Information Security Policy & Governance

Topic 1: Introduction to Management of Information Security

Objectives:

- Describe the importance of the manager's role in securing an organization's use of information technology and explain who is responsible for protecting an organization's information assets
- List and discuss the key characteristics of information security
- Discuss the key characteristics of leadership and management
- Differentiate information security management from general business management
- Identify and describe basic project management practices and techniques

What is Security?

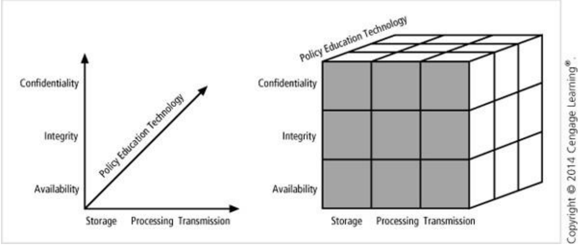
- The quality or state of being secure
  - To be free from danger
- To be secure is to be protected from the risk of loss, damage, or unwanted modification,or other hazards
- Management's role
  - To ensure that each strategy is properly planned, organized,staffed, directed, and controlled
- Specialized areas of security include:
  - ***Physical security***
    - Protecting people, physical assets, and the workplace from various threats
      - Fire, unauthorized access, and natural disasters
  - ***Operations security***
    - Protecting the organization's ability to carry out operational activities without interruption or compromise
  - ***Communications security***
    - Protecting communications media, technology, and content
  - ***Network security***
    - Protecting data networking devices, connections, and contents
      - Router, Switches etc.
- Information security (InfoSec)
  - Protection of information and its critical elements (confidentiality, integrity and availability), including the systems and hardware that use, store,and transmit that information

NSTISSI (CNSS) Security Model

- Aka the McCumber Cube
- Serves as the standard for understanding aspects of InfoSec
- Main goal is to identify gaps in the coverage of an InfoSec program

The model covers the three dimensions central to InfoSec

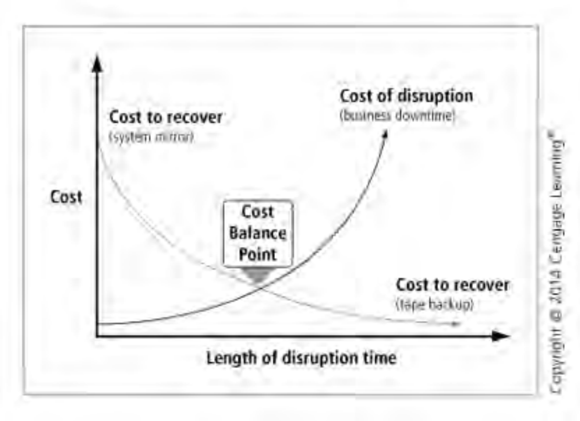
- Information characteristics
- Information location
- Security control categories



Note: When using this model, ensure all 27 cells are properly addressing the use of technology to protect integrity of information while in storage

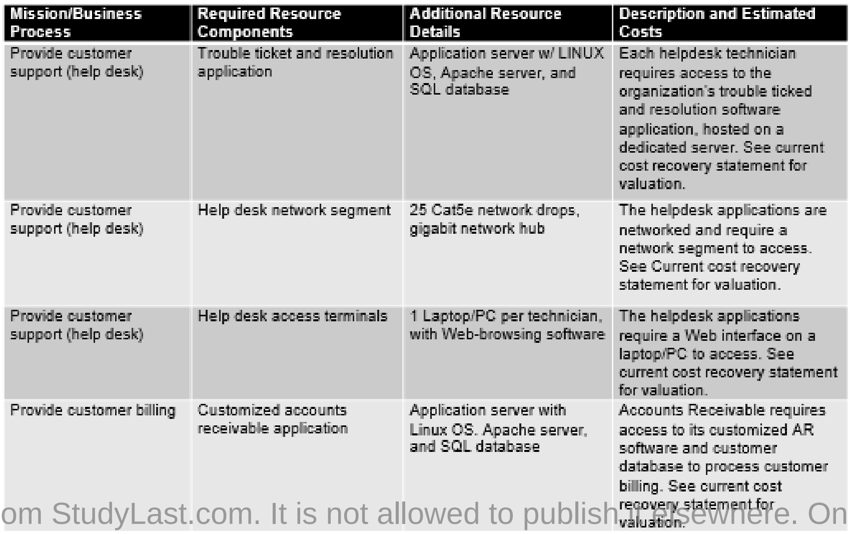
- The CPMT conducts the BIA in three stages:
  - ***Determine mission/business processes and recovery criticality***
    - Determine how important its each business department/unit/division functions are to the organization
    - Weighted analysis table useful to determine which business functions is most critical
    - Key recovery measures:
      - Maximum Tolerable Downtime (MTD)
        - ✓ Total amount of time that system resources is allowed to remain unavailable
      - Recovery Time Objective (RTO)
        - ✓ Maximum amount of time system resources can remain unavailable
      - Recovery Point Objective (RPO)
        - ✓ Point in time, prior to disruption/system outage, mission/business process data can be recovered after an outage
      - Work Recovery Time (WRT)
        - ✓ Amount of effort required to get the business functionality operational, after the technology element is recovered

Figure 3-3 Cost balancing



  - ***Identify resource requirements***
    - Need to determine resources required to recover processes & assets

Table 3-1 Example resource/components table



Mission/Business Process	Required Resource Components	Additional Resource Details	Description and Estimated Costs
Provide customer support (help desk)	Trouble ticket and resolution application	Application server w/ LINUX OS, Apache server, and SQL database	Each helpdesk technician requires access to the organization's trouble ticked and resolution software application, hosted on a dedicated server. See current cost recovery statement for valuation.
Provide customer support (help desk)	Help desk network segment	25 Cat5e network drops, gigabit network hub	The helpdesk applications are networked and require a network segment to access. See Current cost recovery statement for valuation.
Provide customer support (help desk)	Help desk access terminals	1 Laptop/PC per technician, with Web-browsing software	The helpdesk applications require a Web interface on a laptop/PC to access. See current cost recovery statement for valuation.
Provide customer billing	Customized accounts receivable application	Application server with Linux OS, Apache server, and SQL database	Accounts Receivable requires access to its customized AR software and customer database to process customer billing. See current cost recovery statement for valuation.

Topic 6: Security Management Models

Objectives

- Describe the dominant InfoSec blueprints, frameworks, and InfoSec management models, including U.S. government-sanctioned models
- Explain why access control is an essential element of InfoSec management
- Recommend an InfoSec management model and explain how it can be customized to meet the needs of a particular organization
- Describe the fundamental elements of key InfoSec management practices
- Discuss emerging trends in the certification and accreditation of U.S. federal information technology (IT) systems

Blueprints, Frameworks, and Security Models

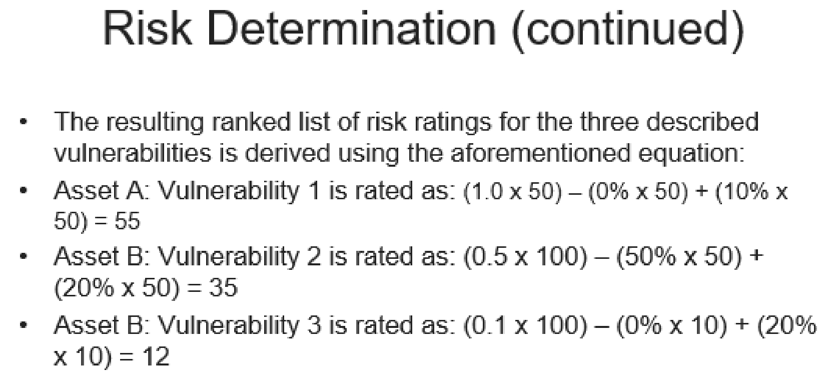
- **Blueprint**
  - Describes existing controls and identifies other necessary security controls
- **Framework**
  - The outline of the more thorough blueprint
  - Sets out the model to be followed in the creation of the design, selection, and initial implementation of all subsequent security controls
- **Security model**
  - A generic blueprint offered by a service organization
  - Free models are available from the National Institute of Standards andTechnology (NIST)
- **Benchmarking**
  - Comparison of two related measurements
  - Or whether new controls should be considered
  - However, it doesn’t provide details on how controls should be put into action

Access Control Models

- Access controls
  - Regulates the admission of users into trusted areas of the organization
- Access control is **maintained by** means of:
  - A collection of policies
  - Programs to carry out those policies
  - Technologies to enforce policies
- General application of access control comprises **four processes**:
  - ***Identification***
    - Obtaining identity of the entity requesting access to a logical or physical area
  - ***Authentication***
    - Confirming the identity
  - ***Authorization***
    - Determining which actions an authenticated entity can performin that physical logical area
  - ***Accountability***
    - Documenting the activities of the authorized individual and systems
- Access control is built on several **key principles**:
  - ***Least privilege***
    - Member of the organization can access the minimum amount of information for the minimum amount of time necessary
  - ***Need-to-know***
    - Limits a user’s access to the specific information required to perform the currently assigned task
  - ***Separation of duties***

Risk Determination

- For the purpose of relative risk assessment:
  - Likelihood of vulnerability occurrence *times* value is Product A
  - Risk *equals* Product A *minus* (percentage risk already controlled *times* Product A) *plus* (an element of uncertainty *times* Product A)
  - Example:
    - Information asset A has a value score of 50 and one vulnerability:
      - Vulnerability 1has a likelihood of 1.0 with no current controls. You estimate that assumptions and data are 90% accurate
    - Information asset B has a value score of 100 and two vulnerabilities:
      - Vulnerability2 has a likelihood of 0.5 with a current control that addresses 50% of its risk. Vulnerability 3 has a likelihood of 0.1 with no current controls. You estimate thatassumptions and data are 80% accurate.



Risk Determination (continued)

- The resulting ranked list of risk ratings for the three described vulnerabilities is derived using the aforementioned equation:
- Asset A: Vulnerability 1 is rated as: (1.0 x 50) – (0% x 50) + (10% x 50) = 55
- Asset B: Vulnerability 2 is rated as: (0.5 x 100) – (50% x 50) + (20% x 50) = 35
- Asset B: Vulnerability 3 is rated as: (0.1 x 100) – (0% x 10) + (20% x 10) = 12

Identify Possible Controls

- For each threat and its associated vulnerabilities that have residual risk
  - The organization should create a preliminary list of control ideas
  - Purpose of the list is to identify areas of ***residual risk***
    - Risk that remains even after the existing control has been applied
- “Controls”, “safeguards”, and “countermeasures” are terms used to describe security mechanisms which counter attacks, reduce risk, resolve vulnerabilities, and improve security

   - Readily available for employee reference
   - Easily understood, with multilingual translations and translations for visually impaired or low-literacy employees
   - Acknowledged by the employee
   - Uniformly enforced for all employees

Ethics in InfoSec

- The foundations and frameworks of ethics include:
   - ***Normative ethics*** - the study of what makes actions right or wrong
   - ***Meta-ethics*** - the study of the meaning of ethical judgments and properties
   - ***Descriptive ethics*** - study of the choices that have been made by individuals inthe past
   - ***Applied ethics*** - applies moral codes to actions drawn from realistic situations
   - ***Deontological ethics*** - study of the rightness or wrongness of intentions and motives
- From ethical frameworks come a series of ethical standards:
   - ***Utilitarian approach*** - emphasizes that an ethical action is one that results in themost good
   - ***Rights approach*** - the ethical action is the one that best protects and respectsthe moral rights of those affected by that action
   - ***Fairness or justice approach*** - defines ethical actions as those that have outcomes that regard all human beings equally
   - ***Common good approach*** - this approach tends to focus on the common welfare
   - ***Virtue approach*** - ethical actions ought to be consistent with so-called idealvirtues

Ethics and Education

- These ethical standards or approaches offer a set of tools for decision making in the eraof computer technology
- Key studies reveal that the overriding factor in leveling the ethical perceptions within asmall population is education
- Employees must be trained and kept up to date on InfoSec topics
   - Including the expected behaviors of an ethical employee
- Proper ethical and legal training is vital to creating an informed, well-prepared, and low-risk system user

Deterring Unethical and Illegal Behavior

- **Three general categories** of unethical behavior that organizations and society shouldseek to eliminate: