Lecture 3: Planning for Contingencies

Topic 3.1 Fundamentals of CP

Contingency Planning

- Planning for **unexpected** adverse events
  - When the use of technology is disrupted
  - When business operations come to a standstill
  - E.g., fire, break-in, storm, loss of key personnel, etc.
- To avoid or reduce the damage,
  - Proper planning for an unexpected event and the execution of such a plan are needed
  - Some (e.g., governmental agencies) are charged by law or mandate to have CP
  - Over 40% of businesses that don't have a disaster plan go out of business after a major loss [Hartford Insurance]

Lack of CP

- Example: what happens to small businesses after a networking disaster without proper CP?
- **Statistics:**
  - 70% of businesses that experience a major data loss are out of business within one year (DTI/ PricewaterhouseCoopers)
  - 94% of companies suffering from a catastrophic data loss do not survive (University of Texas)
  - 96% of all business workstations are not being backed up

    (Contingency Planning and Strategic Research Corporation)
  - 30% of small businesses will experience a natural disaster (NFIB)
  - 10% of small businesses will experience a major data loss as result of human error (NFIB)

Lack of CP

- Example: what happens to small businesses after a networking disaster without proper CP?
- **Cost** for restoring data [National Computer Security Association]
  - Takes 19 days and $17,000 to recreate 20 MB of lost sales/marketing data
  - Takes 21 days and $19,000 to recreate 20 MB of lost accounting data
  - Takes 42 days and $98,000 to recreate 20 MB of lost engineering data

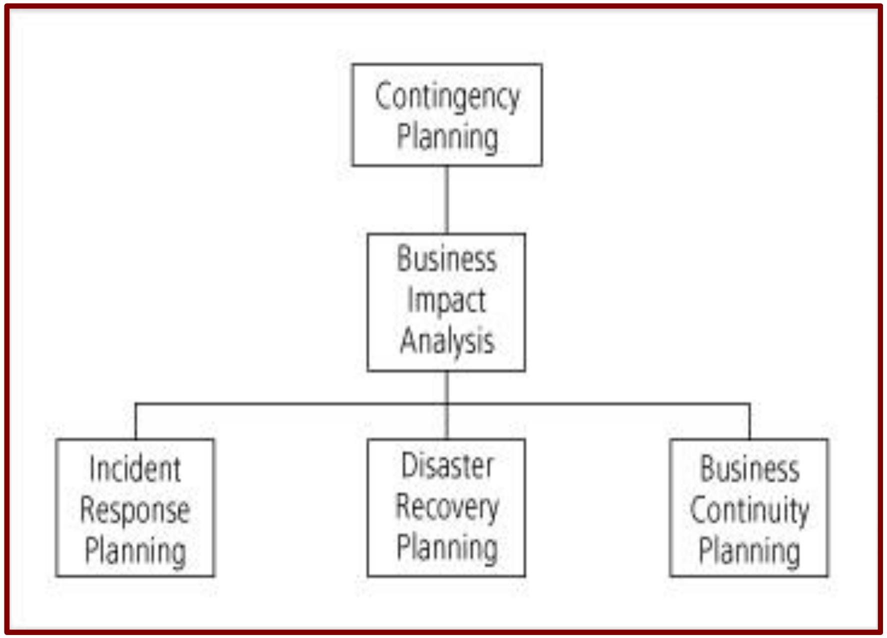
Lack of CP

- Example: what happens to small businesses after a networking disaster without proper CP?
- What should be considered in CP?
  - Data critical to business
  - Systems, applications,…critical to business
  - Process for backing up critical information assets
  - How much redundancy needed
  - Process for restoring critical information assets
  - Process for restoring systems
  - Categorized events and estimate risks and consequences
    - Power outage, loss of Internet access/phone service, …
  - Securing personnel

What is contingency planning?

- **Contingency planning** is the overall process of preparation for unexpected adverse events
  - To prepare for, detect, react to, and recover from events that threaten the security of information resources and assets
- **Main goal**:
  - To restore to normal modes of operation with *minimum cost and disruption* to normal business activities after an unexpected event, within a *reasonable period of time*

Contingency Planning Components


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

- **Business impact analysis (BIA)**
  - determines critical business functions and information systems
- **Incident response plan (IRP)**
  - focuses on immediate response
- **Disaster recovery plan (DRP)**
  - focuses on restoring operations at the primary site after disasters occur
- **Business continuity plan (BCP)**
  - facilitates establishment of operations at an alternate site

Contingency Planning Teams

- **CP management team (CPMT) conducts BIA**
  - Champion (e.g., COO or CEO)
  - Project manager (e.g., CISO or mid-level)
  - Team members (from different COIs)
- **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

Contingency Planning Components

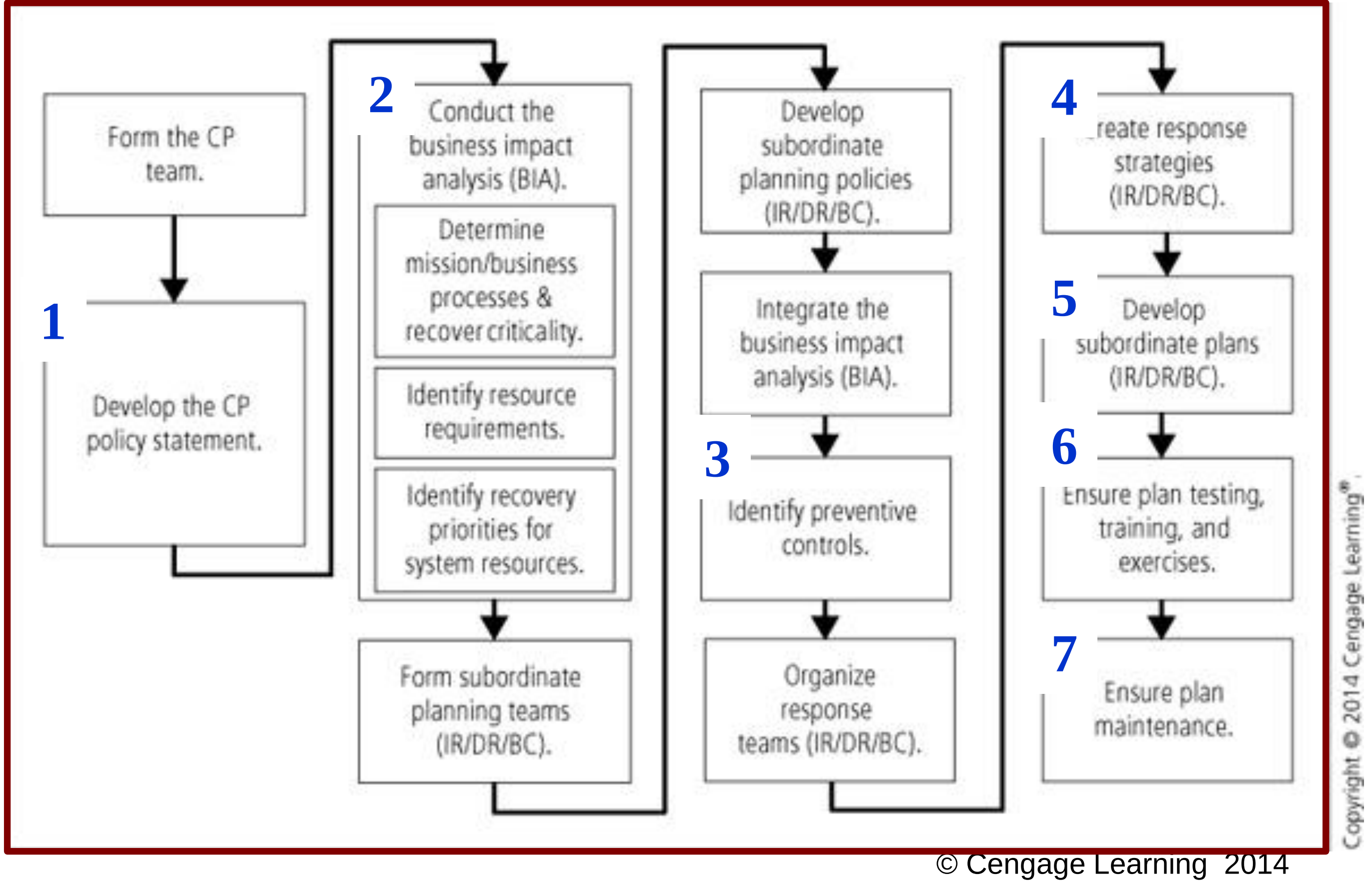
- IT and InfoSec managers can either create the four CP components
  - as one unified plan
  - or separately in conjunction with a set of interlocking procedures that enable continuity
- Typically,
  - Larger organizations create the CP components separately, with non-overlapping team memberships
  - Smaller organizations tend to adopt a one-plan method, and the four teams may include overlapping groups

Contingency Planning Procedures

- As recommended by **NIST**, **CPMT** begins developing a CP document in **7** steps:
  - Develop the CP policy statement
  - Conduct the BIA
  - Identify preventative controls
  - Create contingency strategies
  - Develop a contingency plan
  - Ensure plan testing, training, and exercises
  - Ensure plan maintenance

Contingency Planning Life Cycle

- 12-step contingency planning process based on NIST's 7 steps



Form the CP team.
1
Develop the CP policy statement.
2
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).
3
Identify preventive controls.
Organize response teams (IR/DR/BC).
4
Create response strategies (IR/DR/BC).
5
Develop subordinate plans (IR/DR/BC).
6
Ensure plan testing, training, and exercises.
7
Ensure plan maintenance.
Copyright © 2014 Cengage Learning®

Contingency Planning Policies

- The CP team should develop the policy environment that will enable the BIA process
  - Should provide specific policy environment that will enable the BIA process and provide guidance toward the creation of the IR, DR, and BC plans
- Each of the CP documents will include a policy similar in structure to all other policies used by the organization

Contingency Planning Policies

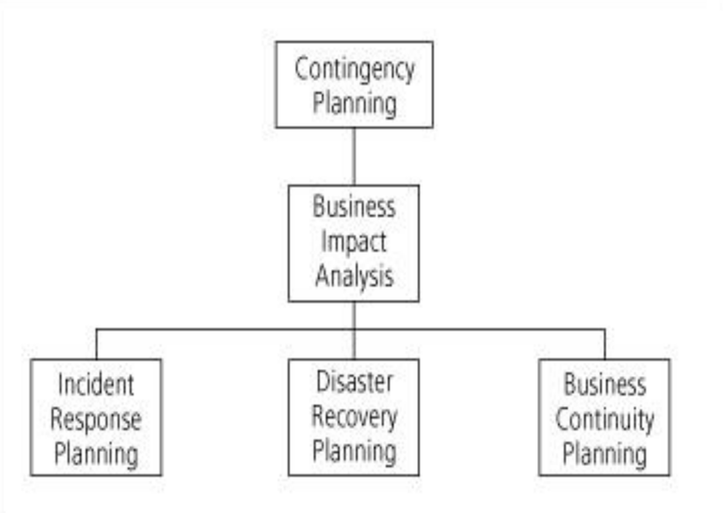
- **CP policy** should contain, at a minimum:
  - An introductory statement of philosophical perspective by senior management
  - A statement of the scope and purpose of the CP operations
  - A call for periodic risk assessment and BIA
  - A description of the CP major components
  - A call for, and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

to be continued

Contingency Planning Policy (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

Topic 3.2 CP Components


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

Business Impact Analysis

- BIA serves as an investigation and assessment of the impact that various adverse events can have on an organization
- ***BIA*** vs. ***Risk Management***
  - 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
    - Worst-scenario that the attack succeeded
    - How to respond to adverse event, minimize the damage, recover from the effects and return to normal operations

Business Impact Analysis

- BIA begins with the list of threats and vulnerabilities identified in the risk management process
  - Enhances the list by adding information needed to respond to the adversity
- When undertaking the BIA, an organization should consider the following:
  - Scope
  - Plan
  - Balance
  - Know the objective
  - Follow-up

Problem-based Learning

- NIST SP 800-34: Contingency Planning Guide for Federal Information Systems
  - Read sample template of BIA
- The CPMT conducts the BIA in three steps:
  - **Step 1:** Determine mission/business processes and recovery criticality
  - **Step 2:** Identify resource requirements
  - **Step 3:** Identify recovery priorities for system resource

Problem-based Learning

- **Step 1:** Determine Mission/Business Processes and Recovery Criticality
  - “mission/business process”
    - A task performed by an organization or organizational subunit in support of the overall organization’s mission
  - Each business department, unit, or division must be evaluated
    - Prioritize: IT and network >> HR
    - Focus on the selection of business functions necessary for operations to continue
  - How to do it?
    - Read BIA sample template

Problem-based Learning

- **Step 1:** Determine Mission/Business Processes and Recovery Criticality
  - BIA questionnaire: functional managers enters:
    - Information about their functions
    - Impacts the functions have on the business
    - Dependencies that exist for the functions from specific resources and outside service providers
  - Weighted factor analysis: a weighted analysis table can be useful in determining what business function is most critical
    - Identify types of impact categories (criterion)
    - Business functions scores × Criterion weights

Problem-based Learning

- **Step 1:** Determine Mission/Business Processes and Recovery Criticality
  - Key recovery measures describe how much assets need to recover within specific timeframe
  - 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

Problem-based Learning

- **Step 1:** Determine Mission/Business Processes and Recovery Criticality
  - Work Recovery Time (WRT) - amount of effort necessary to get the business function operational AFTER the technology element is recovered
    - Can be added to the RTO to determine the realistic amount of elapsed time before a business function is back in useful service
    - Total time needed to place the business function back in service must be shorter than the MTD
  - Balance the cost of system inoperability against the cost of recovery

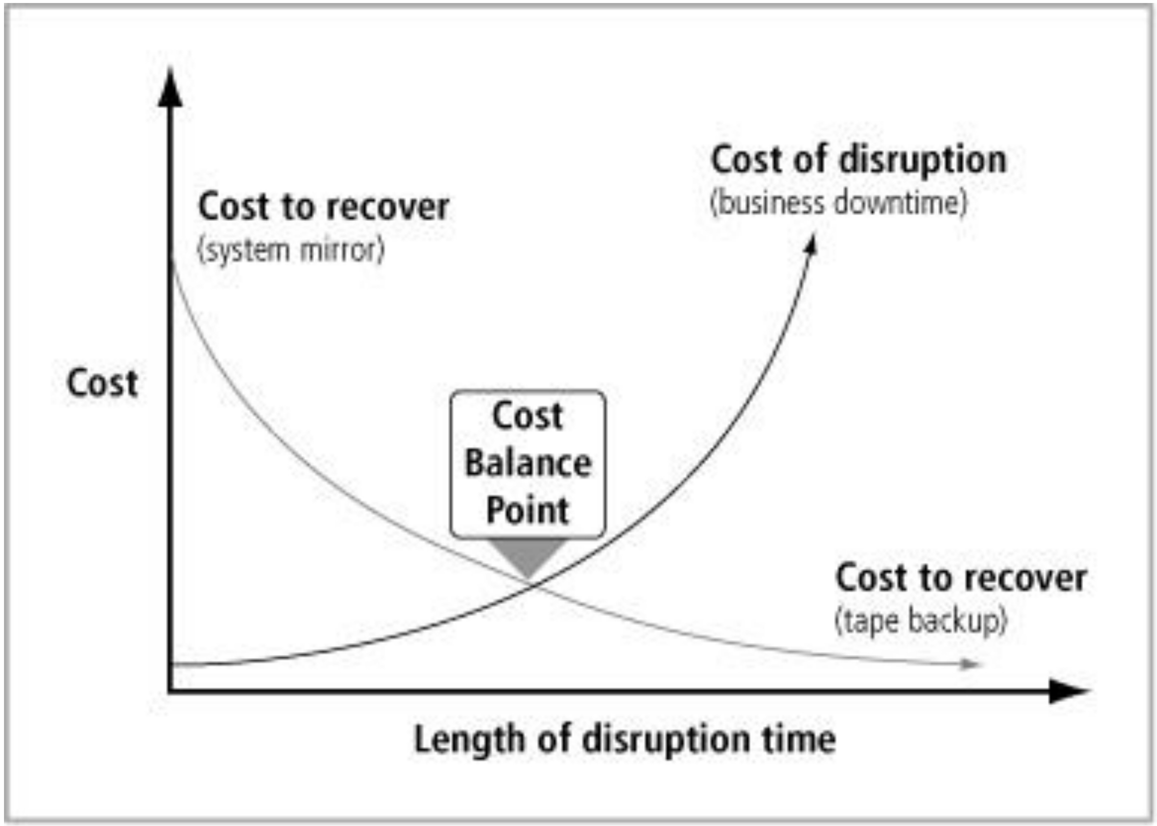
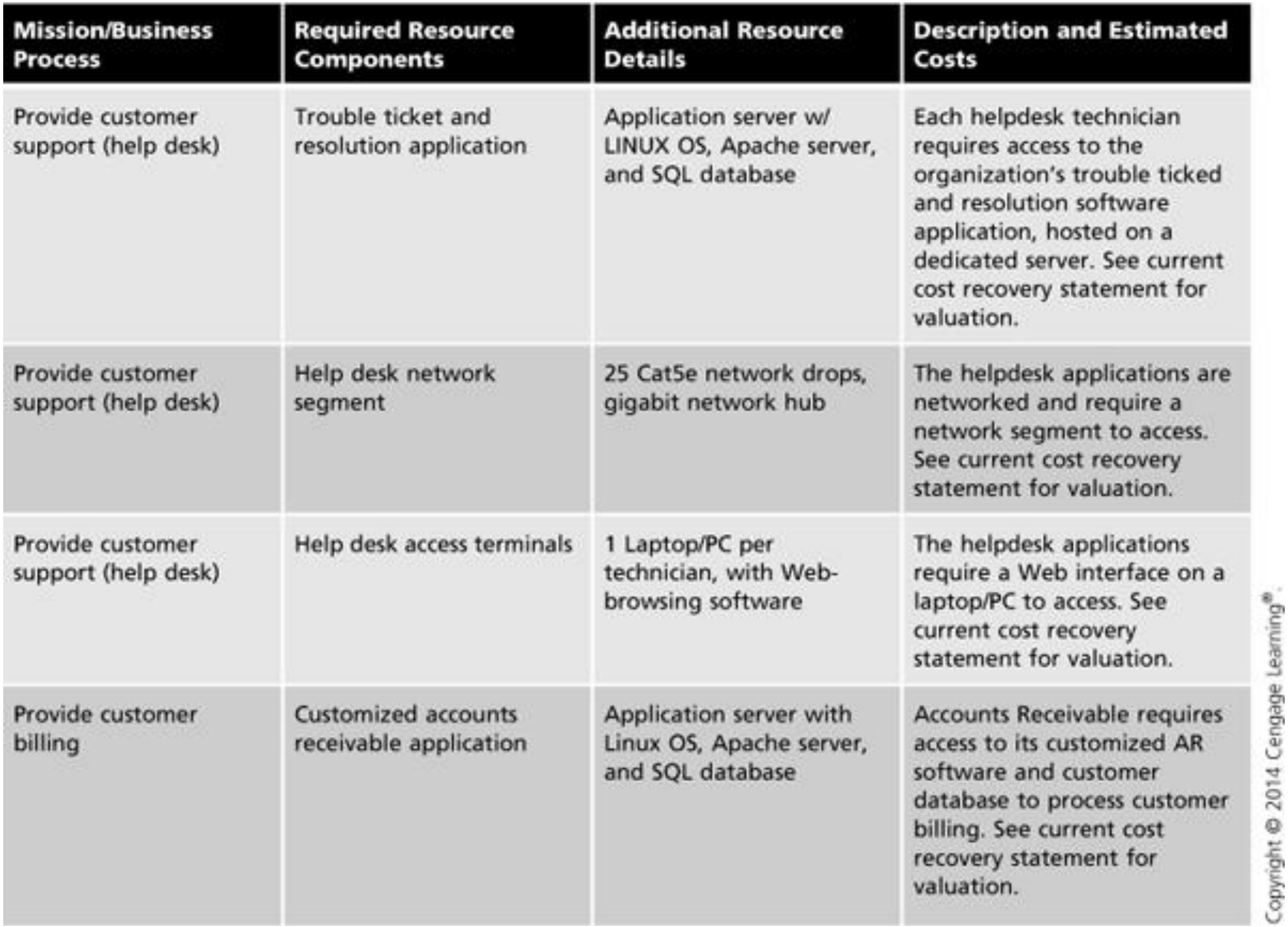


Figure 3-3 Cost balancing

Problem-based Learning

- **Step 2:** Identify Resource Requirements
  - Determine resources required in order to recover those processes and assets
    - Processing, storage, transmission costs for supporting data
  - Should be complete
  - Refer to System Security Plan for information



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.

Table 3-1 Example resource/components table

Problem-based Learning

- **Step 3:** Identify System Recovery Priorities
  - Assign values to each resource listed from the previous step
  - Create Priority Table
    - Determining RTO
  - In addition to weighted tables, a valuation and classification scale can be used to valuate resources
    - Examples:
      - Primary/Secondary/Tertiary
      - Critical/Very Important/Routine

Incident Response

- When a threat becomes a valid attack, it is classified as an info 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
- IR is a reactive measure, not a preventive one

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
- IR must be carefully planned and coordinated
  - Organizations heavily depend on the quick and efficient containment and resolution of incidents

Getting Started

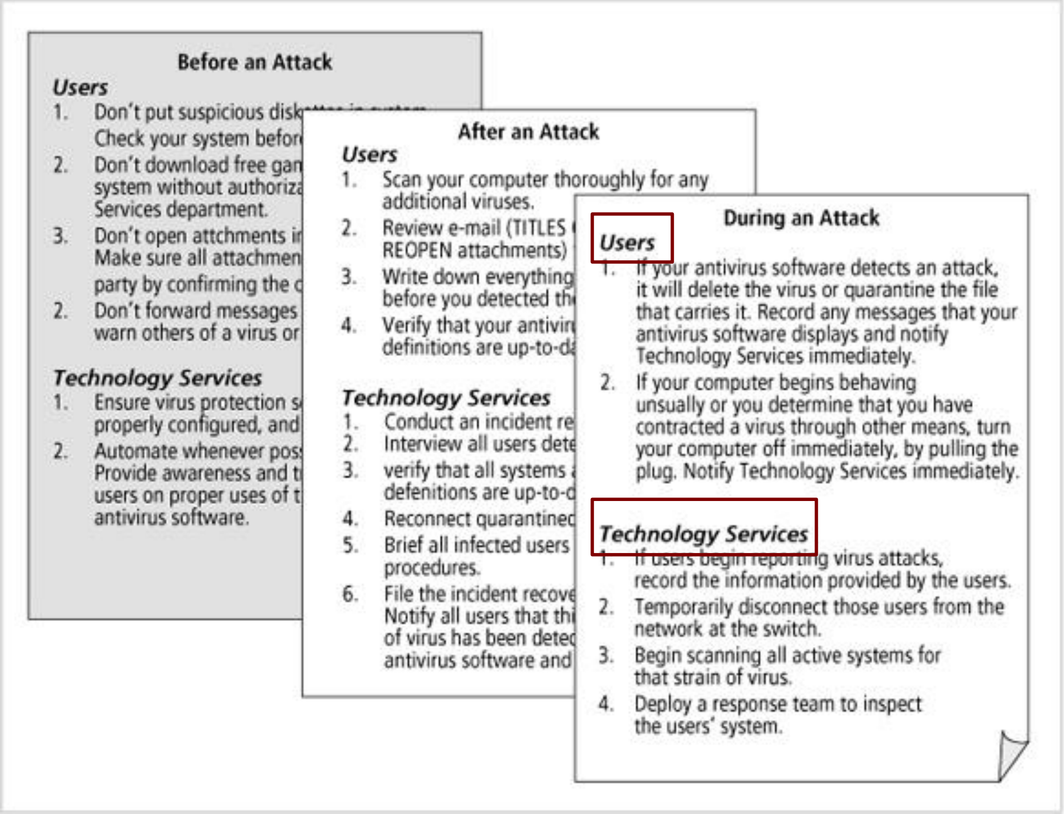
- Form **Computer security incident response team (CSIRT)**
- **IR planning committee** responsible for developing policy to:
  - Define the operations of the team
  - Articulate the organizational response to various types of incidents
  - Advise end users on how to contribute to the effective response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



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 ir
   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 deted
   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.

Incident Detection

- **Challenge**
  - Determining whether an event is routine system use or an actual incident
- **Incident classification**
  - Process of examining a possible incident, or incident candidate, and determining whether or not it constitutes actual incident
- **Ways to track and detect incident candidates**
  - Initial reports from end users, intrusion detection systems, host- and network-based virus detection software, and systems administrators
  - Careful training allows everyone to relay vital information to the IR team

Incident Indicators

- **Possible Indicators:**
  - Presence of unfamiliar files
  - Presence or execution of unknown programs or processes
  - Unusual consumption of computing resources
  - Unusual system crashes
- **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
  - Notifications by hack or partner

Detecting Incidents

- Problem-based Learning
  - Read Incident Response Plan of *American Institute of Certified Public Accountants, Inc*
- Answer the following questions
  - What incidents are defined?
  - What are the defined indicators?

Detecting Incidents

- **Occurrences of actual incidents**:
  - Loss of availability
  - Loss of integrity
  - Loss of confidentiality
  - Violation of policy
  - Violation of law or regulation

Responding to Incidents

- Once an incident has been confirmed and properly classified
  - The IR plan moves from the detection phase to the reaction phase
  - In reaction phase, action steps taken by the IR team and others must occur quickly and may occur concurrently
- An effective IR plan includes the following steps:
  - Notification of key personnel
  - Assignment of tasks
  - Documentation of the incident

Notification of Key Personnel

- Notify right people as soon as incident is declared
- **Alert roster:** a document containing contact information on individuals to be notified in the event of an actual incident
- **Alert message:** scripted description of incident
  - Notifies each responder which portion of the IR plan to implement
- **Other key personnel:**
  - must also be notified only after incident has been confirmed,
  - before media or other external sources learn of it

Documenting an Incident

- Documentation should begin
  - As soon as an incident has been confirmed and notification has begun
  - Record the who, what, when, where, why, and how of each action taken during the incident
    - Serves as a case study after the fact to determine if right actions were taken and if they were effective
    - Can also prove the organization did everything possible to deter the spread of the incident
- Problem-based Learning
  - Read Incident Response Plan of *American Institute of Certified Public Accountants, Inc*
  - Who and what to be documented?

Incident Containment Strategies

- Essential task of IR is to stop the incident or contain its impact
- By means of incident containment **strategies**:
  - Disconnect affected communication circuits
  - Dynamically apply filtering rules to limit certain types of network access
  - 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 (e-mail server)
  - Stopping all computers and network devices

Incident Escalation

- An incident may increase in scope or severity to the point that the IRP cannot adequately contain the incident
- Each organization will have to determine, during the business impact analysis, the point at which the *incident becomes a disaster*
- The organization must also document when to involve outside response

Recovering from Incidents

- Incident recovery phase begins
  - Once the incident has been contained and system control has been regained
  - 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
- **Incident damage assessment**
  - Determination of the scope of the breach of confidentiality, integrity, and availability of information and assets
  - Document damage
  - Preserve evidence - in case the incident is part of a crime or results in a civil action

Recovering from Incidents

- **Recovery process steps:**
  - Identify vulnerabilities that allowed incident to occur
  - Address safeguards that failed to stop or limit the incident
  - Evaluate monitoring capabilities
  - 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, from first detection to final recovery

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
- Involving law enforcement has both advantages and disadvantages
  - Usually better equipped to process evidence, handle warrants and subpoenas, obtain statements, affidavits, and other required documents
  - Involvement can result in loss of control of chain of events following an incident, lost access to equipment, slow processing

Disaster Recovery

- **Disaster recovery planning (DRP):** preparation for and recovery from a disaster, whether natural or human caused
  - Key role of DRP is to define *how to reestablish operations at location where organization is usually located*
- An incident is a disaster when:
  - organization is unable to contain or control the impact of an incident, or
  - level of damage or destruction from incident is so severe, the organization is unable to quickly recover
  - For example: a malicious program evades containment actions and infects many or most of an organization's systems and its ability to function

Disaster Recovery

- Steps in the DRP process (similar?)
  - 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:
  - Separating natural from human-made disasters
  - Speed of development
    - **Rapid-onset disasters**
      - Occur suddenly, with little warning
      - E.g., earthquake, floods, storms, tornadoes
    - **Slow-onset disasters**
      - Occur over time and gradually degrade the capacity of an organization to withstand their effects
      - E.g., droughts, famines, enviromental degradation, deforestation, pest infestation

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

- **Options** for protecting organizations' information and assist:
  - *Traditional data backups*
    - can use a combination of on-site and off-site tape-drive or hard-drive methods
  - *Electronic vaulting*
    - bulk batch-transfer of data to an off-site facility
  - *Remote journaling*
    - transferring live transactions to an off-site facility
  - *Database shadowing*
    - duplicates online transaction data with duplicate databases
    - combines electronic vaulting with remote journaling

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
- When disaster threatens the viability of an organization at the primary site, the DR process *becomes a business continuity process*

Simple Disaster Recovery Plan

- DR plan has nine major sections:
  1. Name of agency
  2. Date of completion or update of the plan
     - also date of the most recent test
  3. Agency staff to be called in the event of a disaster
  4. Emergency services to be called
  5. Locations of in-house emergency equipment
  6. Sources of off-site equipment and supplies
  7. Salvage priority list
  8. Agency disaster recovery procedures
  9. 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
- If a disaster renders the current business location unusable
  - There must be a plan to allow the business to continue to function

Business Continuity

- Steps to develop and maintain a BC program (similar?)
  - 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

- 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

- IR plan focuses on immediate response
- Give way to the DR and BC plan

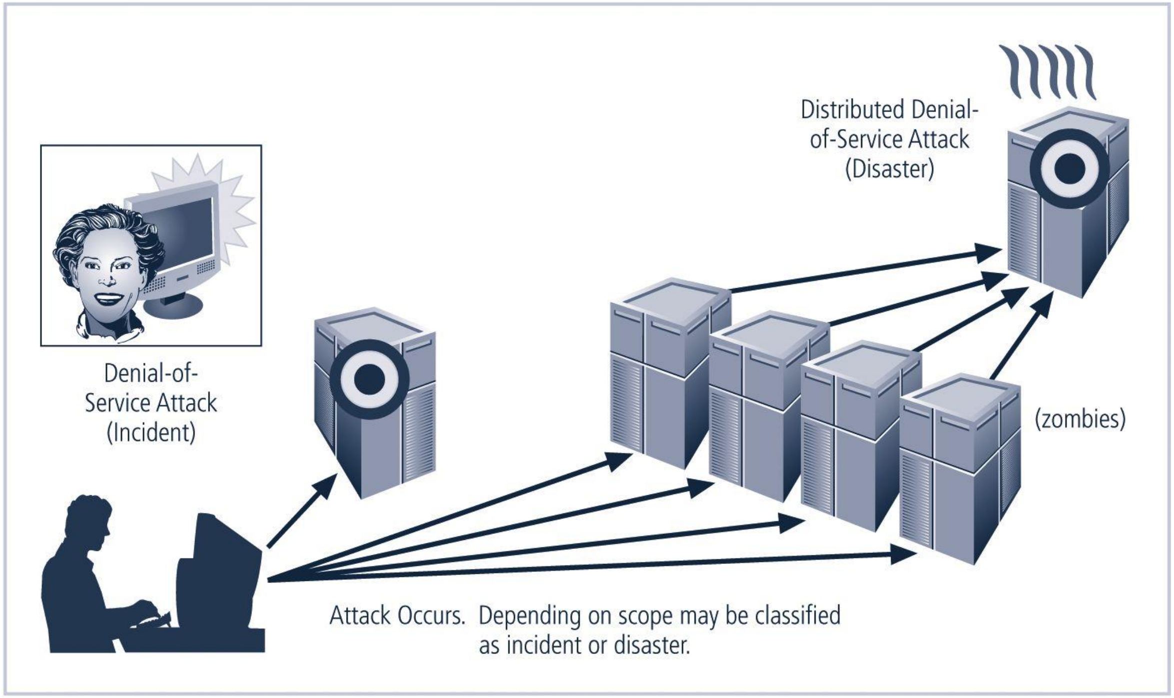

Distributed Denial-of-Service Attack (Disaster)
Denial-of-Service Attack (Incident)
(zombies)
Attack Occurs. Depending on scope may be classified as incident or disaster.

FIGURE 3-3 Incident Response and Disaster Recovery

Timing and Sequence of CP Elements

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

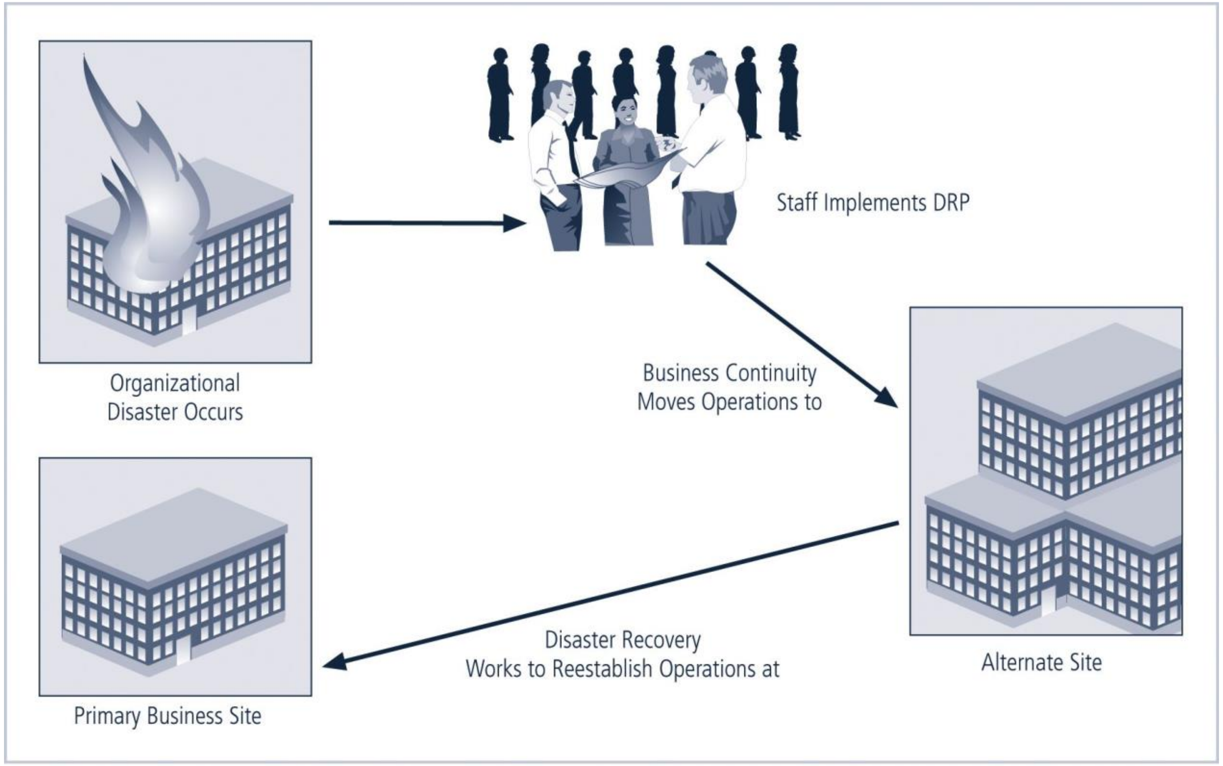

Staff Implements DRP
Organizational Disaster Occurs
Business Continuity Moves Operations to
Alternate Site
Disaster Recovery Works to Reestablish Operations at
Primary Business Site

FIGURE 3-4 Disaster Recovery and Business Continuity Planning

Timing and Sequence of CP Elements

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

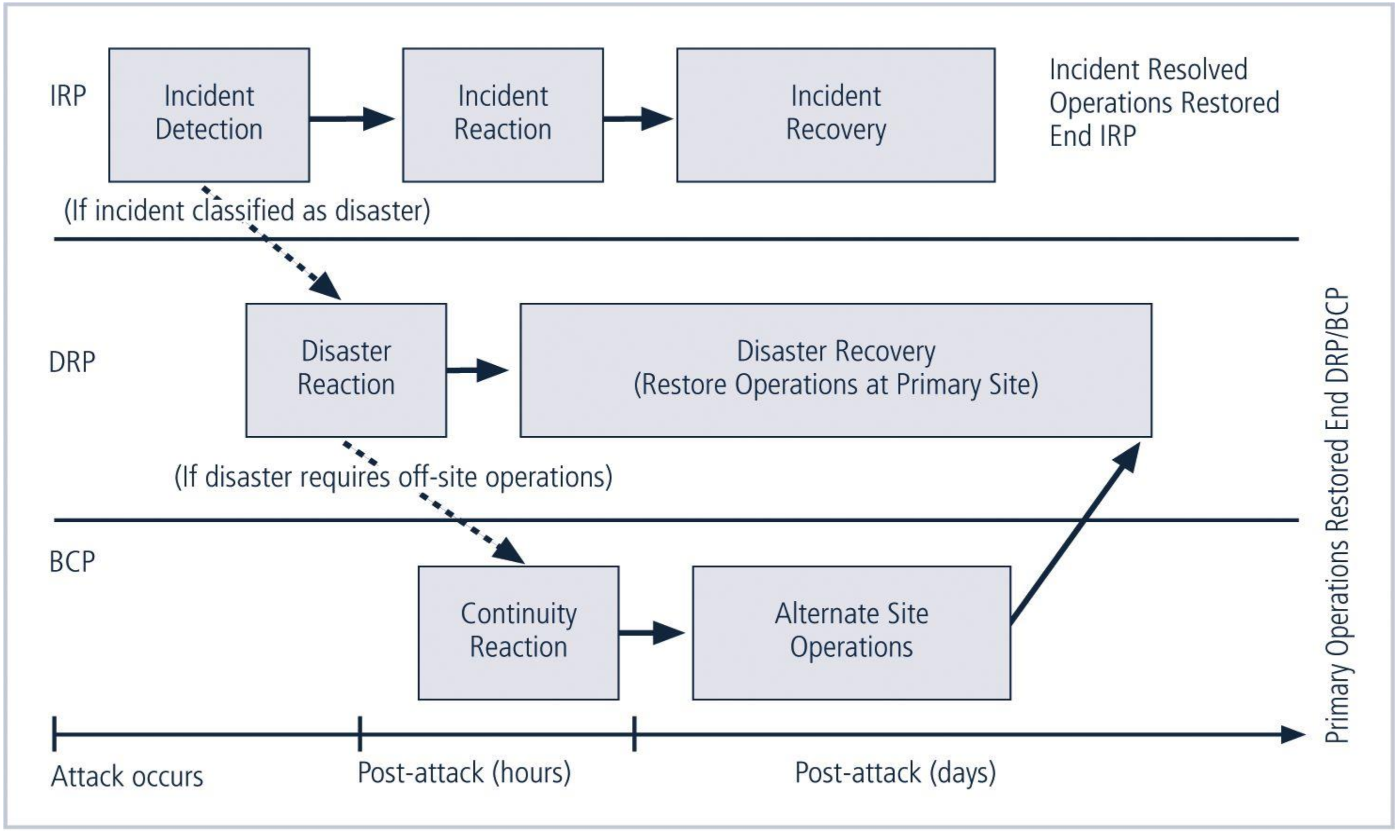


FIGURE 3-5 Contingency Plan Implementation Timeline

Crisis Management

- **Crisis management (CM):** the action steps affecting the people inside and outside the organization that are taken during and after a disaster
  - May be integrated into the DR plan or a crisis management team may be created
- A **crisis management team**'s roles:
  - Supporting personnel and loved ones
  - Keeping the public informed about the event
  - Communicating with major customers, suppliers, regulatory agencies, industry organizations, the media, and other interested parties

Crisis Management

- Crisis management team should establish a base of operations or command center near the site of the disaster
  - Should include individuals from all functional areas of the organization
- CMT primary responsibilities:
  - Verifying personnel status
  - Activating the alert roster

Business Resumption

- **Business resumption plan (BR plan):** combining the DR and BC plan into a single planning document
  - Must be able to support the reestablishment of operations at two different locations
    - One immediately at an alternate site
    - One eventually back at the primary site
- A single planning team can develop the BR plan
  - Execution of the plan requires separate execution teams

Testing Contingency Plans

- Few plans are executable as written so they must be tested to identify vulnerabilities and faults
- Five strategies can be used to test contingency plans:
  1. **Desk check** - distributing copies of the appropriate plans to all individuals with assigned incident roles
  2. **Structured walk-through** - all involved individuals walk through the steps they would take during an event
  3. **Simulation** - each person works individually to simulate the performance of each task

Testing Contingency Plans

- Few plans are executable as written so they must be tested to identify vulnerabilities and faults
- Five strategies can be used to test contingency plans:

4. **Parallel testing** - individuals act as if an actual incident occurred and begin performing their required tasks and executing procedures
   - Without interrupting normal business operations
5. **Full interruption** - individuals follow each and every procedure
   - Including interruption of service, restoration of data from backups, and notification of appropriate individuals