SECURITY IN COMPUTING, FIFTH EDITION

Chapter 10: Management and Incidents

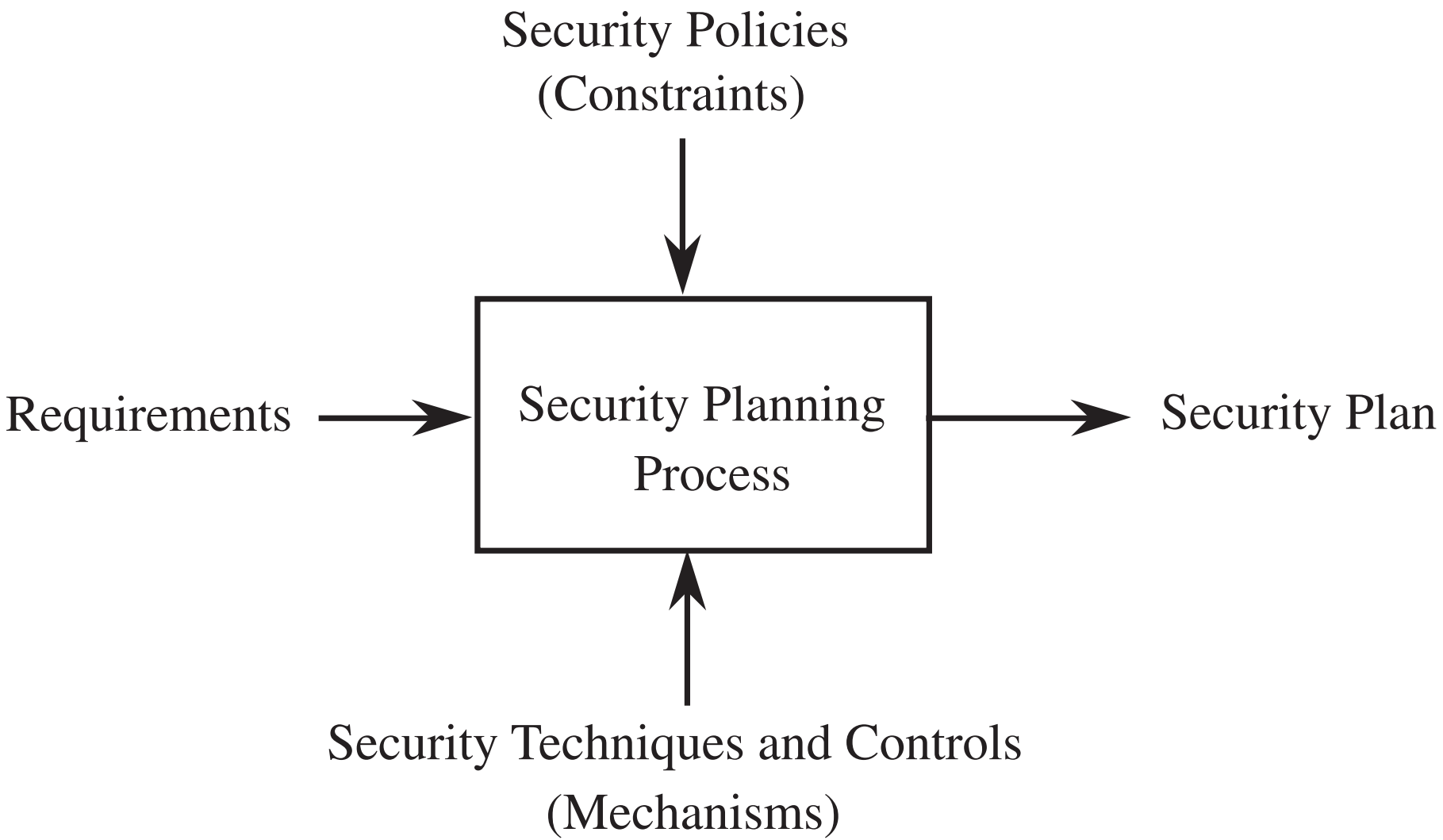
Chapter 10 Objectives

- Study the contents of a good **security plan**
- Learn to plan for responding to **incidents**
- Outline the steps and best practices of **risk analysis**
- Learn to prepare for natural and human-caused **disasters**

Contents of a Security Plan

- *Policy,* indicating the goals of a computer security effort and the willingness of the people involved to work to achieve those goals
- *Current state*, describing the status of security at the time of the plan
- *Requirements*, recommending ways to meet the security goals
- *Recommended controls*, mapping controls to the vulnerabilities identified in the policy and requirements
- *Accountability*, documenting who is responsible for each security activity
- *Timetable*, identifying when different security functions are to be done
- *Maintenance,* specifying a structure for periodically updating the security plan

Inputs to the Security Plan



Security Planning Team Members

- Security planning touches every aspect of an organization and therefore requires participation well beyond the security group
- Common security planning representation:
  - Computer hardware group
  - System administrators
  - Systems programmers
  - Applications programmers
  - Data entry personnel
  - Physical security personnel
  - Representative users

Assuring Commitment to a Security Plan

- A plan that has no organizational commitment collects dust on a shelf
- Three groups of people must contribute to making the plan a success:
  - The planning team must be sensitive to the needs of each group affected by the plan.
  - Those affected by the security recommendations must understand what the plan means for the way they will use the system and perform their business activities. In particular, they must see how what they do can affect other users and other systems.
  - Management must be committed to using and enforcing the security aspects of the system.

Incident Response Plans

- A security incident response plan tells the staff how to deal with a security incident
- In contrast to a business continuity plan, the goal of incident response is handling the current security incident without direct regard for the business issues
- **An incident response plan should**
  - **Define what constitutes an incident**
  - **Identify who is responsible for taking charge of the situation**
  - **Describe the plan of action**

Incident Response Teams

- The response team is charged with responding to the incident. It may include
  - Director : The person in charge of the incident, who decides what actions to take
  - Technicians: People who perform the technical part of the response
  - Advisors: Legal, human resources, or public relations staff members as appropriate
- **Matters to consider when identifying a response team:**
  - **Legal issues**
  - **Preserving evidence**
  - **Records**
  - **Public relations**

CSIRTs

- Computer Security Incident Response Teams (CSIRT) are teams trained and authorized to handle security incidents
- Responsibilities of a CSIRT include
  - Reporting: Receiving reports of suspected incidents and reporting as appropriate to senior management
  - Detection: Investigation to determine if an incident occurred
  - Triage: Immediate action to address urgent needs
  - Response: Coordination of effort to address all aspects in a manner appropriate to severity and time demands
  - Postmortem: Declaring the incident over and arranging to review the case to improve future response
  - Education: Preventing harm by advising on good security practices and disseminating lessons learned from past incidents

CSIRT Skills

- Collect, analyze, and preserve digital forensic evidence
- Analyze data to infer trends
- Analyze the source, impact, and structure of malicious code
- Help manage installations and networks by developing defenses such as signatures
- Perform penetration testing and vulnerability analysis
- Understand current technologies used in attacks

Risk Analysis

- Risk analysis is an organized process for identifying the most significant risks in a computing environment, determining the impact of those risks, and weighing the desirability of applying various controls against those risks
- A risk is a potential problem that the system or its users may experience
- Characteristics of a risk:
  - Associated loss (also known as a *risk impact*)
  - Likelihood of occurring
  - Degree to which we can change the outcome (risk control)
- We can theoretically quantify the effects of a risk, or risk exposure, by multiplying likelihood by risk impact

Strategies for Dealing with Risk

- *Avoid* the risk by changing requirements for security or other system characteristics
- *Transfer* the risk by allocating the risk to other systems, people, organizations, or assets or by buying insurance to cover any financial loss should the risk become a reality
- *Assume* the risk by accepting it, controlling it with available resources, and preparing to deal with the loss if it occurs

Steps of a Risk Analysis

1. Identify assets.
2. Determine vulnerabilities.
3. Estimate likelihood of exploitation.
4. Compute expected annual loss.
5. Survey applicable controls and their costs.
6. Project annual savings of control.

Arguments Against Risk Analysis

- False sense of precision and confidence
- Hard to perform
- Immutability
- Lack of accuracy

Natural Disasters

- Examples:
  - Flood
  - Fire
  - Earthquake
- Mitigations:
  - Develop contingency plans so that people know how to react in emergencies and business can continue
  - Insure physical assets—computers, buildings, devices, supplies—against harm
  - Preserve sensitive data by maintaining copies in physically separated locations
  - Prevent power loss using uninterruptable power supplies and surge suppressors

Contingency Planning

- Backups
  - Offsite backup
  - Cloud backup
- Failover
  - Cold site
  - Hot site

Summary

- A security plan is both an official record of current security practices and a blueprint for orderly change to improve those practices
- Incident response planning help establish an orderly, carefully considered response to emergencies and other security incidents
- Risk analysis is a complex and imperfect process but forces an organization to carefully consider important assets, vulnerabilities, risks, and control options
- Prepare for disasters by contingency planning, insuring assets, backing up data, and deploying failover sites