Policy

- A critical design element of the information security program is the information security policy
- Management must define three types of security policy:
  - General or security program policy (GSP)
  - Issue-specific security policies (ISSP)
  - Systems-specific security policies (SSSP)

SETA

- An integral part of the InfoSec program is
  - Security education and training (SETA) program
  - SETA program consists of three elements:
    - security education, security training, and security awareness
- Purpose of SETA is to enhance security by:
  - Improving awareness
  - Developing skills and knowledge
  - Building in-depth knowledge

Design

- Attention turns to the design of the controls and safeguards used to protect information from attacks by threats

- Three categories of controls:
  - Managerial
  - Operational
  - Technical

Managerial Controls

- Address design/implementation of the
  - security planning process and
  - security program management

- Management controls also address:
  - Risk management
  - Security control reviews

  - Legal compliance and maintenance of the entire security life cycle

Operational Controls

- Cover management functions and lower level planning including:
  - Disaster recovery
  - Incident response planning
- Operational controls also address:
  - Personnel security
  - Physical security
  - Protection of production inputs and outputs

Technical Controls

- Address those tactical and technical issues related to
  - designing and implementing security in the organization
- Technologies necessary to protect information are examined and selected

Contingency Planning

- Essential preparedness documents provide contingency planning (CP) to prepare, react and recover from circumstances that threaten the organization:
  - Incident response planning (IRP)
  - Disaster recovery planning (DRP)
  - Business continuity planning (BCP)

Implementation in the SecSDLC

- Security solutions are acquired, tested, implemented, and tested again
- Personnel issues are evaluated and specific training and education programs conducted
- Perhaps most important element of implementation phase is management of project plan:
  - Planning the project
  - Supervising tasks and action steps within the project
  - Wrapping up the project

InfoSec Project Team

- Should consist of individuals experienced in one or multiple technical and non-technical areas including:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

InfoSec Professionals

- It takes a wide range of professionals to support a diverse information security program:
  - Chief Information Officer (CIO)
  - Chief Information Security Officer (CISO)
  - Security Managers
  - Security Technicians
  - Data Owners
  - Data Custodians
  - Data Users

Maintenance in the SecSDLC

- Once information security program is implemented,
  - it must be properly operated, managed, and kept up to date by means of established procedures
- If the program is not adjusting adequately to the changes in the internal or external environment, it may be necessary to begin the cycle again

3. Contingency Planning

Outline

1. Introduction
2. Incident Response
3. Disaster Recovery
4. Business Continuity

Introduction

- Planning for the unexpected event
  - the use of technology is interrupted
- Procedures are required in order to stand up to unexpected events
- The overall planning for unexpected events is called contingency planning (CP).

What Is Contingency Planning?

- It is how organizational planners position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets.

- Main goal: restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event.

CP Components

- Incident response planning (IRP) focuses on immediate response
- Disaster recovery planning (DRP) focuses on restoring operations at the primary site after disasters occur
- Business continuity planning (BCP) facilitates establishment of operations at an alternate site

CP Components (Continued)

- To ensure continuity across all CP processes during planning process, contingency planners should:
  - Identify the mission- or business-critical functions
  - Identify resources that support critical functions
  - Anticipate potential contingencies or disasters
  - Select contingency planning strategies
  - Implement selected strategy
  - Test and revise contingency plans

Incident Response Plan

- IRP:
  - Detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets

- Incident response (IR):
  - Set of procedures that commence when an incident is detected

Incident Response Plan (Continued)

- When a threat becomes a valid attack, it is classified as an **information security incident** if:
  - It is directed against information assets
  - It has a realistic chance of success
  - It threatens the confidentiality, integrity, or availability of information assets

- It is important to understand that IR is a reactive measure, not a preventive one