, Lawman Publication	

Guidelines for CCA and LCA

Examination Scheme

Sr. No.	Examination Scheme	Marks
1.	Class Continuous Assessment (CCA)	60
2.	End Term Theory Examination	40

CCA Marks Distribution

Examination	Weightage	Marks
Mid-Term Theory Exam	25 %	15
Tutorial SET A	25 %	15
Tutorial SET B	25 %	15
Active Learning	25 %	15
	Total	60

Unit 1: Introduction to Security Management

Basics of Security, Principles of Information Security Management, Need for Security: Threats, Attacks.

Planning for Security, The role of Planning, Information Security Governance.

Information Security Policy, Standards, and Practices, Planning for Information Security Implementation, Types of Information Security Policy, Guidelines for Effective Policy, Information Security Roles.

Security Education, Training, and Awareness Program.

Security- the quality or state of being secure

- Protection from adversaries—those who would do harm, intentionally or otherwise—is the ultimate objective of security.
- National security, for example, is a multilayered system that protects the power of a state, its assets, its resources, and its people.
- Achieving the appropriate level of security for an organization also requires a multifaceted system.

Multiple layers of security in place to protect its operations:

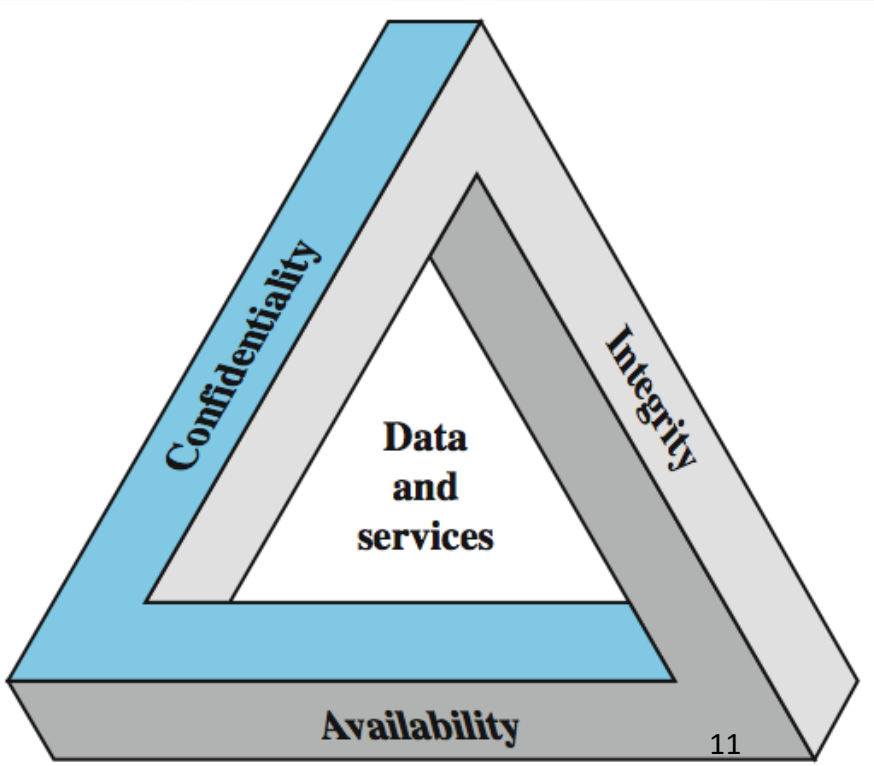
- Physical Security
- Personal Security
- Operations Security
- Communication Security
- Network Security
- Information Security

C.I.A. triangle

- Security A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.
- The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.
- communications security - The protection of all communications media, technology, and content.
- Information security Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.
- Network security A subset of communications security; the protection of voice and data networking components, connections, and content.
- Physical security The protection of physical items, objects, or areas from unauthorized access and misuse.

Critical Characteristics of Information

- Confidentiality, which refers to prevention of unauthorized disclosure of sensitive information and provides access for authorized users only.
- Common threats against confidentiality are:
  - ❑Encryption cracking
  - ❑Malicious insiders
  - ❑Man-in-the-middle attacks



- Integrity prevent unauthorized or contaminating modification of systems & information. And provides authorized actions by authorized users only. It highlights the basic topic of information trustworthiness.
- Challenges that could affect the integrity of your information are:
  - ❑Human error
  - ❑Compromising a server where end to end encryption isn’t present
  - ❑Physical compromise to device

- Availability means we want to prevent disruption or loss of service and associated productivity and that information, with its integrity in tact and its confidentiality are available to authorized users when and where.
- Information unavailability can often occur due to:
  - ❑Distributed Denial of Service attacks (DDOS)
  - ❑Loss of processing ability due to natural disasters and fires
  - ❑Malicious code
  - ❑Insufficient bandwidth

Reflection Spot

An ATM machine

1. **Confidentiality**
2. **Integrity**
3. **Availability**

An ATM machine

1. **Confidentiality-** two-factor authentication
2. **Integrity** - reflection of amount credit/debit must reflect to the account balance
3. **Availability-** available for public use and are accessible at all times.

Principles of Information Security Management

The fundamental principles of information security include:

- Confidentiality
- Privacy
- Quality
- Availability
- Trustworthiness
- Integrity

Need for Security: Threats, Attacks.

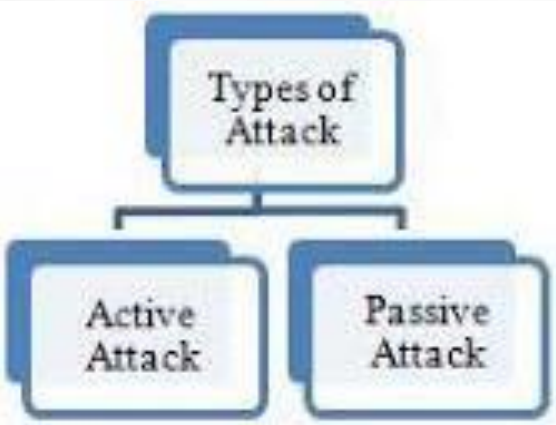
Information security performs four important functions for an organization:

- Protecting the organization’s ability to function
- Protecting the data and information
- Enabling the safe operation of applications running on the organization’s IT systems
- Safeguarding the organization’s technology assets

Key Terms

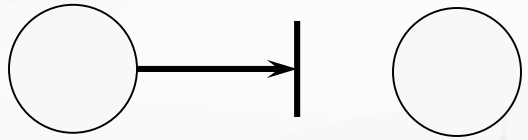
- attack - An ongoing act against an asset that could result in a loss of its value.
- threat - A potential risk of an asset’s loss of value.
- threat agent - A person or other entity that may cause a loss in an asset’s value.
- vulnerability - A potential weakness in an asset or its defensive control system(s).
- exploit - A vulnerability that can be used to cause a loss to an asset.

Security Attacks - Security threats

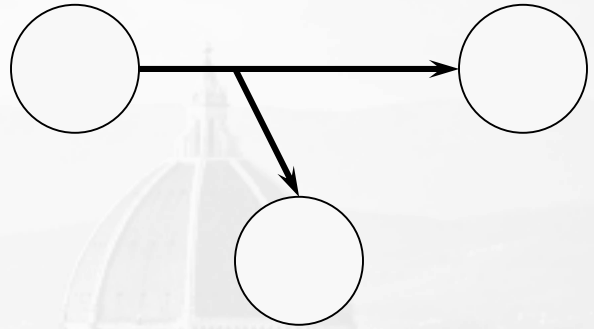


- Interruption – attack on availability
- Interception – attack on confidentiality
- Modification – attack on integrity
- Fabrication – attack on authenticity

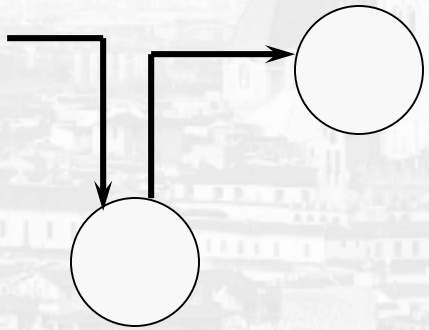
a) Normal flow



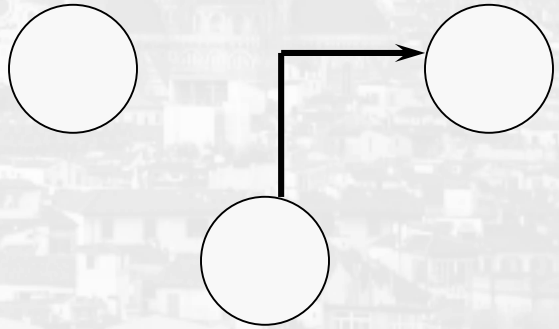
b) Interruption



c) Interception

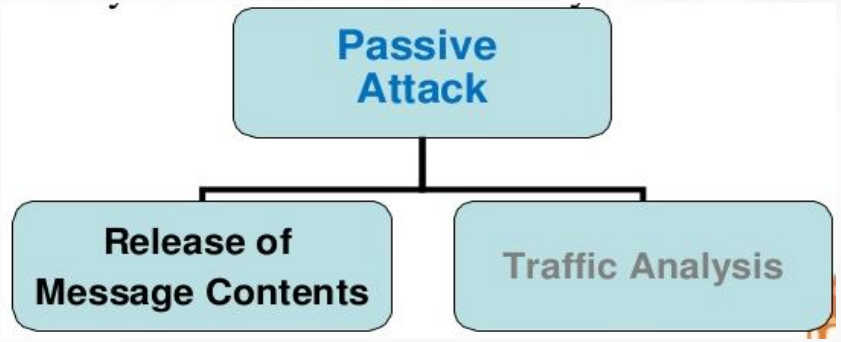


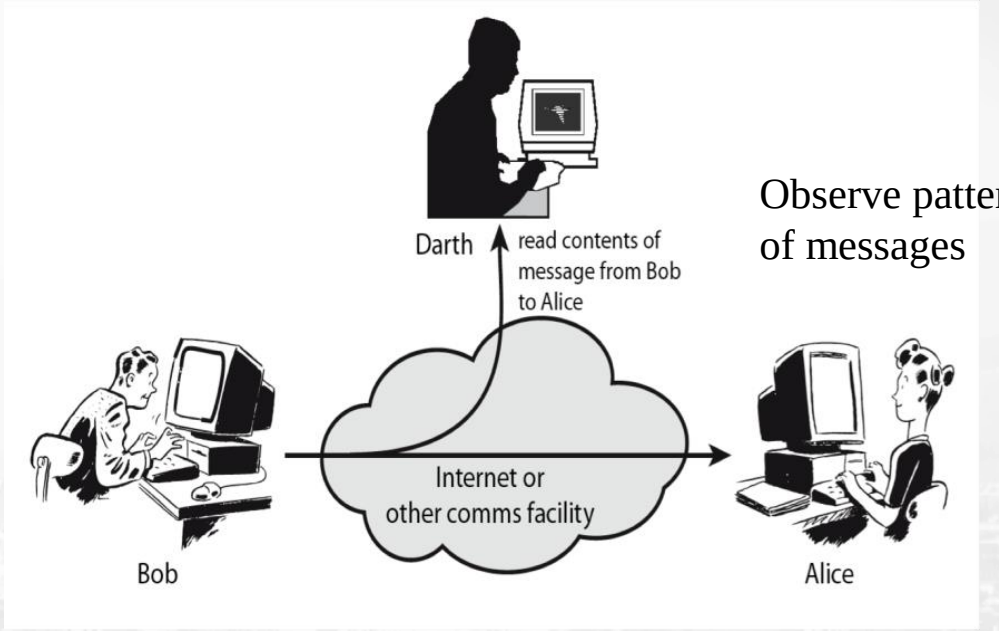
d) Modification



e) Fabrication

- Passive Attack: make use of information from the system but does not affect system resource



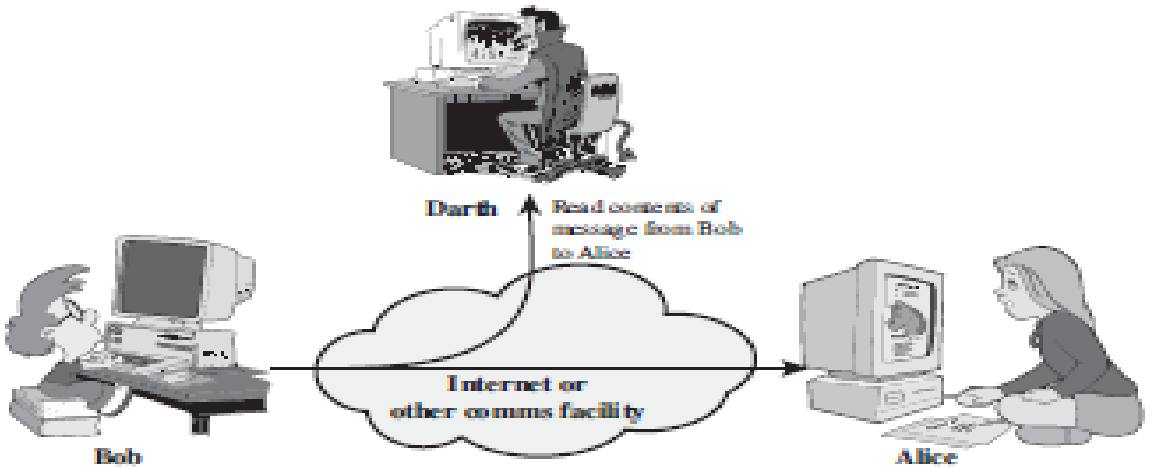


Observe pattern of messages

Note: in dealing with passive attacks is on prevention rather than detection. i.e. encryption

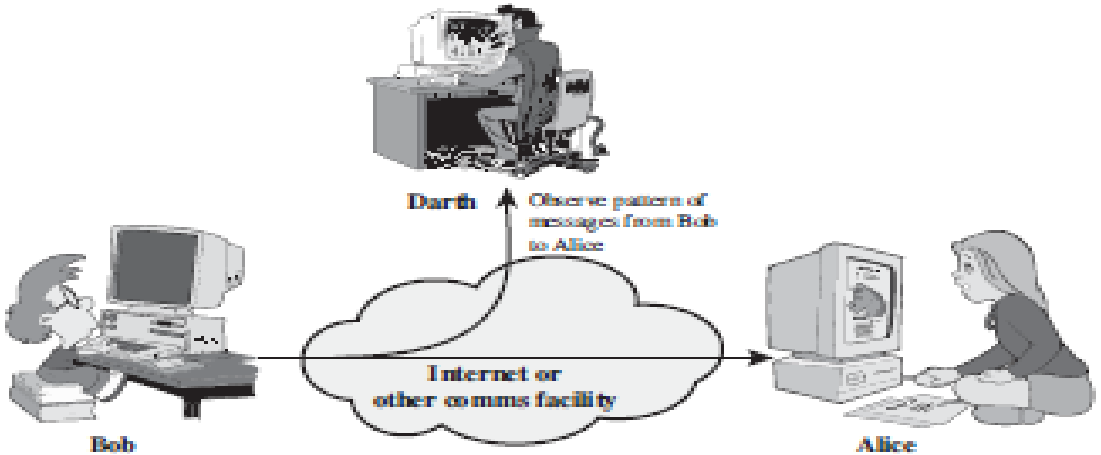
Passive Attacks

- Release of message contents



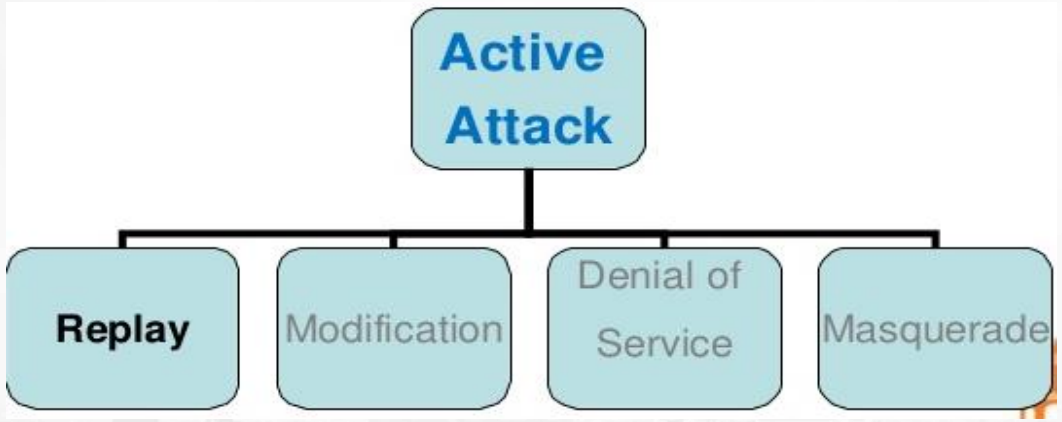
(a) Release of message contents

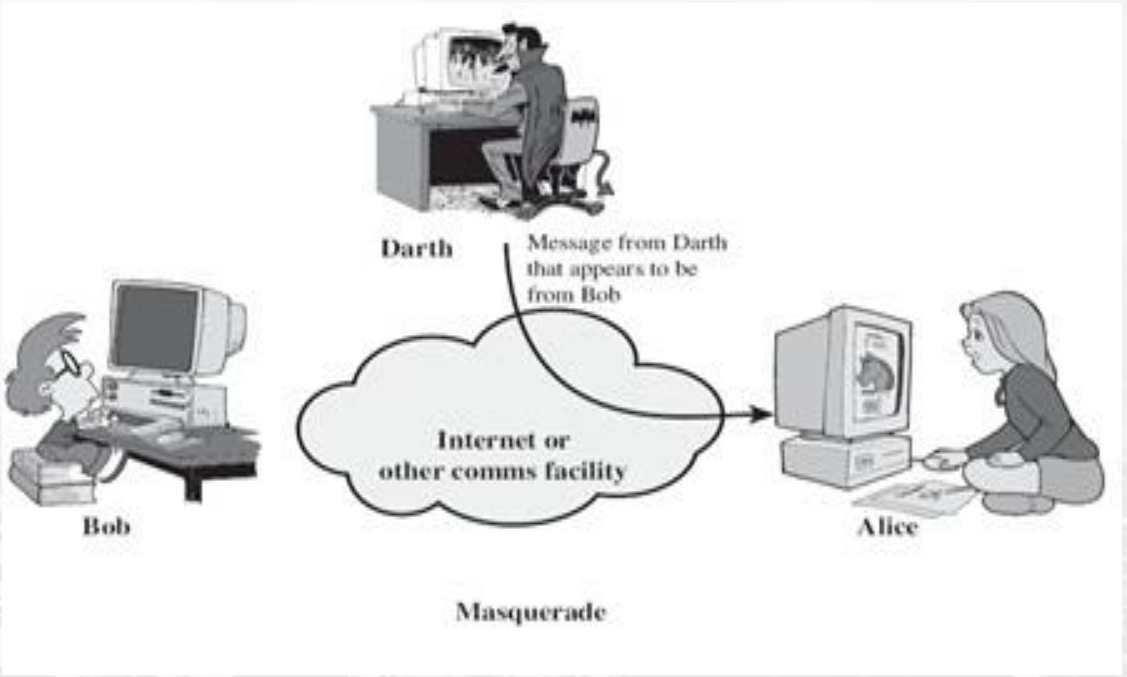
- Traffic analysis



(b) Traffic analysis

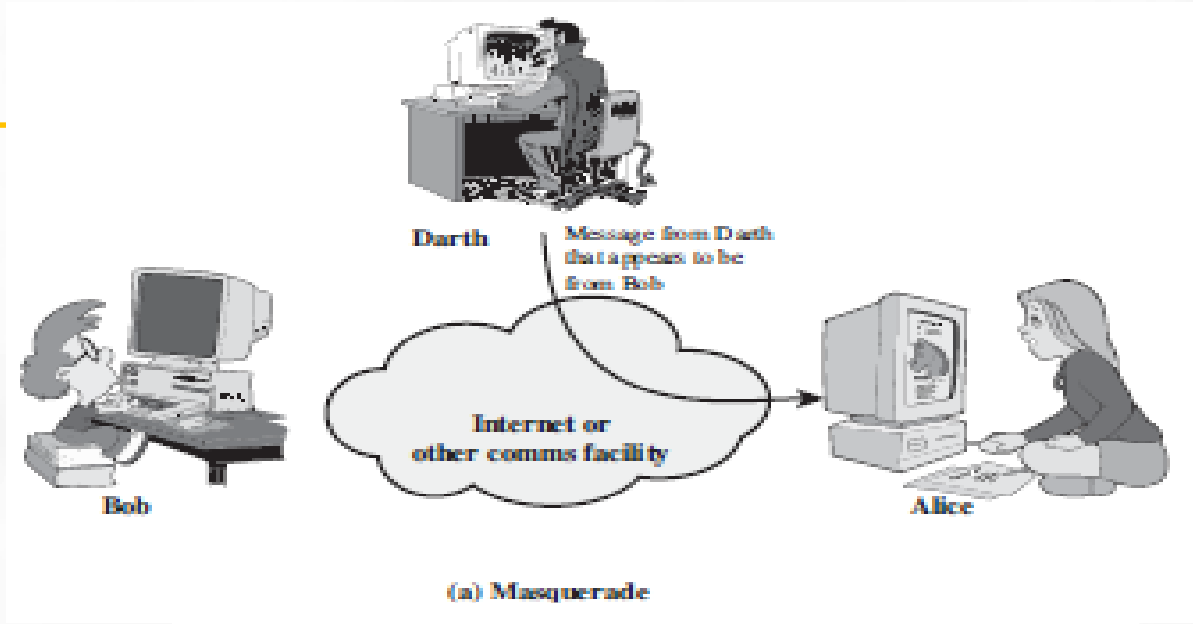
- Active Attack: modification of the data stream or the creation of a false stream





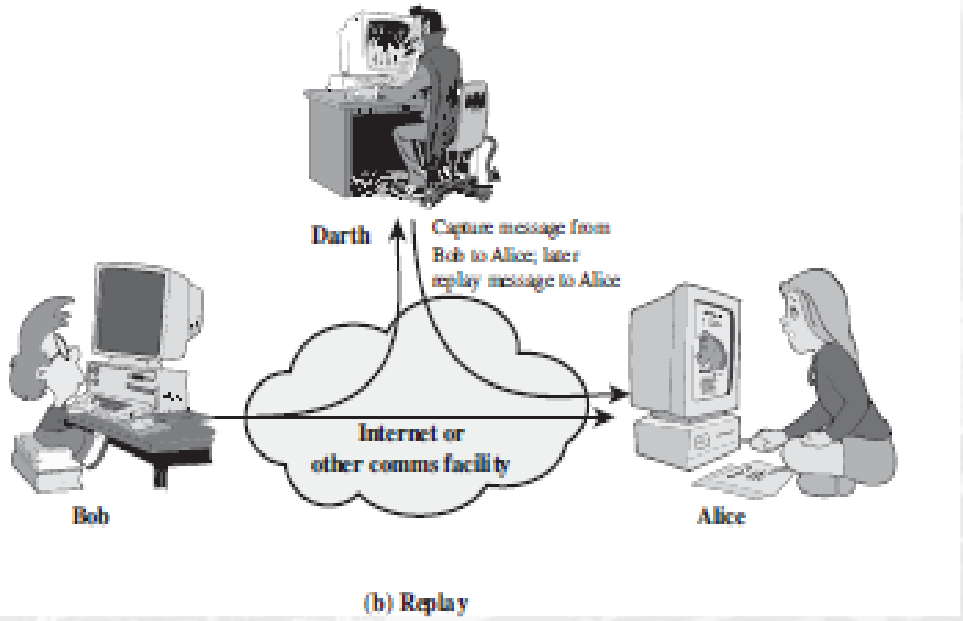
Active Attacks

- Masquerade



(a) Masquerade

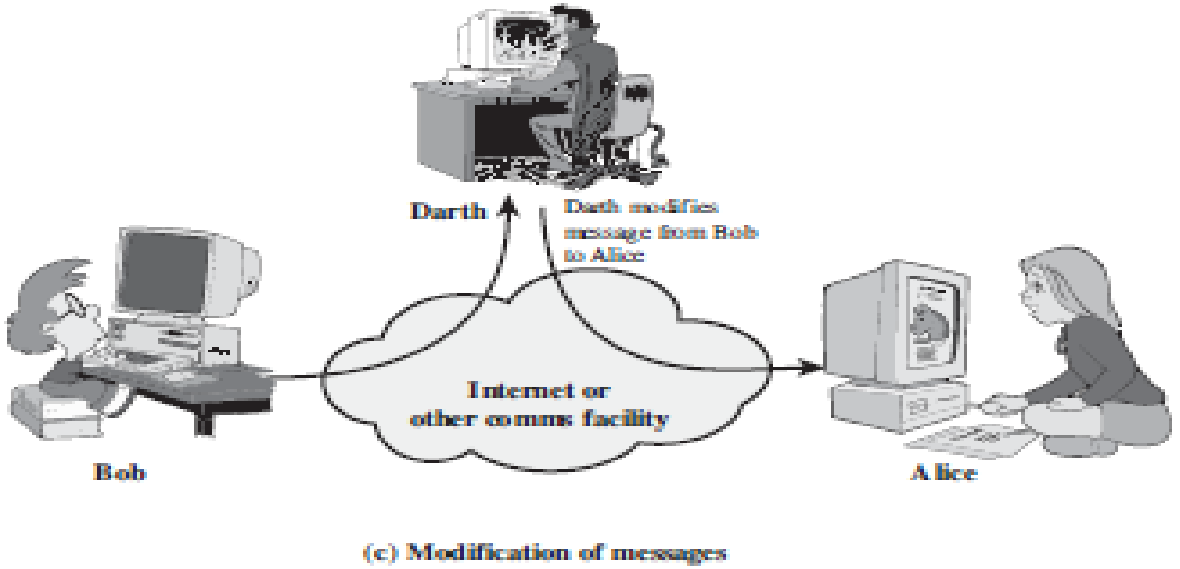
- Replay



(b) Replay

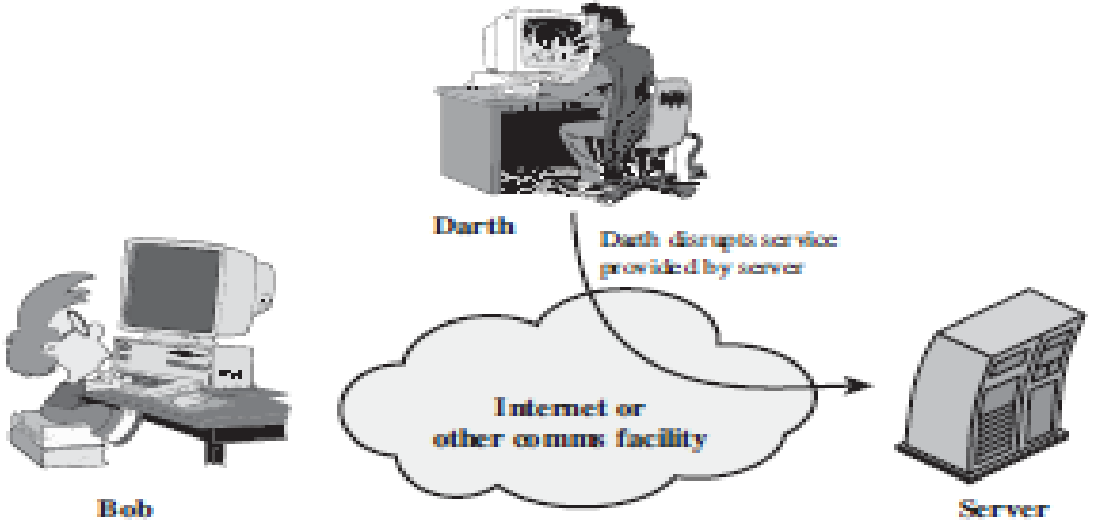
Active Attacks

- Modification of messages



(c) Modification of messages

- Denial of service



(d) Denial of service

Planning for Security

- An organization's information security effort succeeds only when it operates in conjunction with the organization's information security policy. An information security program begins with policy, standards, and practices, which are the foundation for the information security architecture and blueprint. The creation and maintenance of these elements require coordinated planning.
- The role of planning in modern organizations is hard to overemphasize. All but the smallest organizations engage in some planning: strategic planning to manage the allocation of resources and contingency planning to prepare for the uncertainties of the business environment.

Planning Levels

- Operational plan The documented product of operational planning; a plan for the organization's intended operational efforts on a day-to-day basis for the next several months.
- Operational planning The actions taken by management to specify the short-term goals and objectives of the organization in order to obtain specified tactical goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.
- Tactical plan The documented product of tactical planning; a plan for the organization's intended tactical efforts over the next few years.- Management
- Tactical planning The actions taken by management to specify the intermediate goals and objectives of the organization in order to obtain specified strategic goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.
- Strategic plan The documented product of strategic planning; a plan for the organization's intended strategic efforts over the next several years. - Governance
- Strategic planning The actions taken by senior management to specify the long-term goals and objectives of the organization, to plan its future direction, actions, and efforts, and to estimate and schedule the of resources necessary to achieve those goals and objectives.

Planning and the CISO

- The first priority of the CISO and the information security management team is the creation of a strategic plan to accomplish the organization's information security objectives. While each organization may have its own format for the design and distribution of a strategic plan, the fundamental elements of planning share characteristics across all types of enterprises.
- The plan is an evolving statement of how the CISO and various elements of the organization will implement the objectives of the information security charter, which is expressed in the enterprise information security policy (EISP).

Information Security Governance

IT security issues such as data breaches, security policies, and mitigation of security incidents

- Governance describes the entire function of controlling, or governing, the processes used by a group to accomplish some objective.
- It represents the strategic controlling function of an organization's senior management, which is designed to ensure informed, prudent strategic decisions made in the best interest of the organization.
- The governance of information security is a strategic planning responsibility whose importance has grown in recent years. To secure information assets, management must integrate information security practices into the fabric of the organization, expanding corporate governance policies and controls to encompass the objectives of the information security process.
- Information security objectives must be addressed at the highest levels of an organization's management team in order to be effective and sustainable. A broader view of information security encompasses all of an organization's information assets, including the knowledge managed by those IT assets.

Five core components of information security governance

- Provide an organizational structure that constantly works to improve data protection
- Ensure business continuity in case of security breaches or other cybersecurity events.
- Define security measures to assure business needs have the highest priority, and monitor how employees follow those steps.
- Make sure your business stays in compliance with regulatory requirements and other standards.
  - National Institute for Security and Technology (NIST) publication 800-53
  - International Organization for Standardization 27001 (also known as ISO 27001)
  - Control Objectives for Information and Related Technology (COBIT)
  - Health Information Portability and Accountability Act (HIPAA)
  - Payment Card Industry Data Security Standard (PCI DSS)
- Protect and communicate your information security standards both internally to staff and externally to potential business partners.

Information Security Roles

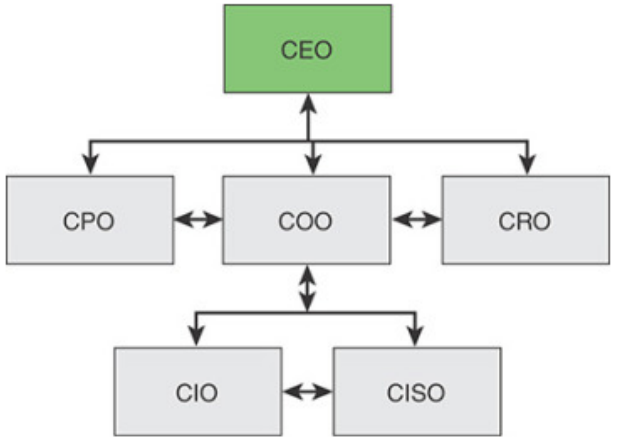


FIGURE 2.5 Possible Reporting Relationships for Security Governance

- **Chief executive officer (CEO):** Responsible for the success or failure of the organization, overseeing the entire operation at a high level.
- **Chief operating officer (COO):** Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies that govern operations.
- **Chief information officer (CIO):** In charge of IT strategy and the computer, network, and third-party (for example, cloud) systems required to support the enterprise's objectives and goals.
- **Chief security officer (CSO)** or **chief information security officer (CISO):** Tasked with ensuring data and systems security. In some larger enterprises, the two roles are separate, with a CSO responsible for physical security and a CISO in charge of digital security.
- **Chief risk officer (CRO):** Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings. This role does not exist in most enterprises. It is most often found in financial service organizations. In enterprises in which a CRO is not present, organizational risk decisions may be the responsibility of the CEO or board of directors.
- **Chief privacy officer (CPO):** Charged with developing and implementing policies designed to protect employee and customer data from unauthorized access.

Information Security Governance Outcomes

The five goals of information security governance are:

1. Strategic alignment of information security with business strategy to support organizational objectives.

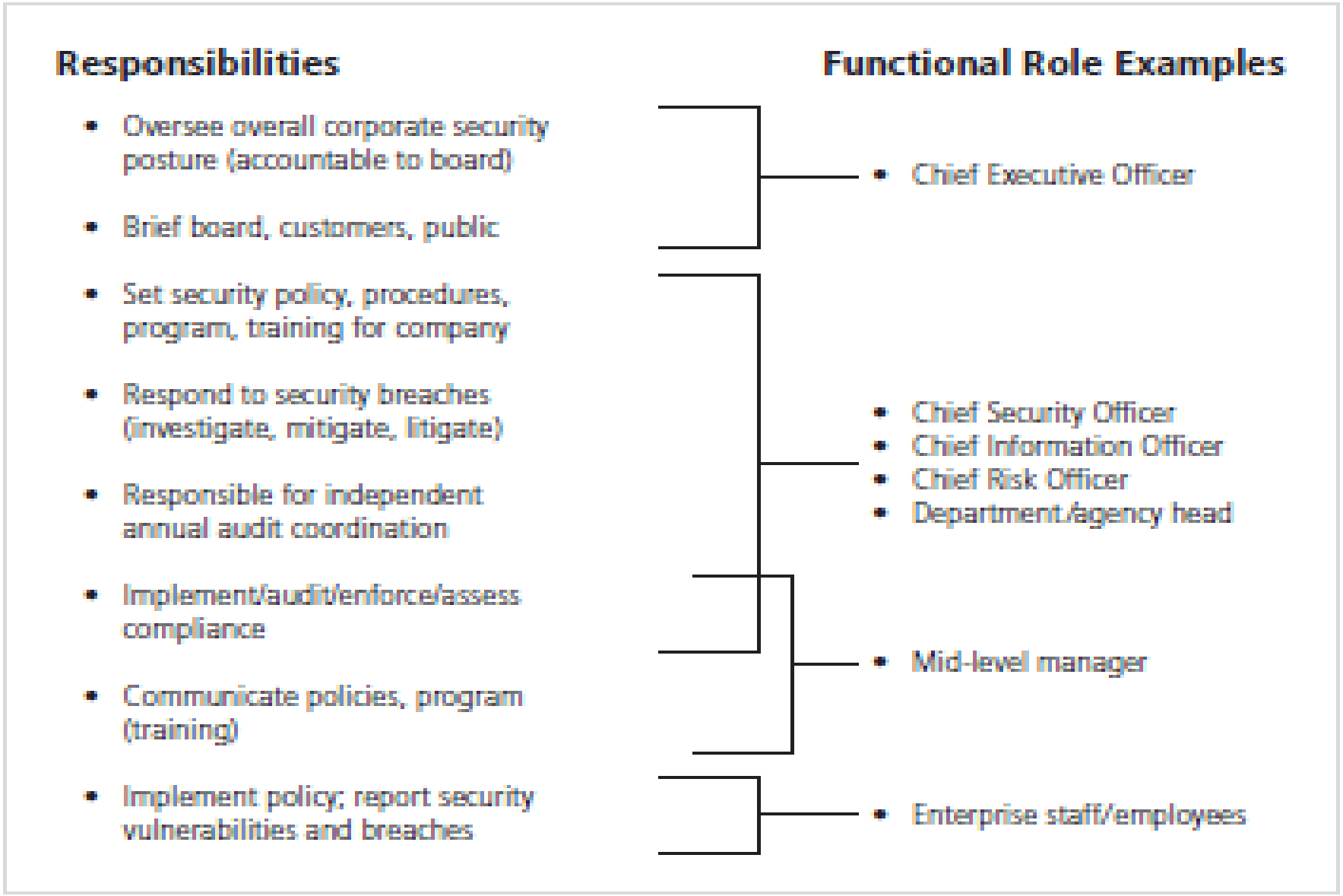
2. Risk management by executing appropriate measures to manage and mitigate threats to information resources.

3. Resource management by using information security knowledge and infrastructure efficiently and effectively

4. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved

5. Value delivery by optimizing information security investments in support of organizational objectives.

Information security governance roles and responsibilities



Information Security Policy

- Information security policy A set of rules that protects an organization's information assets.
- Policy A set of principles or courses of action from an organization's senior management intended to guide decisions, actions, and duties of constituents.
- Practices Within the context of information security, regular actions that an organization identifies as ideal and seeks to emulate. These actions are typically employed by other organizations.
- Procedures Within the context of information security, a set of steps an organization's stakeholders must follow to perform a specified action or accomplish a defined task.
- Standard The normal, targeted, or desired level to which a behavior or action must be performed.
- Guidelines Within the context of information security, a set of recommended actions to assist an organizational stakeholder in complying with policy.

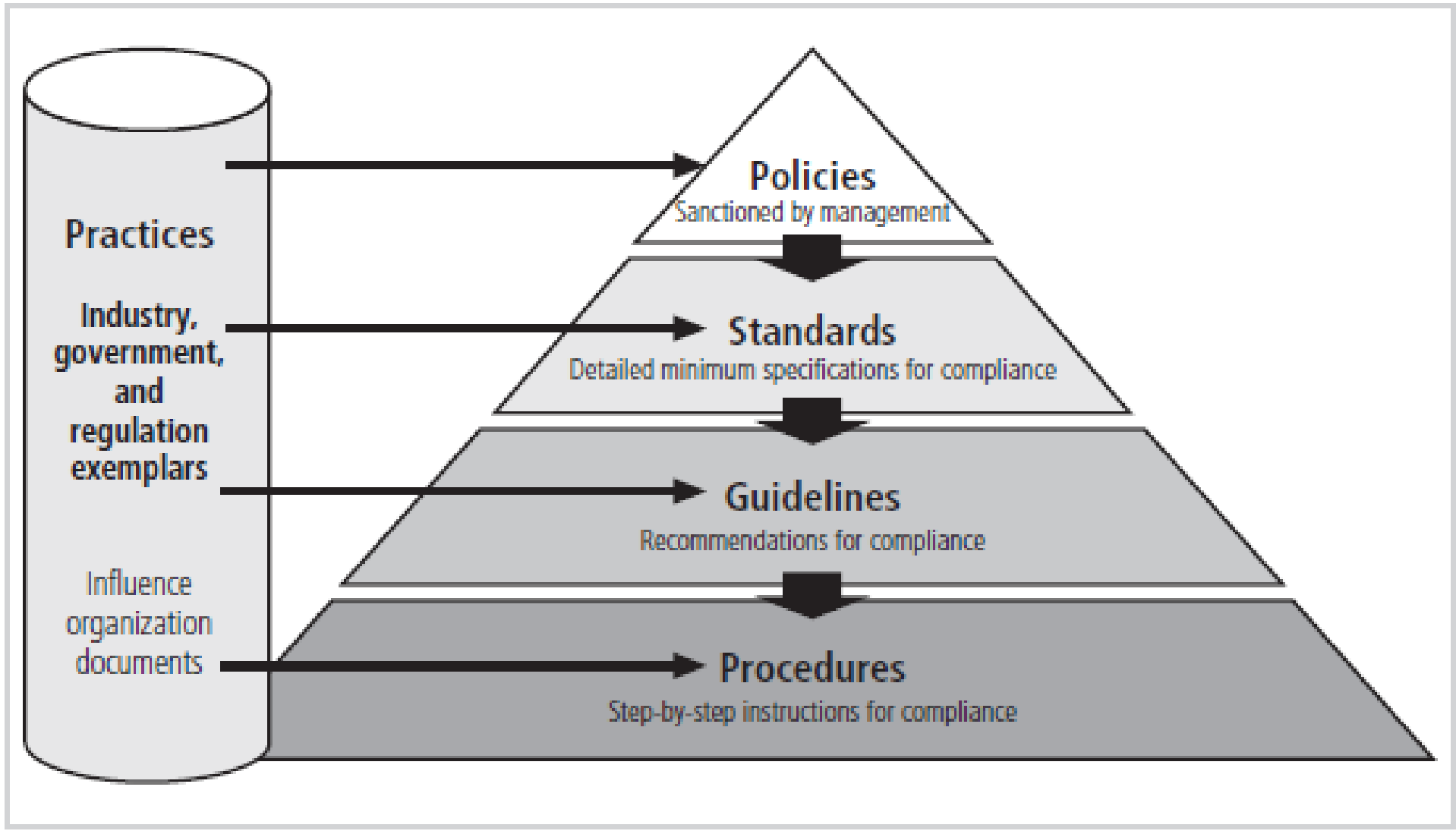


Figure 4-2 Policies, standards, guidelines, and procedures

Policies, Practices, Standards, Guidelines, and Procedures

The relationships among these terms, even when carefully defined, sometimes confuse the reader. The following examples are provided for assistance. Note that many organizations may use the terms differently and publish documents they identify as policy, which may be a combination of what this text defines as policy, standards, or procedures.

The initial statement of intent is the policy.

Policy: Employees must use strong passwords on their accounts. Passwords must be changed regularly and protected against disclosure.

The standard provides specifics to help employees comply with the policy.

Standard: Passwords must be at least 10 characters long and incorporate at least one lowercase letter, one uppercase letter, one numerical digit (0–9), and one special character permitted by our system (&%$#@!). Passwords must be changed every 90 days, and must not be written down or stored on insecure media.

The practice identifies other reputable organizations and agencies that offer recommendations the organization may have adopted or adapted.

Practice: US-CERT recommends the following:

- *Use a minimum password length of 15 characters for administrator accounts.*
- *Require the use of alphanumeric passwords and symbols.*
- *Enable password history limits to prevent the reuse of previous passwords.*
- *Prevent the use of personal information as passwords, such as phone numbers and dates of birth.*
- *Use a minimum password length of 8 characters for standard users.*
- *Disable local machine credential caching if not required through the use of a Group Policy Object (GPO).*
- *Deploy a secure password storage policy that provides password encryption.*[6]

Guidelines provide examples and recommendations to assist users in complying with the new policy.

Finally, procedures are step-by-step instructions for accomplishing the task specified in the policy.

Procedures: To change your log-in password on our system, perform the following steps:

1) *Log in using your current (old) password.*
2) *On your organizational portal home page, click the [Tools] Menu option.*
3) *Select [Change Password].*
4) *Enter your old password in the first field and your new password in the second. The system will ask you to confirm your new password to prevent you from mistyping it.*
5) *The system will then report that your password has been updated, and ask you to log out and log back in with your new password.*

Do not write your new password down. If you own a smartphone, you may request that your department purchase an approved password management application like eWallet for storing passwords.

As stated earlier, many organizations combine their policy and standards in the same document, and then provide directions or a Web link to a page with guidelines and procedures.

Tutorial 1 (non- Graded)

MITWPU Third year CSF students must complete the elective course selection between 9.00am to 6.00pm

Policy

- Policies are the least expensive means of control and often the most difficult to implement.
- Basic rules for shaping policy:
  - Policy should never conflict with law
  - Policy must be able to stand up in court if challenged
  - Policy must be properly supported and administered.
- Why Policy:
  - For internal audit
  - For the resolution of legal disputes about management's due diligence
  - Policy document can act as a clear statement of managements intent.

Management must define three types of security policy, according to Special Publication (SP) 800-14 of the National Institute of Standards and Technology (NIST):

1. Enterprise information security policies
2. Issue-specific security policies
3. Systems-specific security policies

Enterprise information security policies

The high-level security policy that is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.

- Responsibilities for security that are shared by all members of the organization.
- Responsibilities for security that are unique to each role within the organization.

EISP typically addresses compliance in two areas:

1. General compliance to ensure that an organization meets the requirements for establishing a program and assigning responsibilities therein to various organizational components
2. The use of specified penalties and disciplinary action

Components of EISP

Component	Description
Statement of Purpose	Answers the question "What is this policy for?" Provides a framework that helps the reader understand the intent of the document. Can include text such as the following: "This document will: • Identify the elements of a good security policy • Explain the need for information security • Specify the various categories of information security • Identify the information security responsibilities and roles • Identify appropriate levels of security through standards and guidelines This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs."[8]
Information Security Elements	Defines information security. For example: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology …" This section can also lay out security definitions or philosophies to clarify the policy.
Need for Information Security	Provides information on the importance of information security in the organization and the legal and ethical obligation to protect critical information about customers, employees, and markets.
Information Security Responsibilities and Roles	Defines the organizational structure designed to support information security within the organization. Identifies categories of people with responsibility for information security (IT department, management, users) and those responsibilities, including maintenance of this document.
Reference to Other Information Standards and Guidelines	Lists other standards that influence this policy document and are influenced by it, perhaps including relevant federal laws, state laws, and other policies.

Issue-specific security policies

- Commonly referred to as a fair and responsible use policy; a policy designed to control constituents' use of a particular resource, asset, or activity, and provided to support the organization's goals and objectives.
- Provides detailed, targeted guidance.
  - Instruct the organization in secure use of a technology systems.
  - Begins with introduction to fundament technological philosophy of the organization
- Protect organization from inefficiency and ambiguity
  - Documents how the technology-based system is controlled.
  - Identifies the processes and authorities that provide this control.

Components of ISSP

Components of an ISSP
1. Statement of policy a. Scope and applicability b. Definition of technology addressed c. Responsibilities
2. Authorized access and usage of equipment a. User access b. Fair and responsible use c. Protection of privacy
3. Prohibited use of equipment a. Disruptive use or misuse b. Criminal use c. Offensive or harassing materials d. Copyrighted, licensed, or other intellectual property e. Other restrictions
4. Systems management a. Management of stored materials b. Employee monitoring c. Virus protection d. Physical security e. Encryption
5. Violations of policy a. Procedures for reporting violations b. Penalties for violations
6. Policy review and modification a. Scheduled review of policy procedures for modification b. Legal disclaimers
7. Limitations of liability a. Statements of liability b. Other disclaimers as needed

ISSP examples

- Email and internet use
- Minimum system configurations
- Prohibitions against hacking
- Home use of company-owned computer equipment
- Use of personal equipment on company networks.
- Use of telecommunications technologies

Systems-specific security policies

- A systems-specific security policy that expresses technical details for the acquisition, implementation, configuration, and management of a particular technology, written from a technical perspective.
- Typically the policy includes details on configuration rules, systems policies, and access control.
- SysSP can be separated into
  - Management guidance
  - Technical specifications

Management guidance

- Created by management to guide the implementation and configuration of technology
- Applies to any technology that affects the CIA of information.

Technical specifications

- System administrators direction on implementing managerial policy
- Each type of equipment has its own type of policies.
- General methods of implementing technical controls.
  - Access control lists
  - Configuration rules.

Guidelines for Effective Policy

A policy must meet the following criteria to be effective and thus legally enforceable:

- Dissemination (distribution): The organization must be able to demonstrate that the policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
- Review (reading): The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for employees who are illiterate, reading-impaired, and unable to read English. Common techniques include recording the policy in English and other languages.
- Comprehension (understanding): The organization must be able to demonstrate that the employee understands the requirements and content of the policy. Common techniques include quizzes and other assessments.
- Compliance (agreement): The organization must be able to demonstrate that the employee agrees to comply with the policy through act or affirmation. Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
- Uniform enforcement: The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Fair and Responsible Use of Wireless LAN Technology

Issue Specific Security Policy

Title: Fair and Responsible Use of Wireless LAN Technology
Classification: Internal Use Only

Statement of Policy
This policy addresses fair and responsible use of Acme's wireless local area network (WLAN) technologies. This includes but is not limited to hardware, software and protocols associated with WLANs. It is intended for authorized users within the Acme enterprise. Authorized users are defined as anyone who has been granted approval to access Acme information and information systems. This includes employees and contingent workers. Authorized users are expected to understand and comply with the contents of this document.

Appropriate Use
Laptop users are permitted, with prior management approval, to use Acme's internal WLAN solution. The WLAN should be used only when a wired network solution in unavailable or inappropriate for a particular situation. To ensure appropriate protection of privacy, all wireless transmissions will be secured utilizing strong mutual authentication and encryption. When establishing a connection to a public hotspot or WLAN within your home, a VPN connection must be established and used in conjunction with an Acme approved personal firewall solution. Only Acme approved WLAN technologies are permitted within the enterprise. Use of non-standard hardware, software and protocols is strictly prohibited.

Systems Management
It is the responsibility of the Network Administrator, for Acme's WLAN, to ensure all Access Points are configured with proper settings as defined by the WLAN System-Specific Policy. This includes but is not limited to authentication and encryption configurations. It is the responsibility of the end-user to ensure that his/her laptop remains properly configured as defined by Enterprise Workstation Standards. This includes but is not limited to the configuration of the wireless supplicant and network interface card. Acme Information Security will be responsible for defining authentication and encryption requirements as well as development of necessary compliance programs. Acme reserves the right to audit any and all technologies associated with its WLAN.

Violations of Policy
In the event of inappropriate use of WLAN technologies, Acme reserves the right to take whatever steps are deemed appropriate for the specific situation including, but not limited to, termination of employment and/or legal action. Guidelines for action include a warning for first-time violators and formal notice in employee's personnel file for additional occurrences. All violations of this policy should be reported to your direct report manager who will in turn report the violation to the Information Security department.

Policy Review and Modification
This policy will be reviewed by Acme Information Security on an annual basis, or as necessitated by changes in technology, and modified where appropriate.

Limitations of Liability
Acme assumes no liability for unauthorized acts that violate local, state or federal legislation. In the event that such an act occurs, Acme will immediately terminate its relationship with the violator and will provide no legal protection or assistance.

Tutorial 2
Secure Use of Personal Digital Devices Policy

Developing Information Security Policy

- It is often useful to view policy development as a two-part project.
  - First, design and develop the policy (or redesign and rewrite an outdated policy)
  - Second, establish management processes to continue the policy within the organization.
- Policy development projects should be
  - Well planned
  - Properly funded
  - Aggressively managed to ensure that it is completed on time and within budget
- The policy development project can be guided by SecSDLC process.
- Investigation phase
  - Obtain support from senior management and active involvement of IT management specifically the CIO
  - Clearly articulate the goals of the policy project
  - Gain participation of correct individuals affects by the recommended policies.
  - Involve legal, human resources and end users
  - Assign a project champion with sufficient prestige
  - Acquire a capable project manager
  - Develop a detailed outline of and sound estimates for project cost and scheduling.

Figure 4-8 End user license agreement for Microsoft Windows XP

- Analysis phase should produce
  - New or recent risk assessment or IT audit documenting the current information security needs of the organization.
- Design Phase includes
  - How the policies will be distributed
  - How verification of the distribution will be accomplished
  - Specifications for any automated tools
  - Revisions to feasibility analysis reports based on improved costs and benefits as the design is clarified
- Implementation phase includes
  - Writing the policies
    - Making certain the policies are enforceable as written
    - Policy distribution is not always straightforward
    - Effective policy is written at a reasonable reading level and attempts to minimize technical jargon and management terminology.
- Maintenance Phase
  - Maintain and modify the policy as needed to ensure that it remains effective as a tool to meet changing threats.
  - The policy should have a built-in mechanism via which users can report problems with the topic
  - Periodic review should be built into the process.

- The only reason to have policies is to avoid litigation, it is important to emphasize the preventative nature of policy.
  - Policies exist, first and foremost, to inform employees of what is and is not acceptable behavior in the organization.
  - Policy seeks to improve employee productivity and present potentially embarrassing situation.

Security Education, Training and Awareness Program

- SETA
  - Security education, training and awareness
- A managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for organizations.
- It is a control measure designed to reduce accidental security breaches.
- The SETA program is generally the responsibility of the governance and Privacy Dept.
- Purpose
  - Improve awareness of need to protect
  - Develop skills and knowledge
  - Build in-depth knowledge to design, implement, or operate security programs

- Security Education: Everyone in an organization needs to be trained and made aware of information security, but not everyone needs a formal degree or certificate in information security. When management agrees that formal education is appropriate, an employee can investigate courses in continuing education from local institutions of higher learning.

  – College or University
  – Certification
  – Conceptual

- Security Training: Security training provides employees with detailed information and hands-on instruction to prepare them to perform their duties securely. Management of information security can develop customized in-house training or outsource the training program.
  - Practical
  - Applies to each operating environment
  - Include:
    - Acceptable use
    - Standards
    - Procedures
    - Policy Compliance
    - Guidelines
- To all managers, IT design and security, IT Team and security

- Security Awareness: A security awareness program is one of the least frequently implemented but most beneficial programs in an organization. A security awareness program is designed to keep information security at the forefront of users' minds.
  - Focus and attention to specific issue:
    - Phishing
    - Password sharing
    - Social engineering
    - Information sharing

Comparative Framework of SETA

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction •Discussion seminar •Background reading •Hands-on practice	Practical instruction •Lecture •Case study •Posters	Media •Videos •Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	True or false Multiple choice (identify learning)
Impact timeframe	Long-term	Intermediate	Short-term

Topics

- Locking Devices
- Password Reuse
- Multi-Factor
- Clean Desk
- Browser Security
- Social Engineering
- Ransomware
- Vishing

Tutorial 3

Search the web for security education and training program. Keep a list and see which category has the most examples. See if you can determine the cost associated with each example. Which do you think would be more cost-effective in terms of both time and money?