COURSE TECHNOLOGY
CENGAGE Learning™

Security+ Guide to Network Security Fundamentals, Third Edition

Chapter 14

Security Policies and Training

What Is a Security Policy?

- **Security policy**
  - A written document that states how an organization plans to protect the company's information technology assets
- An organization's information security policy can serve several functions:
  - It can be an overall intention and direction
  - It details specific risks and how to address them
  - It can create a security-aware organizational culture
  - It can help to ensure that employee behavior is directed and monitored

Balancing Trust and Control

- An effective security policy must carefully balance two key elements: trust and control
- Three approaches to trust:
  - Trust everyone all of the time
  - Trust no one at any time
  - Trust some people some of the time
- Deciding on the level of control for a specific policy is not always clear
  - The security needs and the culture of the organization play a major role when deciding what level of control is appropriate

Balancing Trust and Control (continued)

User Group	Attitude Toward Security
Users	Want to be able to get their work done without restrictive security controls
System support personnel	Concerned about the ease of managing systems under tight security controls
Management	Concerned about cost of security protection for attacks that may not materialize

Table 14-1 Possible negative attitudes toward security

Designing a Security Policy

- Definition of a policy
  - **Standard**
    - A collection of requirements specific to the system or procedure that must be met by everyone
  - **Guideline**
    - A collection of suggestions that should be implemented
  - **Policy**
    - Document that outlines specific requirements or rules that must be met

Designing a Security Policy (continued)

- A policy generally has these characteristics:
  - Policies communicate a consensus of judgment
  - Policies define appropriate behavior for users
  - Policies identify what tools and procedures are needed
  - Policies provide directives for Human Resource action in response to inappropriate behavior
  - Policies may be helpful in the event that it is necessary to prosecute violators

Designing a Security Policy (continued)

- The security policy cycle
  - The first phase involves a **risk management study**
    - Asset identification
    - Threat identification
    - Vulnerability appraisal
    - Risk assessment
    - Risk mitigation
  - The second phase of the security policy cycle is to use the information from the risk management study to create the policy
  - The final phase is to review the policy for compliance

Designing a Security Policy (continued)

Figure 14-1 Security policy cycle

Designing a Security Policy (continued)

- Steps in development
  - When designing a security policy many organizations follow a standard set of principles
  - It is advisable that the design of a security policy should be the work of a team
  - The team should first decide on the scope and goals of the policy
  - Statements regarding **due care** are often included
    - The obligations that are imposed on owners and operators of assets to exercise reasonable care of the assets and take necessary precautions to protect them

Designing a Security Policy (continued)

Security Policy Must	Security Policy Should
Be implementable and enforceable	State reasons why the policy is necessary
Be concise and easy to understand	Describe what is covered by the policy
Balance protection with productivity	Outline how violations will be handled

Table 14-2 Policy must and should statements

Designing a Security Policy (continued)

- Many organizations also follow these guidelines while developing a policy:
  - Notify users in advance that a new security policy is being developed and explain why the policy is needed
  - Provide a sample of people affected by the policy with an opportunity to review and comment on the policy
  - Prior to deployment, give all users at least two weeks to review and comment
  - Allow users the authority to carry out their responsibilities in a given policy

Types of Security Policies

- The term *security policy* becomes an umbrella term for all of the sub policies included within it.

Name of Security Policy	Description
Acceptable encryption policy	Defines requirements for using cryptography
Analog line policy	Defines standards for use of analog dial-up lines for sending and receiving faxes and for connection to computers
Anti-virus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments, investigate incidents, to ensure conformance to security policies, or to monitor user activity
Automatically forwarded e-mail policy	Prescribes that no e-mail will be automatically forwarded to an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Dial-in access policy	Outlines appropriate dial-in access and its use by authorized personnel
Demilitarized zone security policy	Defines standards for all networks and equipment located in the DMZ
E-mail policy	Creates standards for using corporate e-mail
E-mail retention policy	Helps employees determine what information sent or received by e-mail should be retained and for how long
Extranet policy	Defines the requirements for third-party organizations to access the organization's networks
Information sensitivity policy	Establishes criteria for classifying and securing the organization's information in a manner appropriate to its level of security
Router security policy	Outlines standards for minimal security configuration for routers and switches
Server security policy	Creates standards for minimal security configuration for servers
VPN security policy	Establishes requirements for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the organization's network
Wireless communication policy	Defines standards for wireless systems used to connect to the organization's networks

Table 14-3 Types of security policies

Continuity Strategies

- Incident response plans (IRPs); disaster recovery plans (DRPs); business continuity plans (BCPs)
- Primary functions of above plans
  - IRP focuses on immediate response; if attack escalates or is disastrous, process changes to disaster recovery and BCP
  - DRP typically focuses on restoring systems after disasters occur; as such, is closely associated with BCP
  - BCP occurs concurrently with DRP when damage is major or long term, requiring more than simple restoration of information and information resources

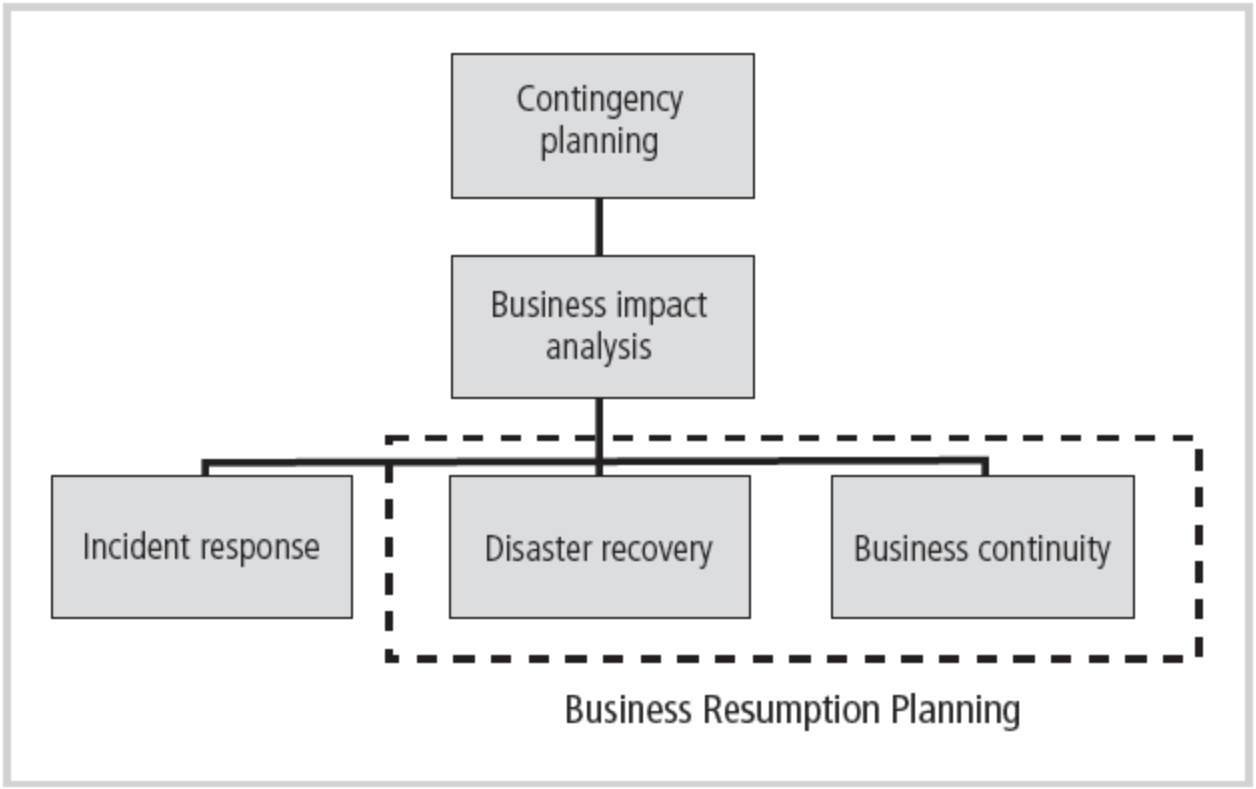

Figure 5-14 Components of Contingency Planning

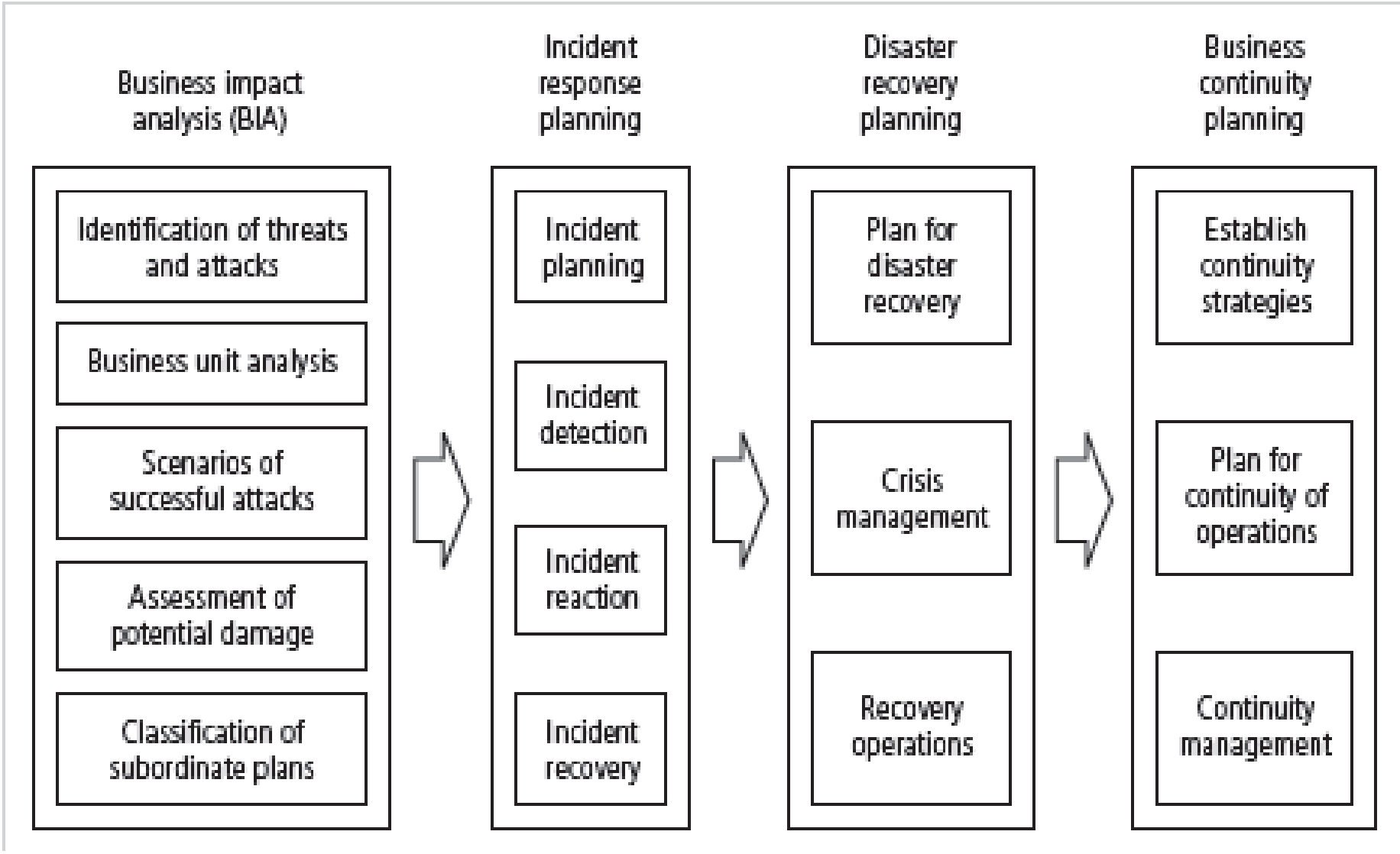

Figure 5-16 Major Steps in Contingency Planning