Management of Information Security, 4th Edition

Chapter 3

Planning for Contingencies

Objectives

- Discuss the need for contingency planning
- Describe the major components of contingency planning
- Develop a simple set of contingency plans, using business impact analysis
- Discuss how the organization would prepare and execute a test of contingency plans
- Explain the unified contingency plan approach

Fundamentals of Contingency Planning Part 1

- IT and InfoSec managers can either
  - Create and develop these four CP components as one unified plan
  - Create the four separately in conjunction with a set of interlocking procedures that enable continuity
- Typically, larger organizations create the CP components separately
  - Smaller organizations tend to adopt a one-plan method

Fundamentals of Contingency Planning Part 2

- The **contingency planning management team (CPMT)** begins developing a CP document by:
  - – Developing the CP policy statement
  - – Conducting the **Business Impact Analysis - BIA**
  - – Identifying preventative controls
  - – Creating contingency strategies
  - – Developing a contingency plan
  - – Ensuring plan testing, training, and exercises
  - – Ensuring plan maintenance

Fundamentals of Contingency Planning Part 3

- The CP policy should contain, at a minimum:
  - An introductory statement of philosophical perspective by senior management
  - A statement of the scope and purpose of the CP operations
  - A call for periodic risk assessment and BIA
  - A description of the CP major components
  - A call for, and guidance in, selection of recovery options and BC strategies
  - A requirement to test various plans regularly

Fundamentals of Contingency Planning Part 4

- The CP policy should contain, at a minimum (cont’d):
  - Identification of key regulations and standards that impact CP planning
  - Identification of key individuals responsible for CP operations
  - An appeal to the individual members of the organization, asking for support
  - Additional administrative information, including original date of document, revision dates, and a schedule for periodic review and maintenance

Fundamentals of Contingency Planning Part 5

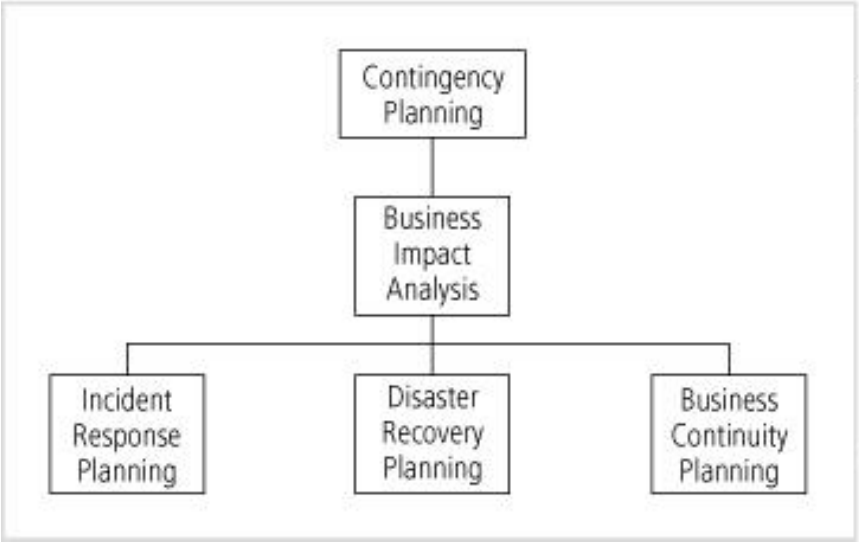
- Individuals and teams involved in CP:
  - **CPMT** - team that collects information about the organization and threats it faces, conducts the BIA, and develops contingency plans and should include:
    - Champion, project manager, team members
  - **Incident response team** - manages and executes the IR plan
  - **Disaster recovery team** - manages and executes the DR plan
  - **Business continuity team** - manages and executes the BC plan

Fundamentals of Contingency Planning Part 6

- In larger organizations these teams are distinct entities
  - With nonoverlapping memberships
- In smaller organizations the four teams may include overlapping groups of people
- CP shares certain characteristics with risk management and the SecSDLC methodology

Components of Contingency Planning

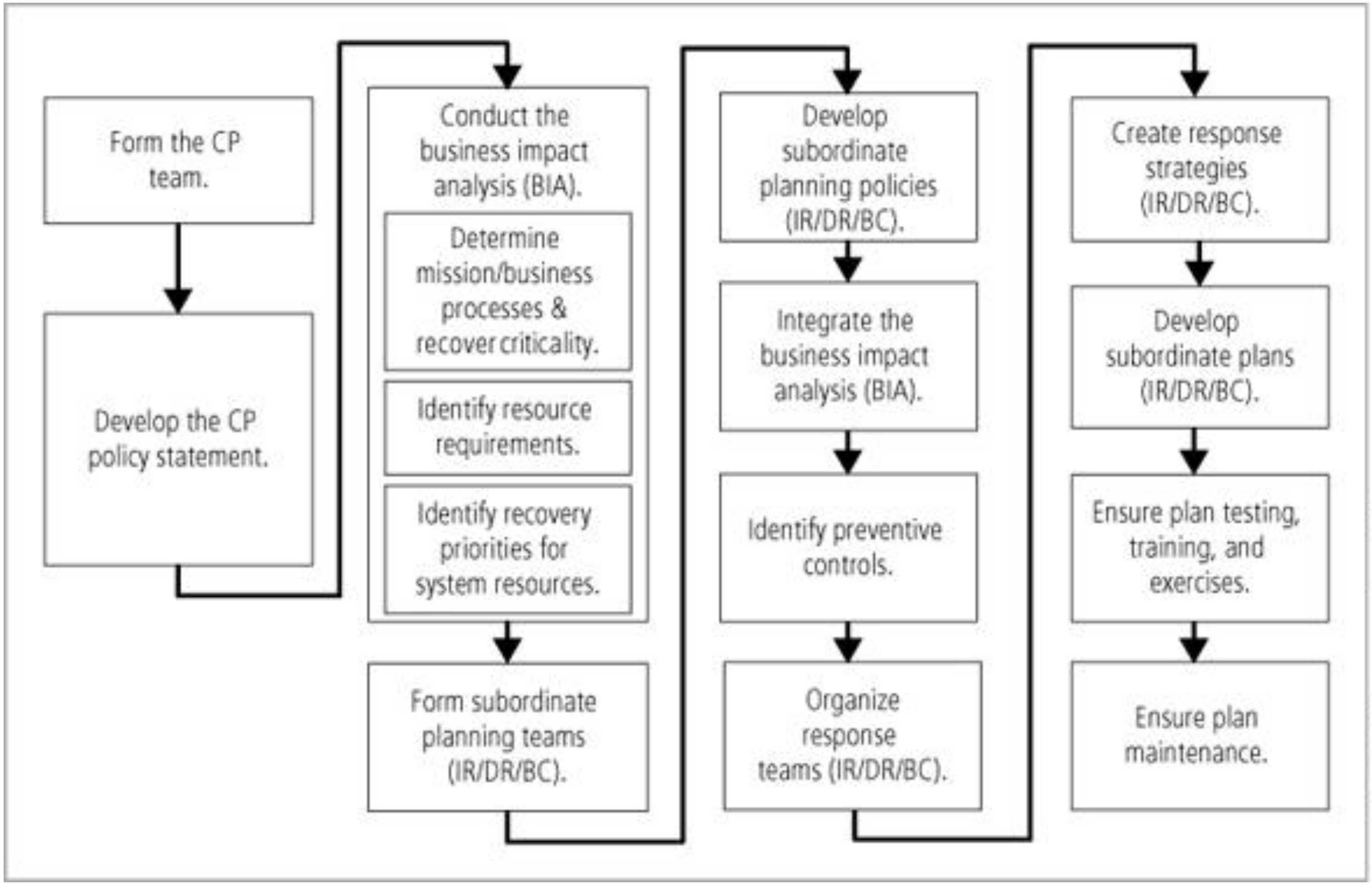
- CP major components:
  - BIA, IR plan, DR plan, BC plan


Contingency Planning
Business Impact Analysis
Incident Response Planning
Disaster Recovery Planning
Business Continuity Planning

Copyright © 2014 Cengage Learning®.

Figure 3-1 Contingency planning hierarchies

Figure 3-2 Contingency planning life cycle


Form the CP team.
Develop the CP policy statement.
Conduct the business impact analysis (BIA).
Determine mission/business processes & recover criticality.
Identify resource requirements.
Identify recovery priorities for system resources.
Form subordinate planning teams (IR/DR/BC).
Develop subordinate planning policies (IR/DR/BC).
Integrate the business impact analysis (BIA).
Identify preventive controls.
Organize response teams (IR/DR/BC).
Create response strategies (IR/DR/BC).
Develop subordinate plans (IR/DR/BC).
Ensure plan testing, training, and exercises.
Ensure plan maintenance.

Copyright © 2014 Cengage Learning®.

Business Impact Analysis Part 1

- BIA - serves as an investigation and assessment of the impact that various adverse events can have
- Difference between a BIA and risk management processes:
  - Risk management focuses on identifying the threats, vulnerabilities, and attacks to determine which controls can protect information
  - BIA assumes these controls have been bypassed, have failed, or have proved ineffective
    - That the attack succeeded

Business Impact Analysis Part 2

- BIA begins with the list of threats and vulnerabilities identified in the risk management process
- When undertaking the BIA, an organization should consider the following:
  - *Scope*
  - *Plan*
  - *Balance*
  - *Know the objective*
  - *Follow-up*

Business Impact Analysis Part 3

- The CPMT conducts the BIA in three stages:
    - Determine mission/business processes and recovery criticality
    - Identify resource requirements
    - Identify recovery priorities for system resources

Determine Mission/Business Processes and Recovery Criticality

- Each business department, unit, or division must be evaluated
  - To determine how important its functions are to the organization as a whole
- The term “mission/business process” \
  - Essentially describing a task performed by an organizational subunit in support of the overall organization’s mission

Determine Mission/Business Processes and Recovery Criticality (continued)

- information about business functions is a BIA questionnaire

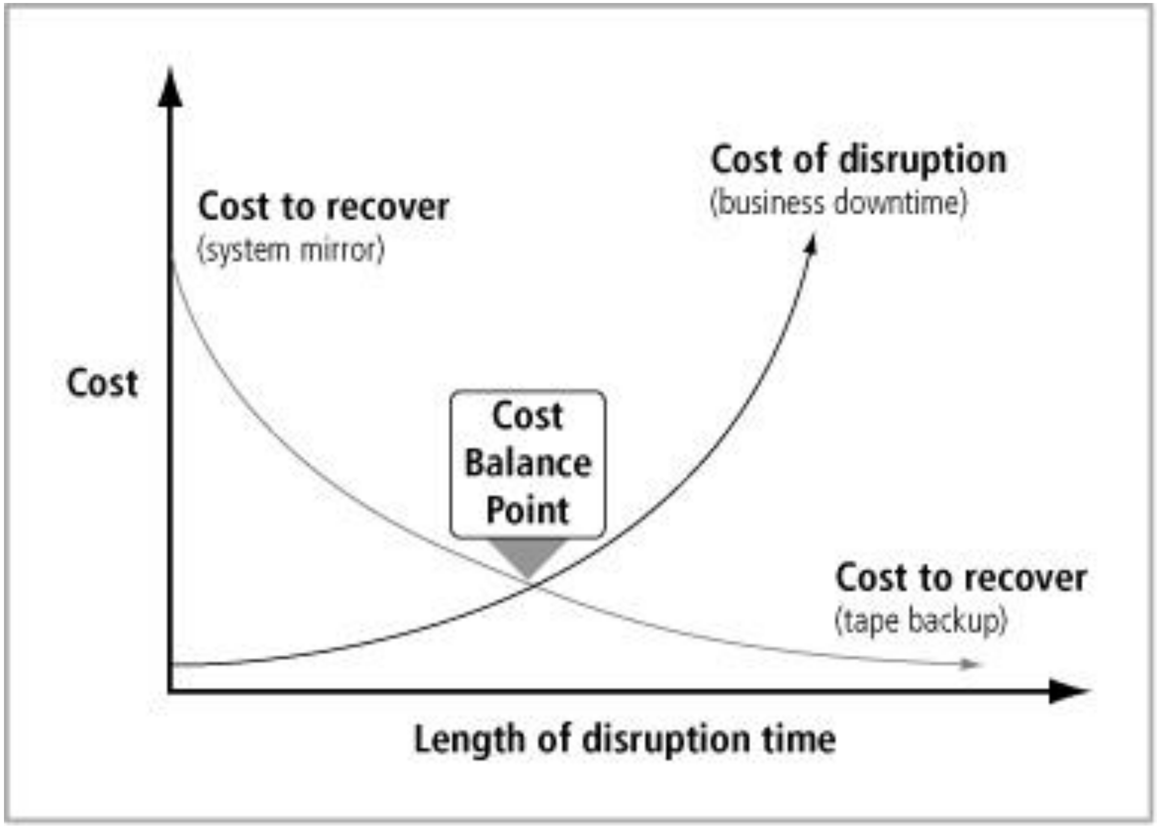
NIST Business Process and Recovery Criticality

- Key recovery measures:
  - Maximum Tolerable Downtime (MTD) - total amount of time the system owner is willing to accept for a mission/business process outage or disruption
  - Recovery time objective (RTO) - maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and processes
  - Recovery point objective (RPO) - point in time, prior to a disruption or system outage, to which mission/business process data can be recovered after an outage

NIST Business Process and Recovery Criticality (continued)

- **Work Recovery Time (WRT)** - amount of effort that is necessary to get the business function operational AFTER the technology element is recovered
- Total time needed to place the business function back in service must be shorter than the MTD

Figure 3-3 Cost balancing



Copyright © 2014 Cengage Learning®.

© Cengage Learning 2014

Identify Resource Requirements

- Once a prioritized list of mission and business processes have been created
  - Organizations need to determine resources required in order to recover those processes and assets
- Some business production-oriented processes require complex or expensive components to operate

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.

Identify System Recovery Priorities

- Prioritizing resources associated with the mission/business processes is the last stage of the BIA
  - Assign values to each resource listed from the previous stage

Contingency Planning Policies

- The CP team should develop the policy environment that will enable the BIA process

Incident Response

- **Incident response (IR) plan**: a detailed set of processes and procedures that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information and assets
- **Incident response planning (IRP)**: the preparation for such an event

Getting Started

- **Computer security incident response team (CSIRT)**: IR planning committee responsible for developing policy to:
  - Define the operations of the team
  - Articulate the organizational response to various types of incidents
  - Advise end users on how to contribute to the effective response of the organization

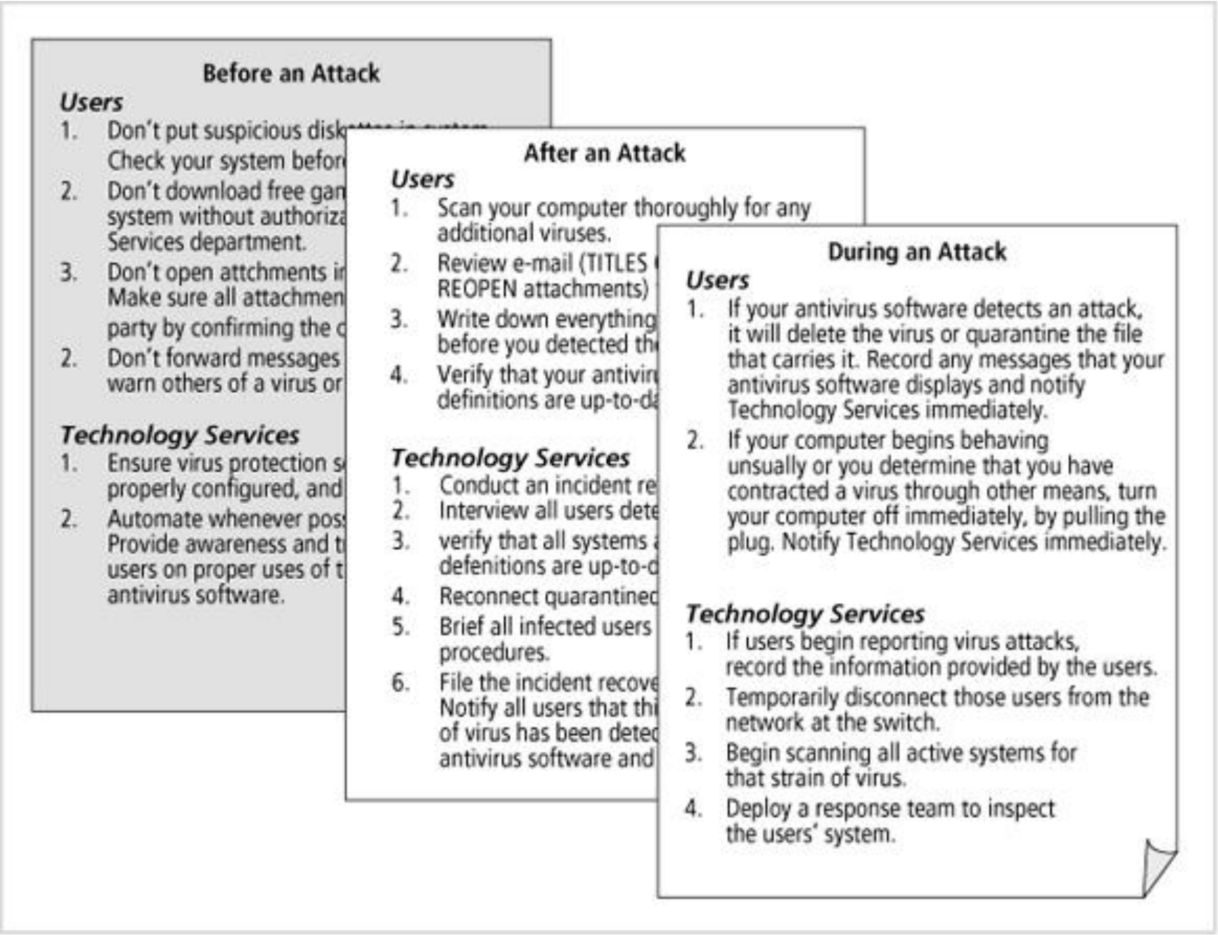
Incident Response Policy

- Key components of a typical IR policy:
  - Statement of management commitment
  - Purpose and objectives of the policy
  - Scope of the policy
  - Definition of InfoSec incidents and related terms
  - Organizational structure and definition of rules, responsibilities, and levels of authority
  - Prioritization or severity ratings of incidents
  - Performance measures
  - Reporting and contact forms

Planning to Respond

- The CP team should create three sets of incident-handling procedures:
  - *During the incident*
  - *After the incident*
  - *Before the incident*

Figure 3-4 Example of IRP incident-handling procedures



Before an Attack

Users

1. Don't put suspicious disk
   Check your system befor
2. Don't download free gan
   system without authoriza
   Services department.
3. Don't open attchments i
   Make sure all attachmen
   party by confirming the c
2. Don't forward messages
   warn others of a virus or

Technology Services

1. Ensure virus protection s
   properly configured, and
2. Automate whenever pos
   Provide awareness and t
   users on proper uses of t
   antivirus software.

After an Attack

Users

1. Scan your computer thoroughly for any additional viruses.
2. Review e-mail (TITLES
   REOPEN attachments)
3. Write down everything
   before you detected th
4. Verify that your antivir
   definitions are up-to-da

Technology Services

1. Conduct an incident re
2. Interview all users dete
3. verify that all systems
   defenitions are up-to-d
4. Reconnect quarantined
5. Brief all infected users
   procedures.
6. File the incident recove
   Notify all users that thi
   of virus has been detec
   antivirus software and

During an Attack

Users

1. If your antivirus software detects an attack, it will delete the virus or quarantine the file that carries it. Record any messages that your antivirus software displays and notify Technology Services immediately.
2. If your computer begins behaving unsually or you determine that you have contracted a virus through other means, turn your computer off immediately, by pulling the plug. Notify Technology Services immediately.

Technology Services

1. If users begin reporting virus attacks, record the information provided by the users.
2. Temporarily disconnect those users from the network at the switch.
3. Begin scanning all active systems for that strain of virus.
4. Deploy a response team to inspect the users' system.

Copyright © 2014 Cengage Learning®.

Detecting Incidents Part 1

- **Incident classification**: process of examining a possible incident, or **incident candidate**
- **Possible Indicators**:
  - *Presence of unfamiliar files*
  - *Presence or execution of unknown programs or processes*
  - *Unusual consumption of computing resources*
  - *Unusual system crashes*

Detecting Incidents Part 2

- **Probable Indicators**:
  - *Activities at unexpected times*
  - *Presence of new accounts*
  - *Reported attacks*
  - *Notification from an Intrusion Detection and Prevention System (IPDS)*
- **Definite Indicators**:
  - *Use of dormant accounts*
  - *Changes to logs*
  - *Presence of hacker tools*

Detecting Incidents Part 3

- **Definite Indicators** (cont'd):
  - *Notifications by partner or peer*
  - *Notification by hacker*
- **Occurrences of Actual Incidents**:
  - *Loss of availability*
  - *Loss of integrity*
  - *Loss of confidentiality*
  - *Violation of policy*
  - *Violation of law or regulation*

Responding to Incidents Part 1

- Once an incident has been confirmed and properly classified
  - The IR plan moves from the detection phase to the reaction phase
- An effective IR plan includes the following steps:
  - Notification of key personnel
  - Assignment of tasks
  - Documentation of the incident

Responding to Incidents Part 2

- **Alert roster**: a document containing contact information on individuals to be notified in the event of an actual incident
- **Alert message**: a description of the incident
- As soon as an incident has been confirmed and notification has begun
  - Documentation should begin
    - Should record the who, what, when, where, why, and how of each action taken during the incident

Responding to Incidents Part 3

- Incident containment strategies:
  - Disabling compromised user accounts
  - Reconfiguring a firewall to block problem traffic
  - Temporarily disabling the compromised process or service
  - Taking down the conduit application or server
    - Example: e-mail server
  - Stopping all computers and network devices

Recovering from Incidents

- Once the incident has been contained and system control has been regained
  - Incident recovery can begin
- First task is to inform the appropriate human resources
- CSIRT must assess the full extent of the damage
  - To determine what must be done to restore the systems

Recovering from Incidents (continued)

- Recovery process steps:
  - Identify vulnerabilities that allowed incident to occur
  - Address safeguards that failed to stop or limit the incident
  - Restore data from backups
  - Restore the services and process in use
  - Continuously monitor the system
  - Restore the confidence of the members of the organization’s communities of interest
- **After-action review (AAR):** detailed examination of the events that occurred

Law Enforcement Involvement

- When an incident violates civil or criminal law
  - The organization is responsible for notifying the proper authorities
- Selecting the appropriate law enforcement agency depends on the type of crime committed

Law Enforcement Involvement (continued)

- Disadvantages of involving law enforcement:
  - Possible loss of control over the chain of events following an incident
  - Organization may not hear about the case for weeks or even months due to heavy caseloads
  - Vital equipment may have to be taken as evidence
- Failure to notify law enforcement of a crime can lead to prosecution of the organization and its officers
  - As accessories to the crimes or for impeding the investigation

Disaster Recovery

- Disaster recovery planning (DRP): entails the preparation for and recovery from a disaster
  - Whether natural or human caused
- Disaster recovery (DR) plan: often activated when the IR plan no longer can handle the effective and efficient recovery from loss

Disaster Recovery (continued)

- Steps in the DRP process
  - – *Organize the DR team*
  - – *Develop the DR planning policy statement*
  - – *Review the BIA*
  - – *Identify preventative controls*
  - – *Create DR strategies*
  - – *Develop the DR plan document*
  - – *Ensure DR plan testing, training, and exercises*
  - – *Ensure DR plan maintenance*

Disaster Recovery Policy

- The DR policy should contain the following:
  - *Purpose*
  - *Scope*
  - *Roles and responsibilities*
  - *Resource requirements*
  - *Training requirements*
  - *Exercise and testing schedules*
  - *Plan maintenance schedule*
  - *Special considerations*

Disaster Classification

- A DR plan can classify disasters by:
  - Separating natural from human-made disasters
  - Speed of development

Planning to Recover

- Key elements CPMT must build into the DR plan:
  - *Clear delegation of roles and responsibilities*
  - *Execution of the alert roster and notification of key personnel*
  - *Clear establishment of priorities*
  - *Procedures for documentation of the disaster*
  - *Action steps to mitigate the impact of the disaster on the operations of the organization*
  - *Alternative implementations for the various system components, should primary versions be unavailable*

Planning to Recover (continued)

- An organization can protect its information and assist in getting information up and running quickly using
  - *backups* files

Responding to Disaster

- CPMT should incorporate a degree of flexibility into the plan
- If physical facilities are intact
  - DR team should begin restoration of systems and data to work toward full operational capability
- If facilities are destroyed
  - Alternative actions must be taken until new facilities can be acquired

Simple Disaster Recovery Plan

- DR plan has nine major sections:
  - *Name of agency*
  - *Date of completion or update of the plan*
  - *Agency staff to be called in the event of a disaster*
  - *Emergency services to be called*
  - *Locations of in-house emergency equipment*
  - *Sources of off-site equipment and supplies*
  - *Salvage priority list*
  - *Agency disaster recovery procedures*
  - *Follow-up assessment*

Business Continuity

- Business continuity planning (BCP) ensures that critical business functions can continue if a disaster occurs
  - Most properly managed by the CEO or COO
  - It is activated and executed concurrently with the DR plan when the disaster is major or long term

Business Continuity (continued)

- Steps to develop and maintain a BC program:
  - – Form the BC Team
  - – Develop the BC planning policy statement
  - – Review the BIA
  - – Identify preventative controls
  - – Create relocation strategies
  - – Develop the BC plan
  - – Ensure BC plan, testing, training, and exercises
  - – Ensure BC plan maintenance

Business Continuity Policy

- The BC policy contains the following key sections:
  - Purpose
  - Scope
  - Roles and responsibilities
  - Resource requirements
  - Training requirements
  - Exercise and testing schedules
  - Plan maintenance schedule
  - Special considerations

Continuity Strategies

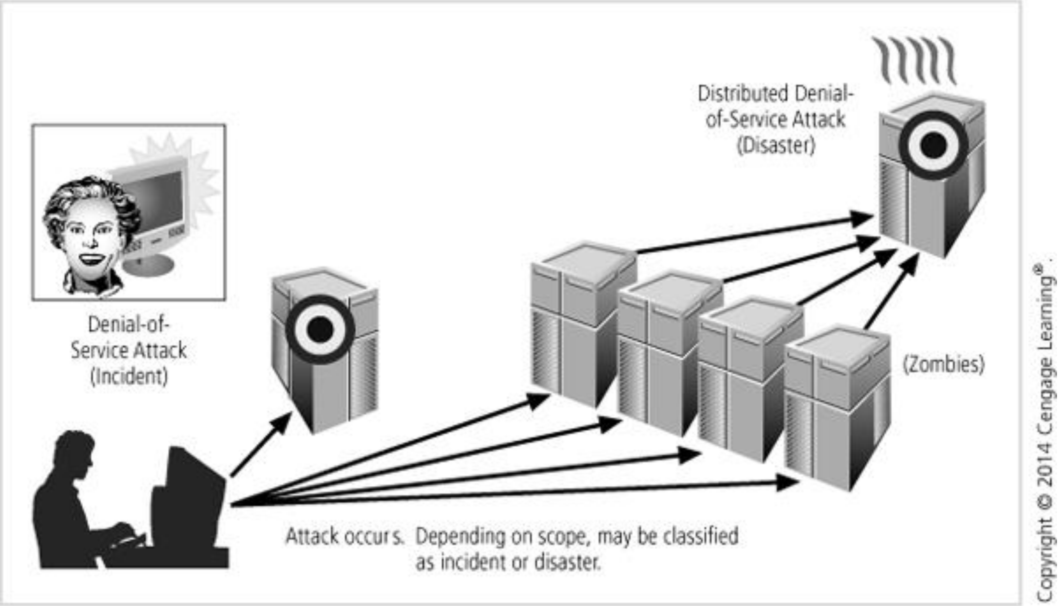
- The CPMT can choose from several strategies in its CP and BC planning
  - Determining factor is usually cost
- There are three types of usage strategies:
  - **Hot site** - a fully configured computer facility, with all services, communication links, and plant operations
  - **Warm site** - provides many of the same services as a hot site, but typically software applications are not installed and configured
  - **Cold site** - provides only rudimentary services and facilities

Continuity Strategies (continued)

- There are three strategies in which an organization can gain shared use of a facility when needed:
  - **Timeshare**- operates like one of the previous three sites but is leased in conjunction with a business partner
  - **Service bureau**- a service agency that provides a service for a fee
  - **Mutual agreement -** a contract between two organizations in which each party agrees to assist the other in the event of a disaster
- **Rolling mobile site**: configured in the payload area of a tractor/trailer

Timing and Sequence of CP Elements Part 1

- The IR plan focuses on immediate response
  - – But may give way to the DR and BC plan

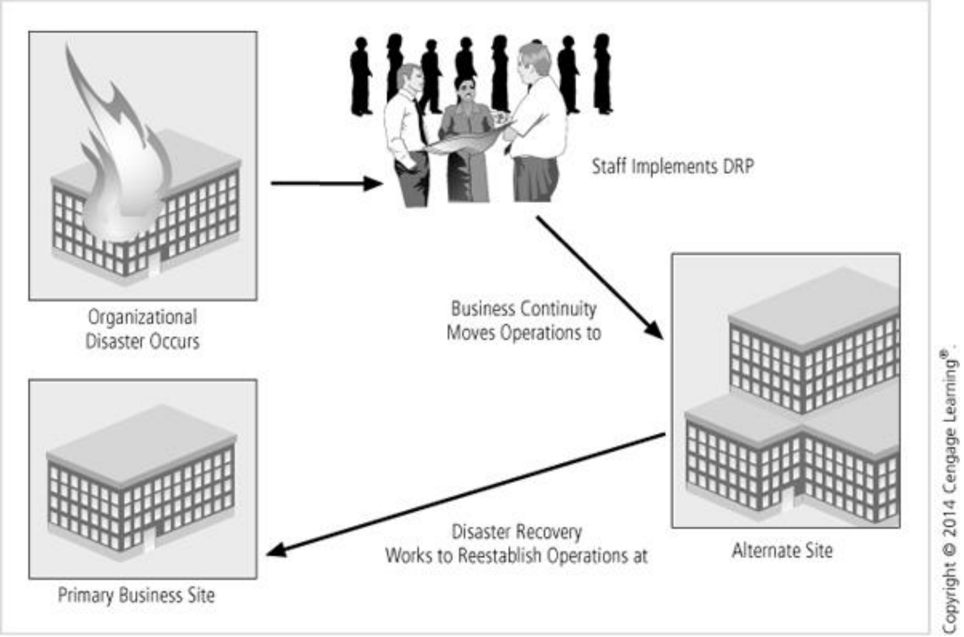

Distributed Denial-of-Service Attack (Disaster)
Denial-of-Service Attack (Incident)
(Zombies)
Attack occurs. Depending on scope, may be classified as incident or disaster.

Copyright © 2014 Cengage Learning®.

Figure 3-6 Incident response and disaster recovery

Timing and Sequence of CP Elements Part 2

- The BC plan occurs concurrently with the DR plan when the damage is long term

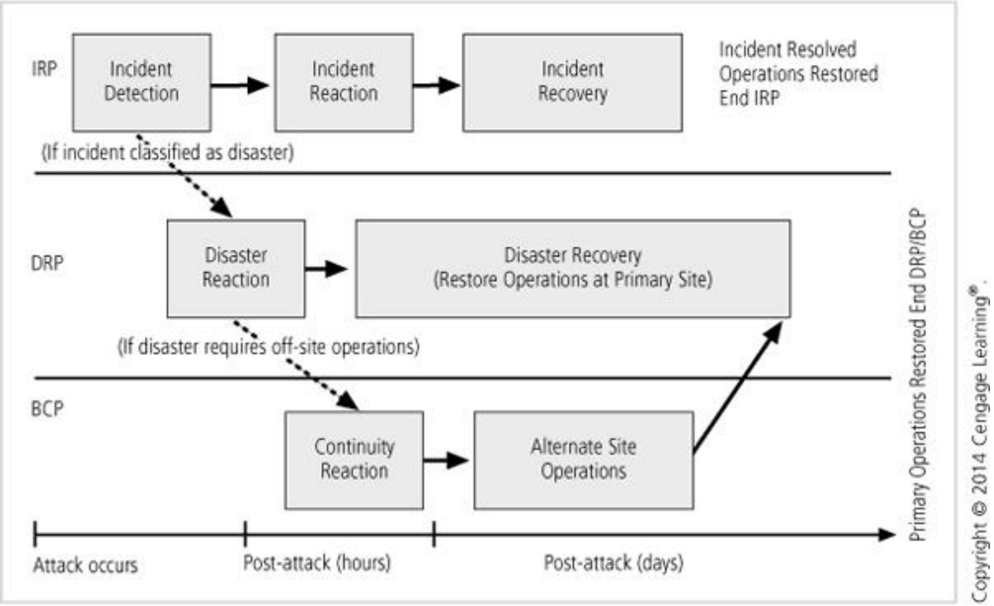

Staff Implements DRP
Organizational Disaster Occurs
Business Continuity Moves Operations to
Alternate Site
Disaster Recovery Works to Reestablish Operations at
Primary Business Site

Copyright © 2014 Cengage Learning®.

Figure 3-7 Disaster recovery and business continuity planning

Timing and Sequence of CP Elements Part 3

- The three planning components (IR, DR, and BC)
  - Each have a distinct place, role, and planning requirement



Copyright © 2014 Cengage Learning®.

Figure 3-8 Contingency planning implementation timeline

Crisis Management

- **Crisis management (CM):** the action steps affecting the people inside and outside the organization that are taken during and after a disaster

Summary Part 1

- Planning for unexpected events is usually the responsibility of managers from IT and InfoSec
- For a plan to be seen as valid, it must be sanctioned and supported by the general business community of interest
- Some organizations are required by law to have CP procedures in place at all times
- Contingency planning (CP) is made up of four major components: BIA, IR plan, DR plan, and BC plan
- Organizations can either create one unified plan or create three separate IR, DR, and BC plans

Summary Part 2

- Four teams of individuals are involved in CP and contingency operations: the CP team, IR team, DR team, and BC team
- The IR plan is a set of processes that plan for, detect, and resolve the effects of an unexpected event
- Three categories of incident indicators are used: possible, probable, and definite
- DR planning encompasses preparation for handing and recovering from a disaster
- DR plan must include crisis management

Summary Part 3

- BC planning ensures that critical business functions continue if a catastrophic incident or disaster occurs
- Because the DR and BC plans are closely related, most organizations prepare the two at the same time and may combine them into a single document called the business resumption (BR) plan
- All plans must be tested to identify vulnerabilities, faults, and inefficient processes