Module 2: Security Policies

CSC3207 Computer Security

Outline

- Computer Security Strategy
- Security Policies
  - types
  - components
  - importance
- Policies, Standards, Procedures, Guidelines, and Practices

References

- Chapter 9 Security Engineering: A Guide to Building Dependable Systems, 3rd Edition by Ross Anderson
- Chapter 4 Introduction to Computer Security by Matt Bishop
- Chapter 4: Management of Information Security, Sixth Edition, by Michael E. Whitman and Herbert J. Mattord

Computer Security Strategy

- A computer security/cybersecurity strategy is a high-level plan for how your organization, nation will secure its assets during the next three to five years.
- A comprehensive security strategy involves three aspects:
  - **Specification/policy**: What is the security scheme supposed to do?
  - **Implementation/mechanisms**: How does it do it?
  - **Correctness/assurance**: Does it really work?
- A cyber security strategy is not meant to be perfect, but it must be proactive, effective, actively supported and evolving

Assurance and Evaluation

- Consumers of computer security services and mechanisms (system managers, vendors, customers, and end users) desire a belief that the security measures in place work as intended.
- **Assurance** is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. This encompasses both system design and system implementation.

  - Assurance deals with the questions, "Does the security system design meet its requirements?" and "Does the security system implementation meet its specifications?"
- Evaluation is the process of examining a computer product or system with respect to certain criteria.
- Evaluation involves testing and may also involve formal analytic or mathematical techniques.

Security Implementation

- Security implementation involves 4 complementary courses of action:
  - Prevention
  - Detection
  - Response
  - Recovery
- Prevention of attacks eg. in the transmission of encrypted data. If a secure encryption algorithm is used, and if measures are in place to prevent unauthorized access to encryption keys, then attacks on confidentiality of the transmitted data will be prevented.
- Detection: absolute protection is not feasible, but it is practical to detect security attacks. For example, there are intrusion detection systems designed to detect the presence of unauthorized individuals logged onto a system.

Security Implementation

- Response: If security mechanisms detect an ongoing attack, such as a denial of service attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.
- Recovery: eg the use of backup systems, so that if data integrity is compromised, a prior, correct copy of the data can be reloaded.

Security Policies

- The first step in devising security services and mechanisms is to develop a security policy.
- A security policy is a a document that states in writing rules and practices that specify or regulate how an organization provides security services to protect sensitive and critical system resources both physical and information technology (IT) assets.
- Information security policies are high-level documents that outline an organization's stance on security issues.
- They are typically supported by senior executives and are intended to provide a security framework that guides managers and employees throughout the organization.

Security Policies

- Information security policies rarely mandate specific security technologies and approaches, but they do define the organization's goals, requirements, and responsibilities concerning information security.
- Security policies are living documents that are continuously updated and changing as technologies, vulnerabilities and security requirements change.
- For example, a security policy might mandate that
  - data on company-owned laptops is encrypted
  - employees must not share data using unencrypted services
  - team leaders are responsible for ensuring people under their supervision follow these encryption best practices.
- High-level policies do not usually explain which encryption algorithms should be used or how encryption should be implemented.

Security Policies

- A security policy is a succinct description of what we are trying to achieve, the protection properties that a system must have and what the protection mechanisms are to achieve
- It is the document in which the protection goals of the system are agreed with an entire community, or with the top management of a customer
- A security policy defines "secure" for a system or a set of systems
- It is driven by our understanding of threats, the bad outcomes we wish to avoid, and in turn drives our system design and engineering
- Policies require constant modification and maintenance

Security Policy Considerations

In developing a security policy, a security manager needs to consider the following factors:

- The value of the assets being protected
- The vulnerabilities of the system
- Potential threats and the likelihood of attacks

How to Develop a Security Policy

- Identify sensitive information and critical systems
- Incorporate local, state, and federal laws, as well as relevant ethical standards
- Define institutional security goals and objectives
- Set a course for accomplishing those goals and objectives
- Ensure that necessary mechanisms for accomplishing the goals and objectives are in place

Security Policy Trade-offs

In developing a security policy, a security manager must consider the following trade-offs:

- Ease of use versus security: Virtually all security measures involve some penalty in the area of ease of use.
  - Access control mechanisms require users to remember passwords and perhaps perform other access control actions.
  - Firewalls and other network security measures may reduce available transmission capacity or slow response time.
  - Virus-checking software reduces available processing power and introduces the possibility of system crashes or malfunctions due to improper interaction between the security software and the operating system.

Security Policy Trade-offs

- Cost of security versus cost of failure and recovery:In addition to ease of use and performance costs, there are direct monetary costs in implementing and maintaining security measures.
  - All of these costs must be balanced against the cost of security failure and recovery if certain security measures are lacking.
  - The cost of security failure and recovery must take into account the value of the assets being protected, the damages resulting from a security violation, but also the risk, which is the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policies

- Some basic rules must be followed when shaping a security 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

Security Mechanism Vs Policy

- A security mechanism is an entity or procedure that enforces some part of the security policy
- In the example, the policy is the statement that no student may copy another student's homework
- One mechanism is the file access controls
- if the second student had set permissions to prevent the first student from reading the file containing her homework, the first student could not have copied that file.

Security Mechanism Vs Policy

- A company's security policy states that information relating to a particular product is proprietary and is not to leave the control of the company
- The company stores its backup tapes in a vault in the town's bank (just in case the computer installation is completely destroyed)
- The company must ensure that only authorized employees have access to the backup tapes even when the tapes are stored off-site; hence, the bank's controls on access to the vault, and the procedures used to transport the tapes to and from the bank, are considered security mechanisms
- Note that these mechanisms are not technical controls built into the computer
- Procedural, or operational, controls also can be security mechanisms

Types of Security Policies

- Security policies can be categorized according to various criteria.
- One method is to categorize policies by scope:
  - Organizational/Enterprise information security policy
  - System-specific security policies
  - Issue-specific security policies

Types of Security Policies

- **Enterprise information security policy (EISP)** describes the whole organization's security objectives and its commitment to information security.
  - Is high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts
  - An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, organizational security policy, or simply an InfoSec policy - It can be thought of as the primary document from which other security policies are derived.
  - Also, it often informs the organization's compliance goals.
  - The EISP should not contradict the organizational mission statement

Table 4-1 Components of the EISP

Component	Description
Purpose	Answers the question, "What is this policy for?" Provides a framework that helps the reader to understand the intent of the document. Can include text such as the following, which is taken from Washington University in St. Louis: *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.*[5]
Elements	Defines the whole topic of information security within the organization as well as its critical components. For example, the policy may state: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology" and then identify where and how the elements are used. This section can also lay out security definitions or philosophies to clarify the policy.
Need	Justifies the need for the organization to have a program for information security. This is done by providing information on the importance of InfoSec in the organization and the obligation (legal and ethical) to protect critical information, whether regarding customers, employees, or markets.
Roles and responsibilities	Defines the staffing structure designed to support InfoSec within the organization. It will likely describe the placement of the governance elements for InfoSec as well as the categories of individuals with responsibility for InfoSec (IT department, management, users) and their InfoSec responsibilities, including maintenance of this document.
References	Lists other standards that influence and are influenced by this policy document, including relevant federal and state laws and other policies.

Types of Security Policies

- **System-specific security policies** focus on the information security policies of particular systems.
  - For example, policies for customer-facing applications, payroll systems, or data archive systems.
  - They typically articulate security objectives and the operational security rules intended to support them.
- **Issue-specific security policies (ISSP)** provide guidelines for particular threats or categories of threats.
  - For instance, an organization might develop issue-specific policies for email security, phishing attacks, remote access, or data classification.
  - These policies provide clear directives for managing these specific risks, reducing the likelihood of security incidents in these areas

Issue-specific Security Policy (ISSP)

An effective ISSP accomplishes the following:

- It articulates the organization's expectations about how its technology-based system should be used
- It documents how the technology-based system is controlled and identifies the processes and authorities that provide this control
- It indemnifies the organization against liability for an employee's inappropriate or illegal use of the system
- Every organization's ISSP should:
  - Address specific technology-based systems
  - Require frequent updates
  - Contain a statement on the organization's position on an issue

Issue-Specific Policy Topics

- Use of electronic mail, IM, and other communications apps
- Use of the Internet, the Web, and company networks by company equipment
- Malware protection requirements
- Use of non-organizationally issued software or hardware on organization assets
- Use of organizational information on non-organizationally owned computers
- Prohibitions against hacking or testing security controls or attempting to modify or escalate privileges
- Personal and/or home use of company equipment

Issue-Specific Policy Topics

- Removal of organizational equipment from organizational property
- Use of personal equipment on company networks (BYOD)
- Use of personal technology during work hours
- Use of photocopying and scanning equipment
- Requirements for storage and access to company information while outside company facilities
- Specifications for the methods, scheduling, conduct, and testing of data backups
- Requirements for the collection, use, and destruction of information assets
- Storage of access control credentials by users

Examples of Issue-Specific Policies

- Email Security Policy: outlines the procedures and best practices for using email within the organization.
  - It may include guidelines on identifying phishing emails, using encryption, and managing attachments to prevent the spread of malware.
- Remote Access Policy: With the rise of remote work, a remote access policy is essential.
  - This policy would specify how employees can securely access the organization's network from off-site locations.
  - It might cover using virtual private networks (VPNs), multi-factor authentication (MFA), and handling sensitive information while working remotely.
- Data Classification Policy: helps employees understand how to handle different types of data based on their sensitivity.
  - It might define categories such as "Confidential," "Internal Use Only," and "Public," along with corresponding handling procedures for each.

Elements of the Issue-Specific Policy

- Statement of Purpose - Scope and Applicability, Definition of Technology Addressed, Responsibilities
- Authorized Access and Usage of Equipment: User Access, Fair and Responsible Use, Protection of Privacy
- Prohibited Usage of Equipment - Disruptive Use or Misuse, Criminal Use, Offensive or Harassing Materials
  - Copyrighted, Licensed, or Other Intellectual Property
- Systems Management: Management of Stored Materials, Employer Monitoring, Virus Protection, Physical Security, Encryption
- Violations of Policy - Procedures for Reporting Violations, Penalties for Violations
- Policy Review and Modification - Scheduled Review of Policy and Procedures for Modification
- Limitations of Liability - Statements of Liability or Disclaimers

Common approaches to Implementing the ISSP

- A number of independent ISSP documents, each tailored to a specific issue
- A single comprehensive ISSP document that covers all issues
- A modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements
- The recommended approach is the modular policy, which provides a balance between issue orientation and policy management

Table 4-4 ISSP Document Organization Approaches

Approach	Advantages	Disadvantages
Individual Policy	• Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• Typically yields a scattershot result that fails to cover all of the necessary issues • Can suffer from poor policy dissemination, enforcement, and review
Comprehensive Policy	• Well controlled by centrally managed procedures assuring complete topic coverage • Often provides better formal procedures than when policies are individually formulated • Usually identifies processes for dissemination, enforcement, and review	• May overgeneralize the issues and skip over vulnerabilities • May be written by those with less complete subject matter expertise
Modular Policy	• Often considered an optimal balance between the individual ISSP and the comprehensive ISSP approaches • Well controlled by centrally managed procedures, assuring complete topic coverage • Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• May be more expensive than other alternatives • Implementation can be difficult to manage

Types of Security Policies

- Each organization has its own requirements for the levels of confidentiality, integrity, and availability, and the organization's policy states these needs for that particular organization
- A military security policy (a governmental security policy) is a security policy developed primarily to provide confidentiality
- A commercial security policy is a security policy developed primarily to provide integrity e.g in a bank
- A confidentiality policy is a security policy dealing only with confidentiality e.g the Bell-LaPadula Model
- Confidentiality policies emphasize the protection of confidentiality; prevent the unauthorized disclosure of information
- An integrity policy is a security policy dealing only with integrity.

Policies, Standards, Procedures, Guidelines, and Practices

- Policy is a set of organizational guidelines that dictate certain behavior within the organization
  - are high-level statements that define an organization's security objectives, goals, and requirements
  - provide direction on how the organization will achieve its security objectives and what is expected of employees, contractors, and partners
  - Security policies should be aligned with an organization's principles and reflect industry standards and regulations
  - For example, an organization might have a policy that requires employees to use strong passwords that meet specific complexity requirements

Policies, Standards, Procedures, Guidelines, and Practices

- A standard is a detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance
  - are specific, mandatory requirements that outline how security policies will be implemented
  - provide detailed guidance on how to implement policies, what technologies to use, and how to configure them
  - are often technical and reflect industry best practices and regulations
  - For example, an organization might have a standard that requires all devices accessing the network to have the latest security patches installed.

Policies, Standards, Procedures, Guidelines, and Practices

- Guidelines are non-mandatory recommendations the employee may use as a reference in complying with a policy
  - are recommendations or suggestions for best practices that can help achieve an organization's security objectives
  - are less prescriptive than policies and standards and provide general guidance on how to achieve security objectives
  - are often flexible and can be adapted to fit the needs of the organization
  - For example, an organization might have guidelines on how to configure firewalls, including recommended settings and best practices.

Policies, Standards, Procedures, Guidelines, and Practices

- Procedures are step-by-step instructions on how to carry out a specific task or process; designed to assist employees in following policies, standards, and guidelines
  - provide detailed guidance on how to implement standards and policies.
  - are often detailed and reflect specific requirements of the organization.
  - For example, an organization might have a procedure that outlines how to respond to a security incident, including who to contact, what actions to take, and how to document the incident.

Policies, Standards, Procedures, Guidelines, and Practices

- Practices are examples of actions that illustrate compliance with policies
- A Process defines a series of actions taken to achieve a particular end
  - A process is a set of activities that interact to achieve a result.
- Principles are broad statements that outline an organization's overall approach to information security
  - provide guidance on the organization's values, objectives, and goals
  - serve as a foundation for developing security policies and are often aligned with industry standards and regulations
  - For example, the principle of "Least Privilege" states that users should only be given the minimum level of access needed to perform their job functions.
- Policies define what you can do and not do, whereas the other documents focus on the how

Security Policies, Standards and Practices

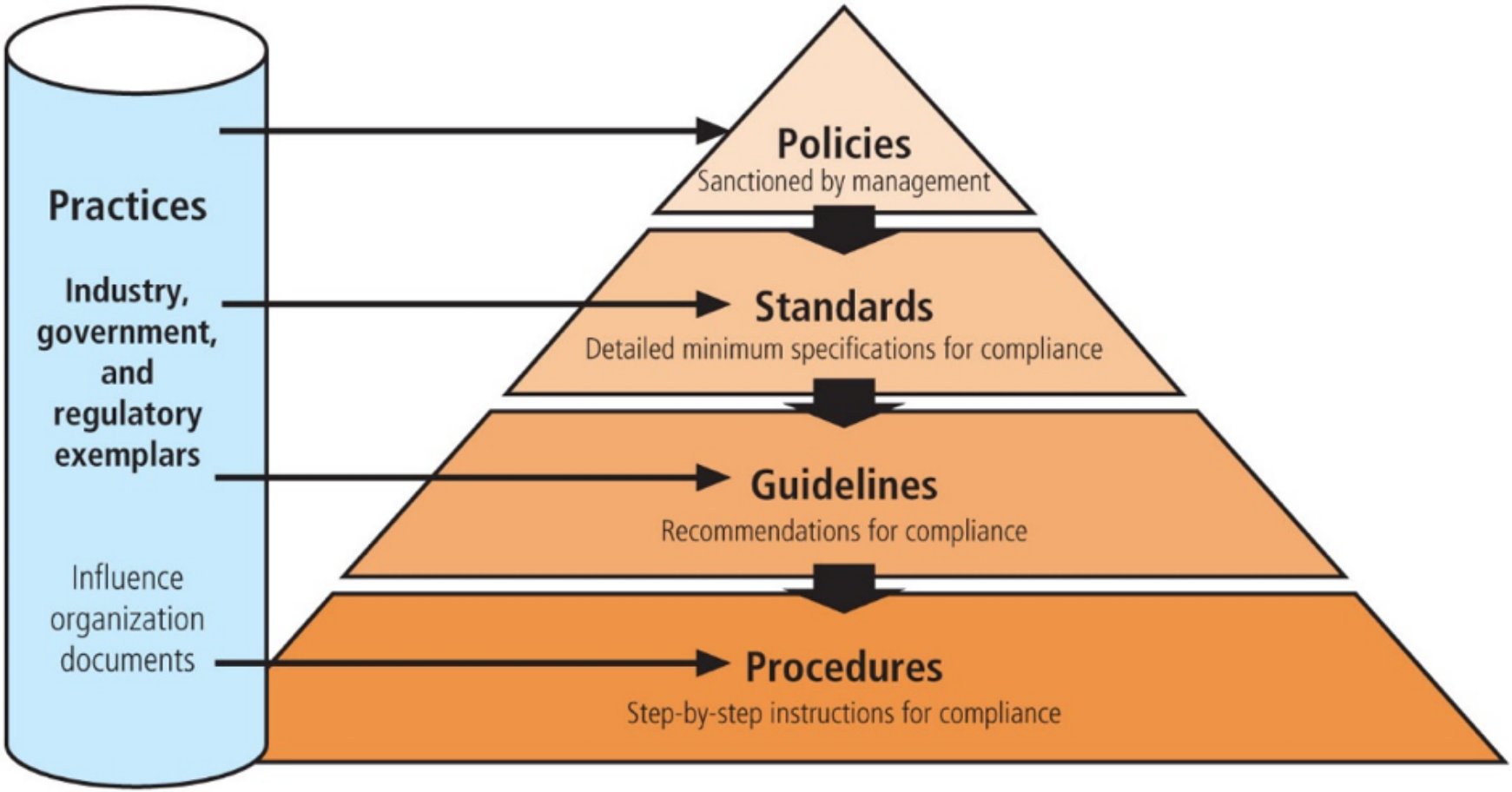

Figure 4-3 Policies, standards, practices, procedures, and guidelines

Group Discussion Questions

- Define an information security policy and discuss its central role in a successful information security program
- List and describe the three major types of information security policy and discuss the major components of each
- Explain what is necessary to implement effective policy and what consequences the organization may face if it does not
- Discuss the process of developing, implementing, and maintaining various types of information security policies
- What's the difference between an ICT policy and a security policy?
- Why do organizations need a Security Policy?
- What are the elements of an Information Security Policy?

Group Discussion Questions

This is to be presented in the next lecture

- Search on the Internet for at least 2 security policies of different organizations including one for Makerere University. Discuss the security policy's components, importance, compliance, incident response, and categorize it as EISP, ISSP or SSP.
- Describe security standards, frameworks and regulations namely: ISO/IEC 27000 series, FISMA, PCI DSS, HIPAA, Sarbanes-Oxley Act, the NIST standards, and GDPR