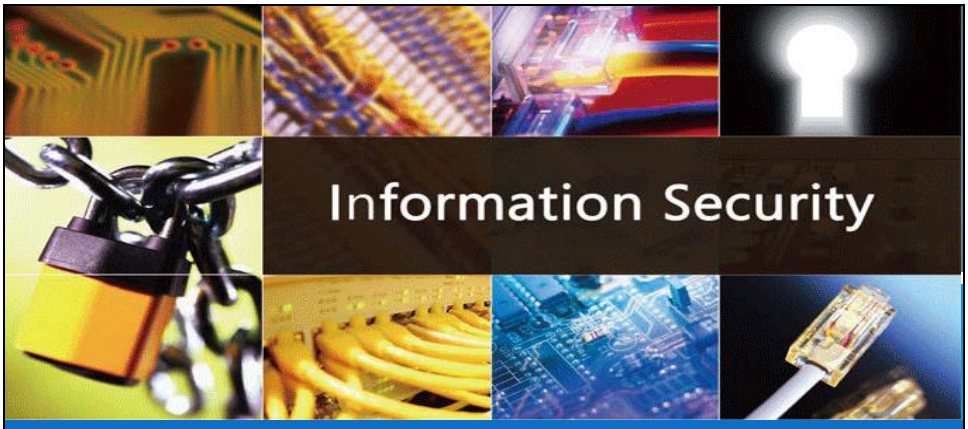


Introduction to Information Security

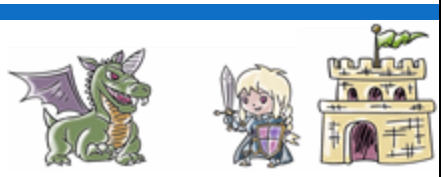
Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Objective

- Understand the definition of information security
- Understand the critical characteristics of information
- Understand the comprehensive model for information security
- Outline the approaches to *information security* implementation
- Outline the phases of the security systems development life cycle
- Understand the key terms of information security

Introduction

- We worry about security when...
  - ...we have something of value and there is a risk it could be harmed



- Individuals store a lot of sensitive data online
  - if stolen, criminals can profit from it
- Societies rely on the internet
  - nefarious parties could profit by controlling it
- Business and government proprietary information is often stored on the internet
  - unauthorized access could be economically or politically disasterous

- How do we understand the risk to our online information and systems?
- We need to develop a security mindset

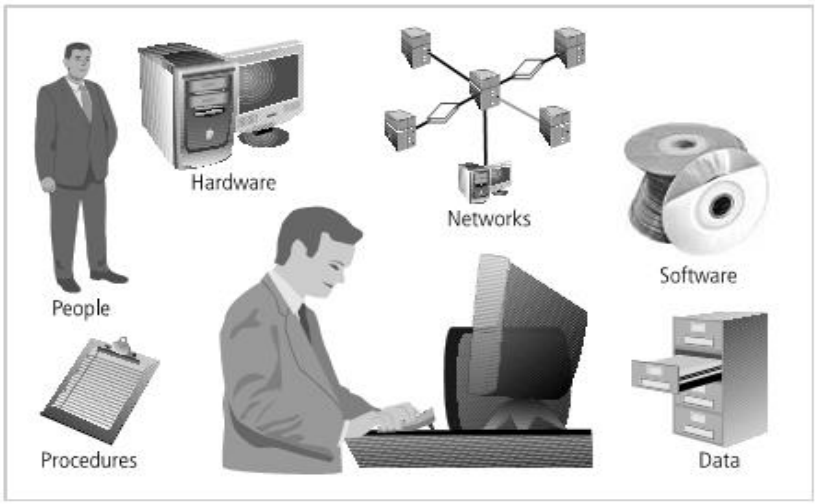
Information security

- Information security: a "well-informed sense of assurance that the information risks and controls are in balance." —James Anderson, Inovant (2002)
- The practice of defending information from
  - unauthorized access,
  - use,
  - disclosure,
  - disruption,
  - modification,
  - perusal,
  - inspection,
  - recording
  - destruction.

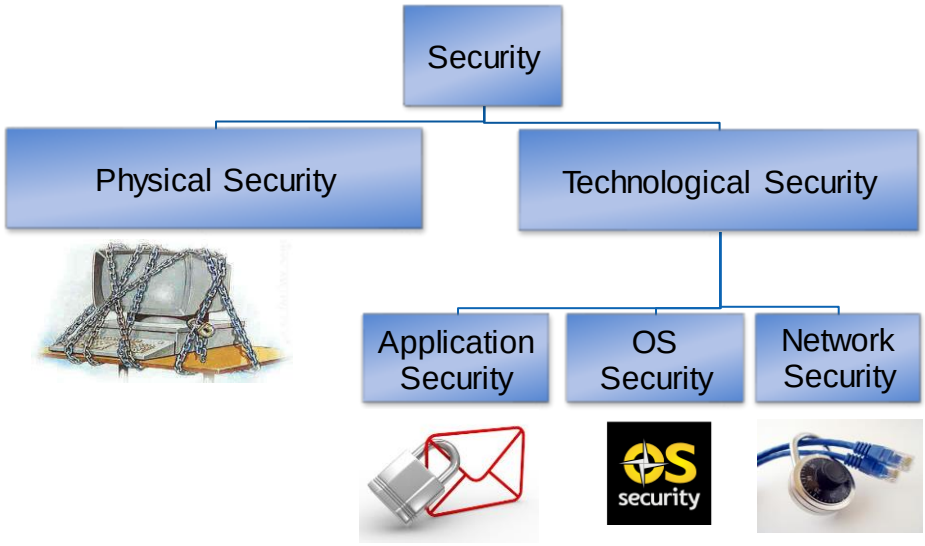
The History of Information Security

- Began immediately after the first mainframes were developed
- Groups developing code-breaking computations during World War II created the first modern computers
- Physical controls to limit access to sensitive military locations to authorized personnel
- Rudimentary in defending against physical theft, espionage, and damage

Components of an Information System



Security



Critical Characteristics of Information

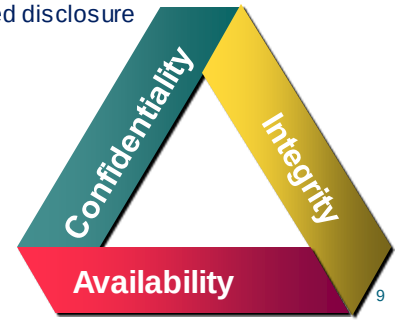
- Availability : Enables authorized users or computers to access information without interference or obstruction and to receive it in the required format
- Accuracy : When it is free from mistakes or errors and it has the value that user expects [Bank Balance]
- Authenticity : The Quality or State of being genuine or Original, rather than a Reproduction or Fabrication [Email spoofing]
- Confidentiality : Prevented from the disclosure or exposure to unauthorized individuals or systems [bits & pieces of info / Salami theft]
- Integrity : It is Whole, complete and uncorrupted [file hashing]
- Utility : The quality or state of having value for some purpose or end
- Possession: The quality or state of having ownership or control of some object or item

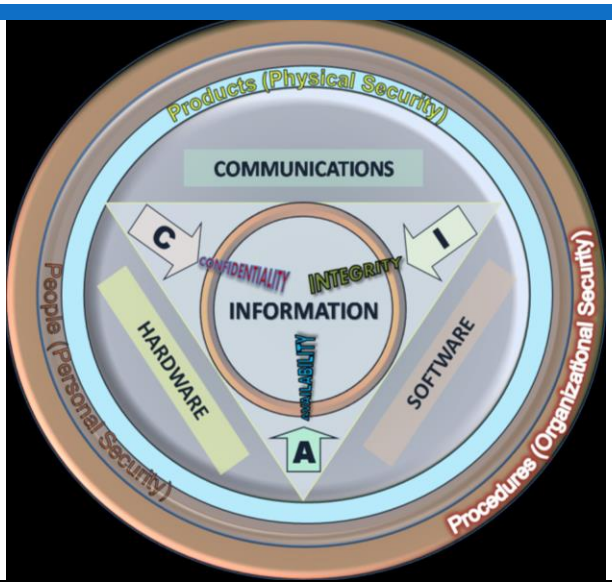
8

Security concepts

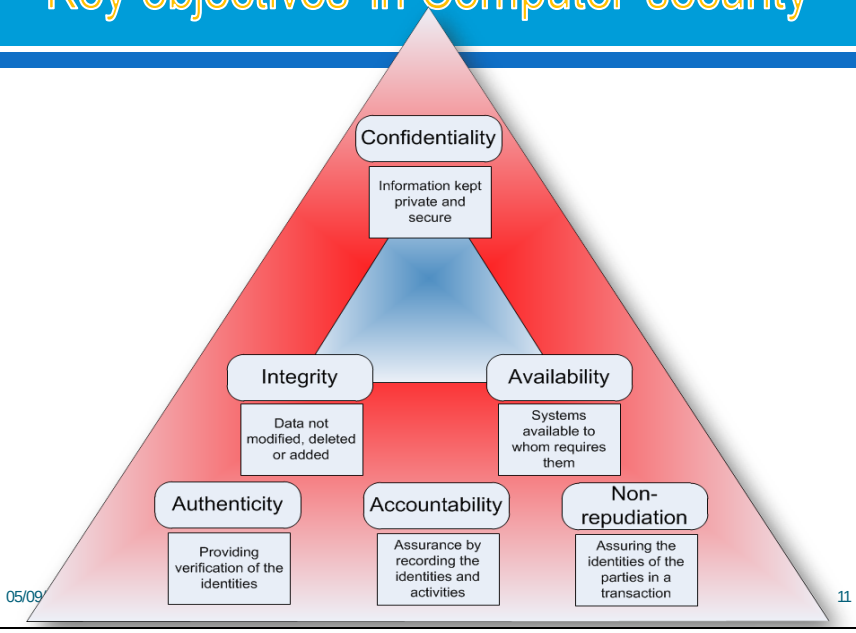
- Computer Security: The protection an information system in order to attain the applicable objectives of preserving of information system resources: (CIA Triad)
  - Integrity: Prevents unauthorized modification of S&I
  - Availability: Prevents disruption of service and productivity.
  - Confidentiality: Prevents unauthorized disclosure of systems and information

  (includes hardware, software, firmware, information/ data, and telecommunications)





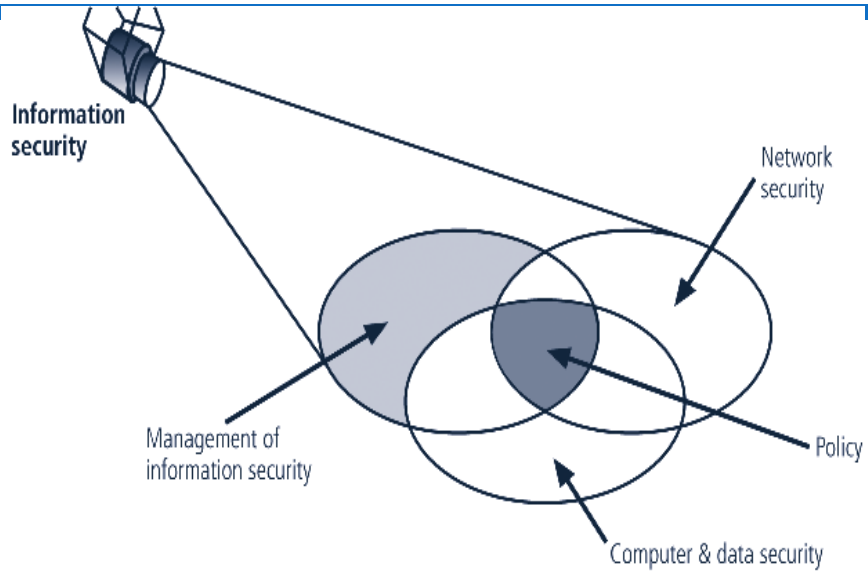
Key objectives in Computer security



Multiple layers of security in an organization

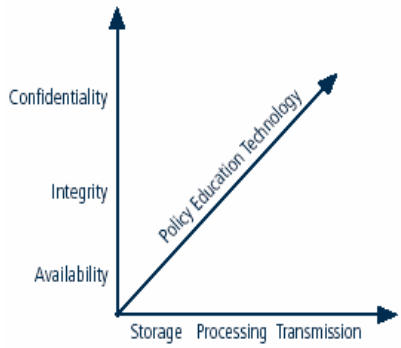
- A successful organization should have multiple layers of security in place:
  - Physical security - Product the Physical items, object or areas from unauthorized access and misuse
  - Personal security - Protection to personal who authorized to access organization and its operation
  - Operations security - Protection of the details of particular operation or activities
  - Communications security - Protection of organizations communication media, technology and content
  - Network security - Protection of Networking Components, Connections and Contents
  - Information security - Protection of information and its Critical elements

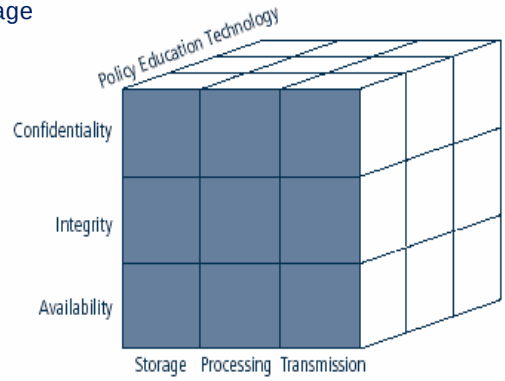
The broad areas of Information Security



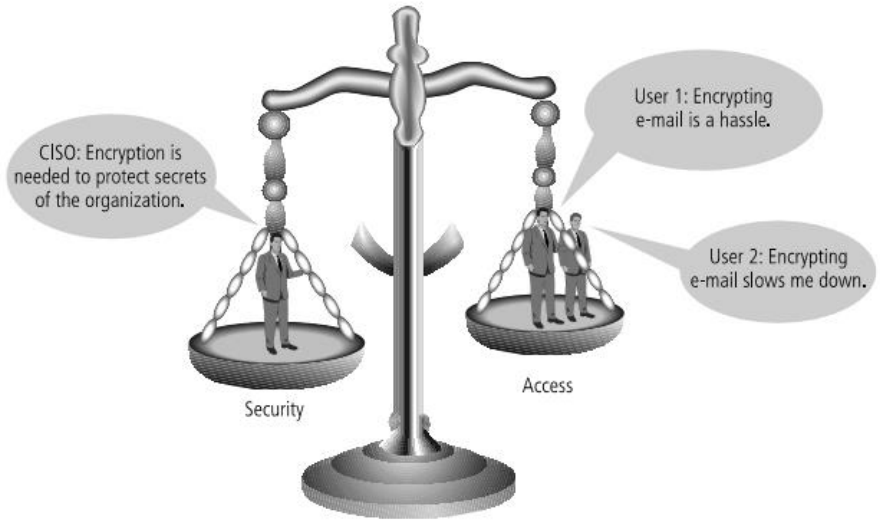
NSTISSC Security Model

- National Security Telecommunications, and Information Systems Security Committee
- Model for Information Security and is becoming Evaluation Standard
- 27 Cells representing areas that must be addressed on the security process
- A control / safeguard that addresses the need to use Technology to protect the Integrity of information while in Storage





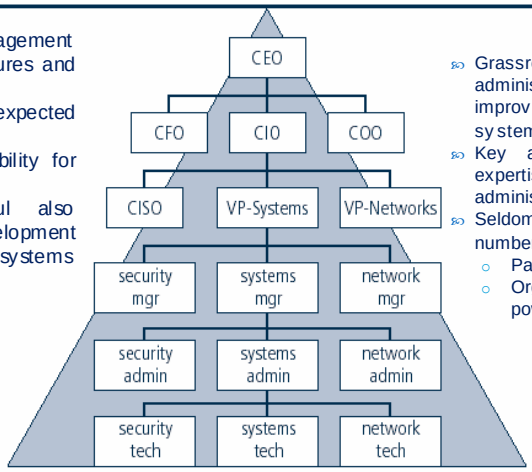
Balancing IS and Access



Approaches to IS Implementation Contd...

Top-down approach

- Initiated by upper management
  - Issue policy, procedures and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful also involve formal development strategy referred to as systems development life cycle



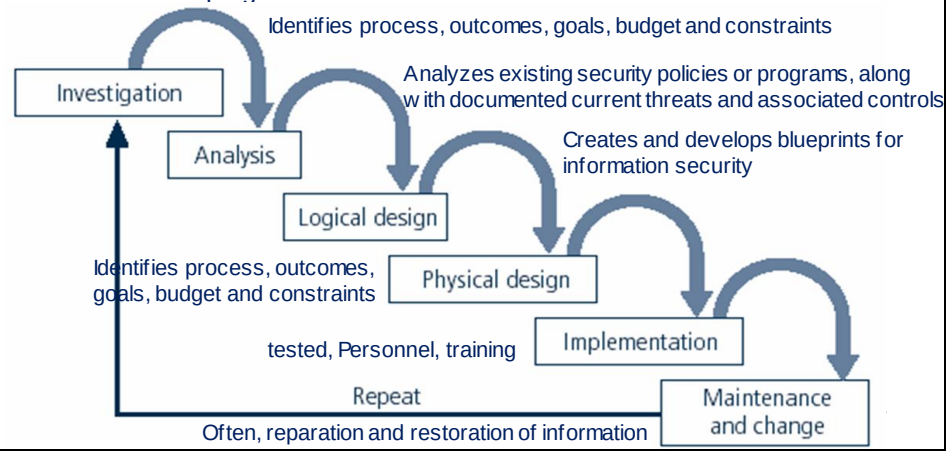
Bottom-up approach

- Grassroots effort: systems administrators attempt to improve security of their systems
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power

16

The Security Systems Development Life Cycle

- be adapted to support specialized implementation of an IS project
- Identify specific threats and creating controls to counter them
- is a coherent program rather than a series of random



The Need for Security in organizations

- Information security performs four important functions for an organization:
  - Protecting the organization's ability to function
  - Enabling the safe operation of applications running on the organization's IT systems
  - Protecting the data the organization collects and uses
  - Safeguarding the organization's technology assets
- Security Professionals: are required to implement details of IS program
  - **Senior management** is key component;
  - additional administrative support
  - technical expertise

Senior Management

- **Chief Information Officer (CIO)**
  - Senior technology officer
  - Primarily responsible for advising senior executives on strategic planning
- **Chief Information Security Officer (CISO)**
  - Primarily responsible for assessment, management, and implementation of IS in the organization
  - Usually reports directly to the CIO Senior Management

Information Security Project Team

- A number of individuals who are experienced in one or more facets of required technical and nontechnical areas:
  - Champion: promote, support financially and administratively
  - Team leader: understands project management
  - Security policy developers: understand the culture, policies
  - Risk assessment specialists: financial risk assessment techniques, security methods
  - Security professionals: trained, and well-educated specialists
  - Systems administrators: primary responsibility for administering
  - End users

Data Responsibilities

- Data owner: responsible for the security and use of a particular set of information
- Data guardian: responsible for storage, maintenance, and protection of information
- Data users: end users who work with information to perform their daily jobs supporting the mission of the organization

Summary

- The definition of information security
- The critical characteristics of information
- The comprehensive model for information security
- The approaches to information security implementation
- The phases of the security systems development life cycle
- The key terms of information security

Q & A

- 2. Assume that a security model is needed for the protection of information in your class. Using the CNSS model, examine each of the cells and write a brief statement on how you would address the three components occupying that cell.
  3. Consider the information stored on your personal computer. For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.
  4. Using the Web, identify the chief information officer, chief information security officer, and systems administrator for your school. Which of these individuals represents the data owner? Data custodian?
  5. Using the Web, find out more about Kevin Mitnick. What did he do? Who caught him? Write a short summary of his activities and explain why he is infamous.