Information Systems Security

Lectures 10, 11, 12

Information Security Management

Dr. En. Bader Ahmad

References

1. James Joshi, Security Management Course, http://www.sis.pitt.edu/~jjoshi/IS2820/Fall2007

2. *Network security, The complete Reference*. R. Bragg, M. Rhodes-Ousley, K. Strassberg. McGraw-Hill Osborne, 2004.

3. Management of Information Security, M. E. Whitman, H. J. Mattord

Objective

- The course is aimed at imparting knowledge and skill sets required to assume the overall responsibilities of administration and management of security of an enterprise information system.

Learning Outcome

- After the course, ability to carry out:
  - Detailed analysis of enterprise security by performing various types of analysis
  - Carry out the task of security risk management using various tools.
  - Design detailed enterprise wide security plans and policies, and deploy appropriate safeguards (models, mechanisms and tools)

Outline

1. Introduction
2. Security Planning
3. Continuity Planning
4. Policy
5. Security Management Models and Practices
6. Risk Management
7. Legal and Ethics Issues

Information Security Management

1. Introduction

Outline

1. Introduction
2. Characteristics of management
3. Principles of Information Security Management

1. Introduction

- Information technology is critical to business and society

- Information Security protects:
  - Data
  - Human resources
  - …

- Information security is the responsibility of every member of an organization, especially managers.

Introduction

- Information security involves three decision makers:
  - Information security managers and professionals
  - Information technology managers and professionals
  - Non-technical business managers and professionals
- Communities roles:
  - InfoSec community:
    - protect information assets from threats
  - IT community:
    - support business objectives by supplying appropriate information technology
  - Business community:
    - policy and resources

What Is Security?

- **Security** is "The quality or state of being secure—to be free from danger"

- Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security

What Is Management?

- **Management** : process of achieving objectives using a given set of resources.

- To manage the information security process, first understand core principles of management.

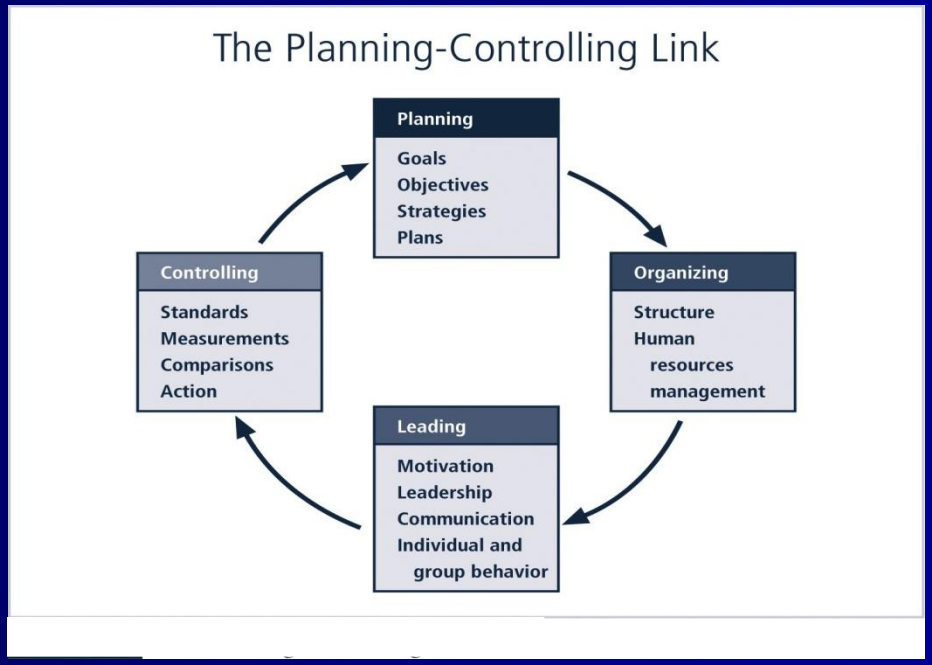
- A manager is
  - "someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals".

Managerial Roles

- Informational role: Collecting, processing, and using information to achieve the objective.
- Interpersonal role: Interacting with superiors, subordinates, outside stakeholders, and other.
- Decisional role: Selecting from alternative approaches and resolving conflicts, dilemmas, or challenges.

2. Characteristics of Management

- A well-known approaches to management:
  - POLC: Popular management theory using principles of management into planning, organizing, leading, and controlling



Planning & Organization

- **Planning**: process that develops, creates, and implements strategies for the accomplishment of objectives.
- Three levels of planning:
  1. **Strategic**: occurs at the highest levels of the organization (five or more years)
  2. **Tactical**: planning focuses on production planning and integrates organizational resources at a level below the entire enterprise (one to five years).
  3. **Operational**: focuses on the day-to-day operation of local resources
- **Organization**: structuring of resources to support the accomplishment of objectives.

Leadership & Controlling

- **Leadership** encourages the implementation of
  - the planning and organizing functions,
    - Includes supervising employee behavior, performance, attendance, and attitude
- Leadership generally addresses the direction and motivation of the human resource
- **Controlling**:
  - Monitoring progress toward completion
  - Making necessary adjustments to achieve the desired objectives
- Controlling function determines what must be monitored as well as using specific control tools to gather and evaluate information

3. Principles Of Information Security Management

1. Planning
2. Policy
3. Programs
4. Protection
5. People
6. Project Management

InfoSec Planning

- **Planning** as part of InfoSec management
  - is an extension of the basic planning model discussed earlier.

- Included in the InfoSec planning model are
  - activities necessary to support the design, creation, and implementation of information security strategies as they exist within the IT planning environment

InfoSec Planning Types

- Several types of InfoSec plans exist:
  - Incident response
  - Business continuity
  - Disaster recovery
  - Policy
  - Personnel
  - Technology rollout
  - Risk management and
  - Security program including education, training and awareness

Policy

- **Policy**: set of organizational guidelines that dictates certain behavior within the organization

- In InfoSec, there are three general categories of policy:
  - General program policy (Enterprise Security Policy)
  - An issue-specific security policy (ISSP)
    - E.g., email, Intenert use
  - System-specific policies (SSSPs)
    - E.g., Access control list (ACLs) for a device

Programs

- **Programs** are operations managed as
  - specific entities in the information security domain
  - Example:
    - Security Education Training and Awareness (SETA) program.
  - Other programs that may emerge include
    - physical security program, complete with fire, physical access, gates, guards, and so on.