# TEL2813/IS2820
# Security Management

## Contingency Planning

Jan 22, 2008

# Introduction

- Planning for the unexpected event,
  - when the use of technology is disrupted and business operations come close to a standstill
- Procedures are required that will permit the organization to
  - continue essential functions if information technology support is interrupted
- Over 40% of businesses that don't have a disaster plan go out of business after a major loss

# What Is Contingency Planning?

- Contingency planning (CP)
  - Overall planning for unexpected events
  - 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

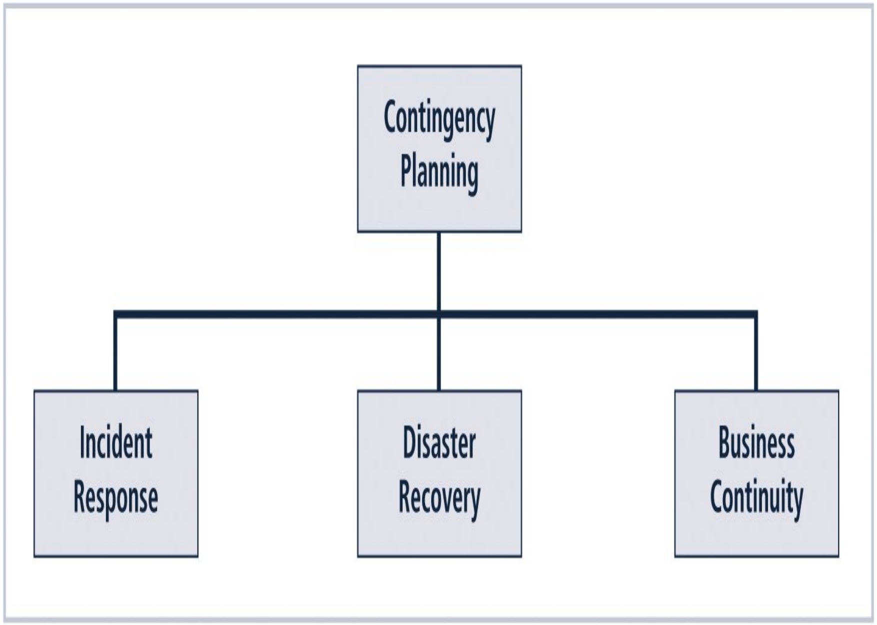


FIGURE 3-1 Contingency Planning Hierarchies

- Incident response (IRP)
  - focuses on immediate response
- Disaster recovery (DRP)
  - focuses on restoring operations at the primary site after disasters occur
- Business continuity (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

# CP Operations

- Four teams are involved in contingency planning and contingency operations:
  - CP team
  - Incident recovery (IR) team
  - Disaster recovery (DR) team
  - Business continuity plan (BC) team

# Contingency Planning

- NIST describes the need for this type of planning

  “*These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated*.”

# 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 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-handling procedures

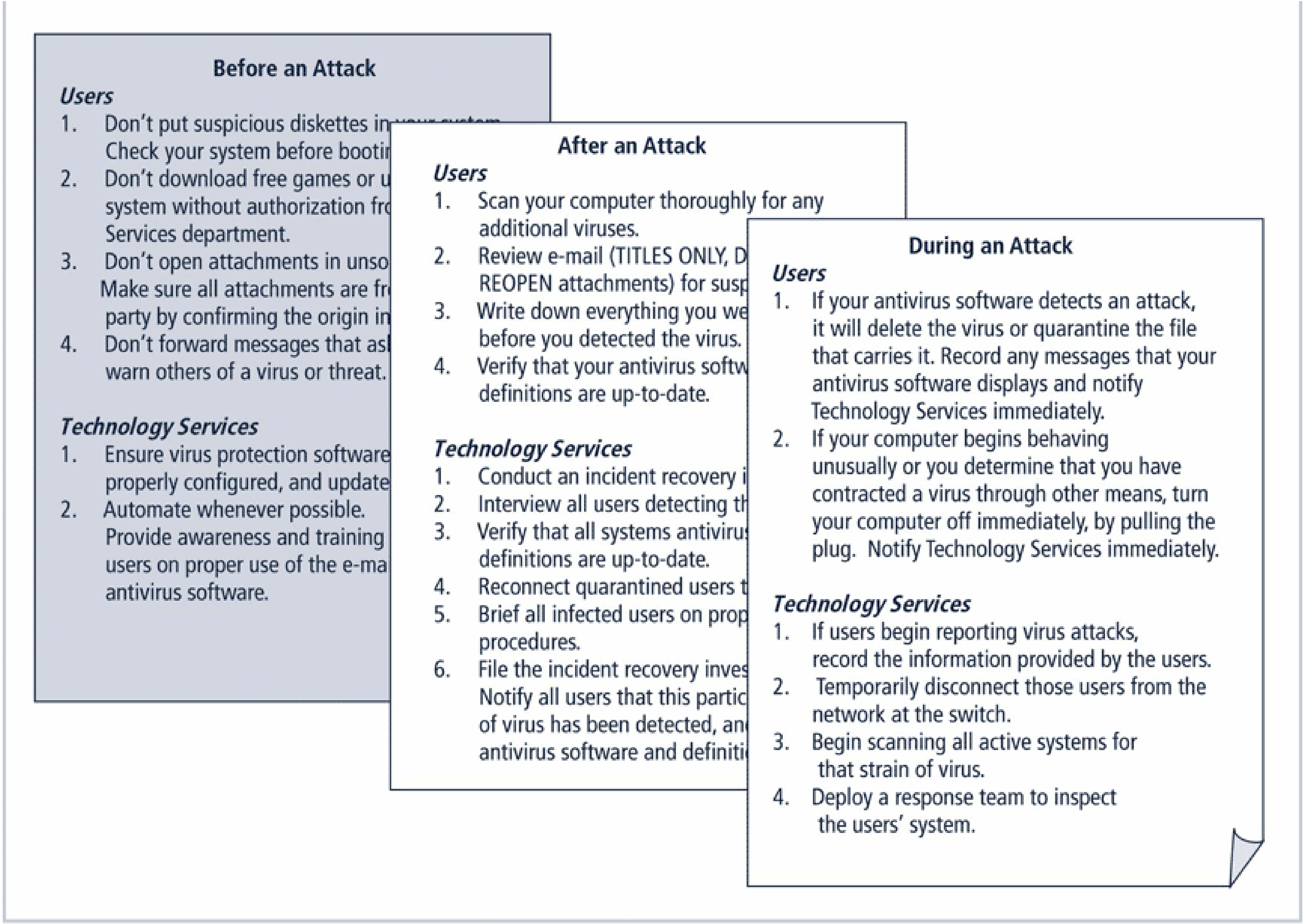
- During Incident
  - Planners develop and document the procedures that must be performed during the incident
  - These procedures are grouped and assigned to various roles
  - Planning committee drafts a set of function-specific procedures

# Incident-handling procedures

- After the Incident
  - planners develop and document the procedures that must be performed immediately after the incident has ceased
  - Separate functional areas may develop different procedures

# Incident-handling procedures

- Before the Incident
  - Planners draft a third set of procedures, those tasks that must be performed in advance of the incident
- Include:
  - Details of data backup schedules
  - Disaster recovery preparation
  - Training schedules
  - Testing plans
  - Copies of service agreements
  - Business continuity plans



Before an Attack

*Users*

1. Don't put suspicious diskettes in your system. Check your system before bootir
2. Don't download free games or u system without authorization fr Services department.
3. Don't open attachments in unso Make sure all attachments are fr party by confirming the origin in
4. Don't forward messages that as warn others of a virus or threat.

*Technology Services*

1. Ensure virus protection software properly configured, and update
2. Automate whenever possible. Provide awareness and training users on proper use of the e-ma antivirus software.

After an Attack

*Users*

1. Scan your computer thoroughly for any additional viruses.
2. Review e-mail (TITLES ONLY, D REOPEN attachments) for susp
3. Write down everything you we before you detected the virus.
4. Verify that your antivirus softw definitions are up-to-date.

*Technology Services*

1. Conduct an incident recovery i
2. Interview all users detecting th
3. Verify that all systems antiviru definitions are up-to-date.
4. Reconnect quarantined users t
5. Brief all infected users on prop procedures.
6. File the incident recovery inves Notify all users that this partic of virus has been detected, an antivirus software and definiti

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 unusually 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.

**FIGURE 3-2** Incident Response Planning

# Preparing to Plan

- Planning requires detailed understanding of
  - information systems and threats they face
- IR planning team
  - develops pre-defined responses that guide users through steps needed to respond to an incident
- Pre-defining incident responses enables rapid reaction without confusion or wasted time and effort

# Preparing to Plan (Continued)

- IR team consists of
  - professionals capable of handling information systems and functional areas affected by an incident
- Each member of the IR team must:
  - Know his or her specific role
  - Work in concert with each other
  - Execute the objectives of the IRP

# Incident Detection

- Challenge
  - determining whether an event is routine system use or an actual incident
- Incident classification:
  - process of examining a possible incident 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

- Probable 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 IDS
- Definite Indicators
  - Use of dormant accounts
  - Changes to logs
  - Presence of hacker tools
  - 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

# Incident Response

- Once an actual incident has been confirmed and properly classified,
  - the IR team moves from detection phase to reaction phase
- In the incident response phase,
  - Action steps taken by the IR team and others must occur quickly and may occur concurrently

# Notification of Key Personnel

- Notify right people as soon as incident is declared,
- Alert roster:
  - contact information of individuals to be notified in the event of actual incident either sequentially or hierarchically
- Alert message:
  - scripted description of incident
- 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

- While the notification process is underway, the team should begin documentation
    - Record the who, what, when, where, why and how of each action taken while the incident is occurring
        - 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

# Incident Containment Strategies

- Essential task of IR is to stop the incident or contain its impact
  - Incident containment strategies focus on two tasks:
    - Stopping the incident
    - Recovering control of the systems

# Incident Containment Strategies

- IR team can stop the incident and attempt to recover control by means of several strategies:
  - Disconnect affected communication circuits
  - Dynamically apply filtering rules to limit certain types of network access
  - Disable compromised user accounts
  - Reconfigure firewalls to block problem traffic
  - Temporarily disable compromised process/service
  - Take down conduit application or server
  - Stop 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

# Initiating Incident Recovery

- Incident recovery
  - After the incident has been contained, and system control regained
- IR team must assess full extent of damage in order to determine what must be done to restore systems
- Incident damage assessment
  - determination of the scope of the breach of confidentiality, integrity, and availability of information/information assets
  - Document damage and
  - Preserve evidence - in case the incident is part of a crime or results in a civil action

# Recovery Process

- Once the extent of the damage has been determined, the recovery process begins:
  - Identify and resolve vulnerabilities that allowed incident to occur and spread
  - Address, install, and replace/upgrade safeguards that failed to stop or limit the incident, or were missing from system in the first place
  - Evaluate monitoring capabilities (if present) to improve detection and reporting methods, or install new monitoring capabilities

# Recovery Process (Continued)

- Restore data from backups as needed
- Restore services and processes in use where compromised (and interrupted) services and processes must be examined, cleaned, and then restored
- Continuously monitor system
- Restore the confidence of the members of the organization’s communities of interest

# After Action Review

- Before returning to routine duties, the IR team must conduct an after-action review, or AAR
  - AAR: detailed examination of events that occurred
- All team members:
  - Review their actions during the incident
  - Identify areas where the IR plan worked, didn’t work, or should improve

# Law Enforcement Involvement

- When incident violates civil or criminal law,
  - it is organization's responsibility to notify proper authorities
  - Selecting appropriate law enforcement agency
    - depends on the type of crime committed: Federal, State, or Local
- Involving law enforcement has both advantages and disadvantages:
  - Usually much better equipped at processing evidence, obtaining statements from witnesses, and building legal cases
  - Involvement can result in loss of control of chain of events following an incident

# Disaster Recovery

- DRP
  - Preparation for and recovery from a disaster, whether natural or man made
- In general, 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
- Key role of DRP: defining how to reestablish operations at location where organization is usually located

# Disaster Classifications

- A DRP can classify disasters in a number of ways
  - Most common:
    - Separate natural disasters from man-made disasters
  - Another way: by speed of development
    - Rapid onset disasters
      - Earthquake, floods, storms, tornadoes
    - Slow onset disasters
      - Droughts, famines, env degradation, deforestation, pest infestation

# Planning for Disaster

- Categorize threat level of potential disasters
  - Uses Scenario development and impact analysis
- DRP must be tested regularly
- Key points in the DRP:
  - Clear delegation of roles and responsibilities
  - Execution of alert roster and notification of key personnel
  - Clear establishment of priorities
  - Documentation of the disaster
  - Action steps to mitigate the impact
  - Alternative implementations for various systems components

# Crisis Management

- DRP should refer to a CM process
  - Set of focused steps taken during and after a disaster that deal primarily with people involved
- Crisis management team manages event:
  - Supporting personnel and their loved ones during crisis
  - Determining event's impact on normal business operations
  - When necessary, making a disaster declaration
  - Keeping public informed about event
  - Communicating with outside parties
- Two key tasks of crisis management team:
  - Verifying personnel status
  - Activating alert roster

# Responding to the Disaster

- Actual events often outstrip even best of plans
- To be prepared, DRP should be flexible
- If physical facilities are intact, begin restoration there
- If organization’s facilities are unusable, take alternative actions
- When disaster threatens organization at the primary site, DRP becomes BCP

# Business Continuity Planning (BCP)

- Ensures critical business functions can continue in a disaster
- Most properly managed by CEO of organization
- Activated and executed concurrently with the DRP when needed
- Reestablishes critical functions at alternate site (DRP focuses on reestablishment at primary site)
- Relies on identification of critical business functions and the resources to support them

# Continuity Strategies

- Several continuity strategies for business continuity
  - Determining factor is usually cost
- Three exclusive-use options:
  - Hot sites
  - Warm sites
  - Cold sites
- Three shared-use options:
  - Timeshare
  - Service bureaus
  - Mutual agreements

# Exclusive Use Options

- Hot Sites
  - Fully configured computer facility with all services
- Warm Sites
  - Like hot site, but software applications not kept fully prepared
- Cold Sites
  - Only rudimentary services and facilities kept in readiness

# Shared Use Options

- Timeshares
  - Like an exclusive use site but leased
- Service Bureaus
  - Agency that provides physical facilities
- Mutual Agreements
  - Contract between two organizations to assist
- Specialized alternatives:
  - Rolling mobile site
  - Externally stored resources

# Off-Site Disaster Data Storage

- To get any BCP site running quickly, organization must be able to recover data
- Options include:
  - Electronic vaulting: bulk batch-transfer of data to an off-site facility
  - Remote Journaling: transfer of live transactions to an off-site facility
  - Database shadowing: storage of duplicate online transaction data

# Incident Response and Disaster Recovery

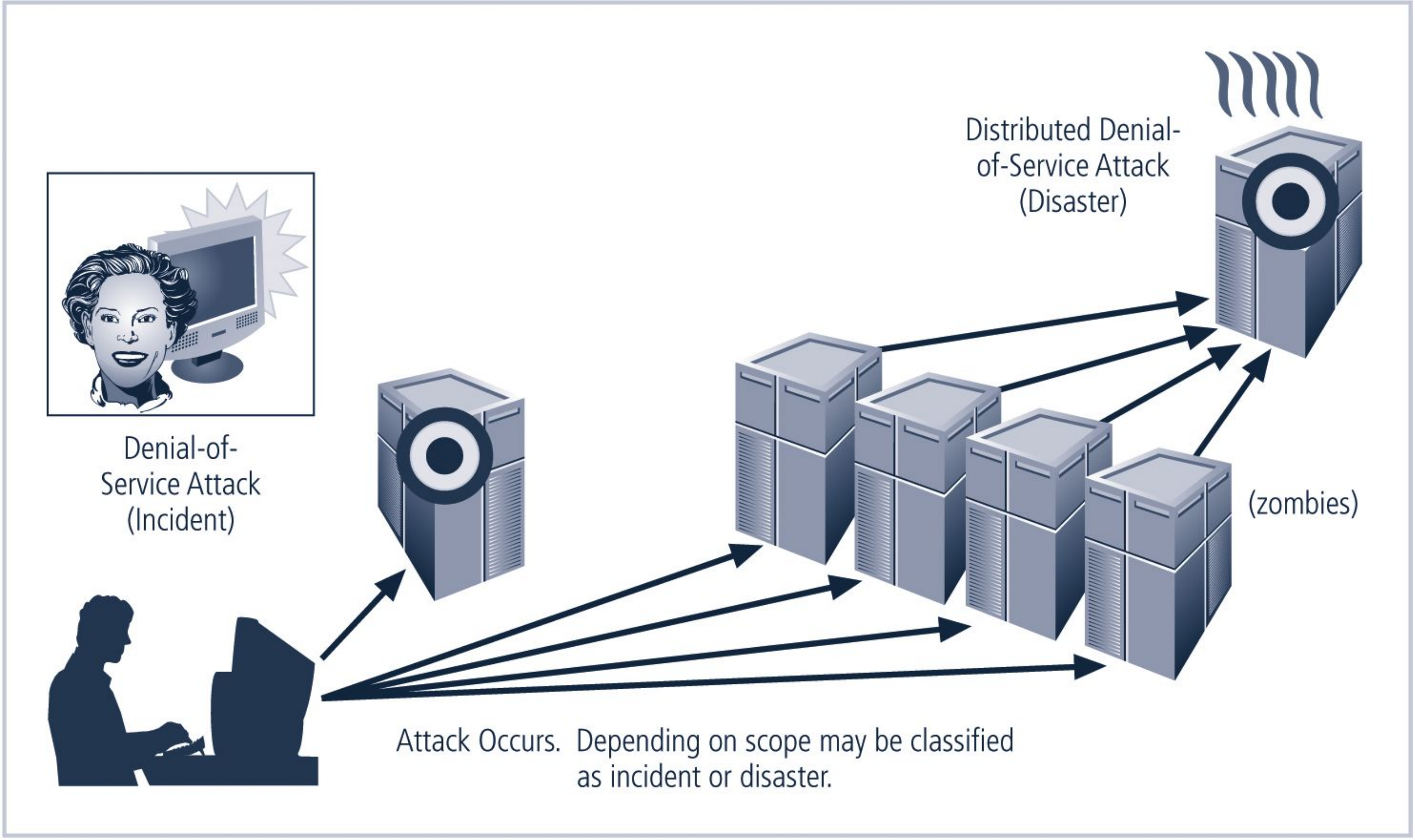

Distributed Denial-of-Service Attack (Disaster)
Denial-of-Service Attack (Incident)
(zombies)
Attack Occurs. Depending on scope may be classified as incident or disaster.

**FIGURE 3-3** Incident Response and Disaster Recovery

# Disaster Recovery and Business Continuity Planning

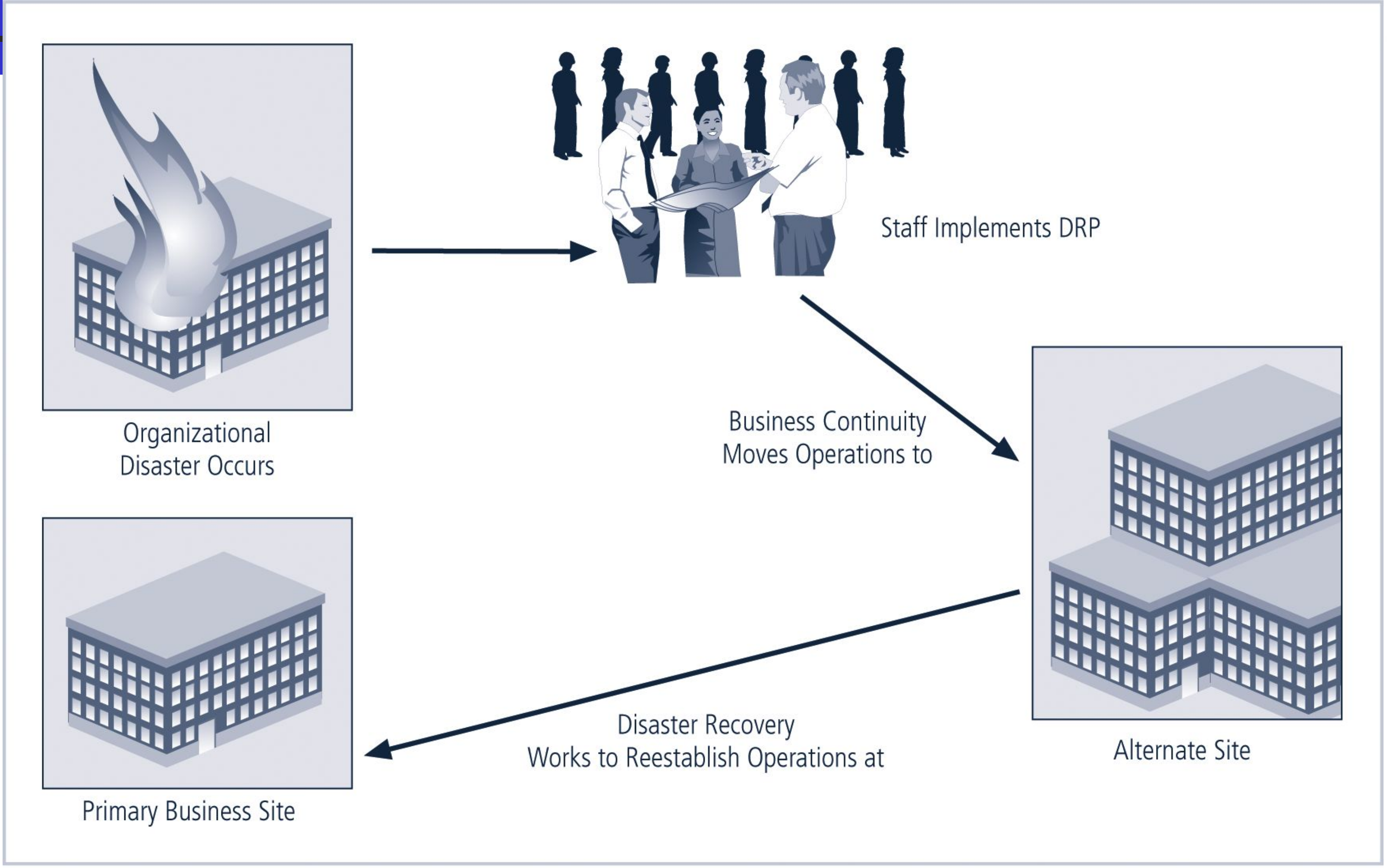

Staff Implements DRP
Organizational Disaster Occurs
Business Continuity Moves Operations to
Alternate Site
Disaster Recovery Works to Reestablish Operations at
Primary Business Site

**FIGURE 3-4** Disaster Recovery and Business Continuity Planning

# Contingency Plan Implementation Timeline

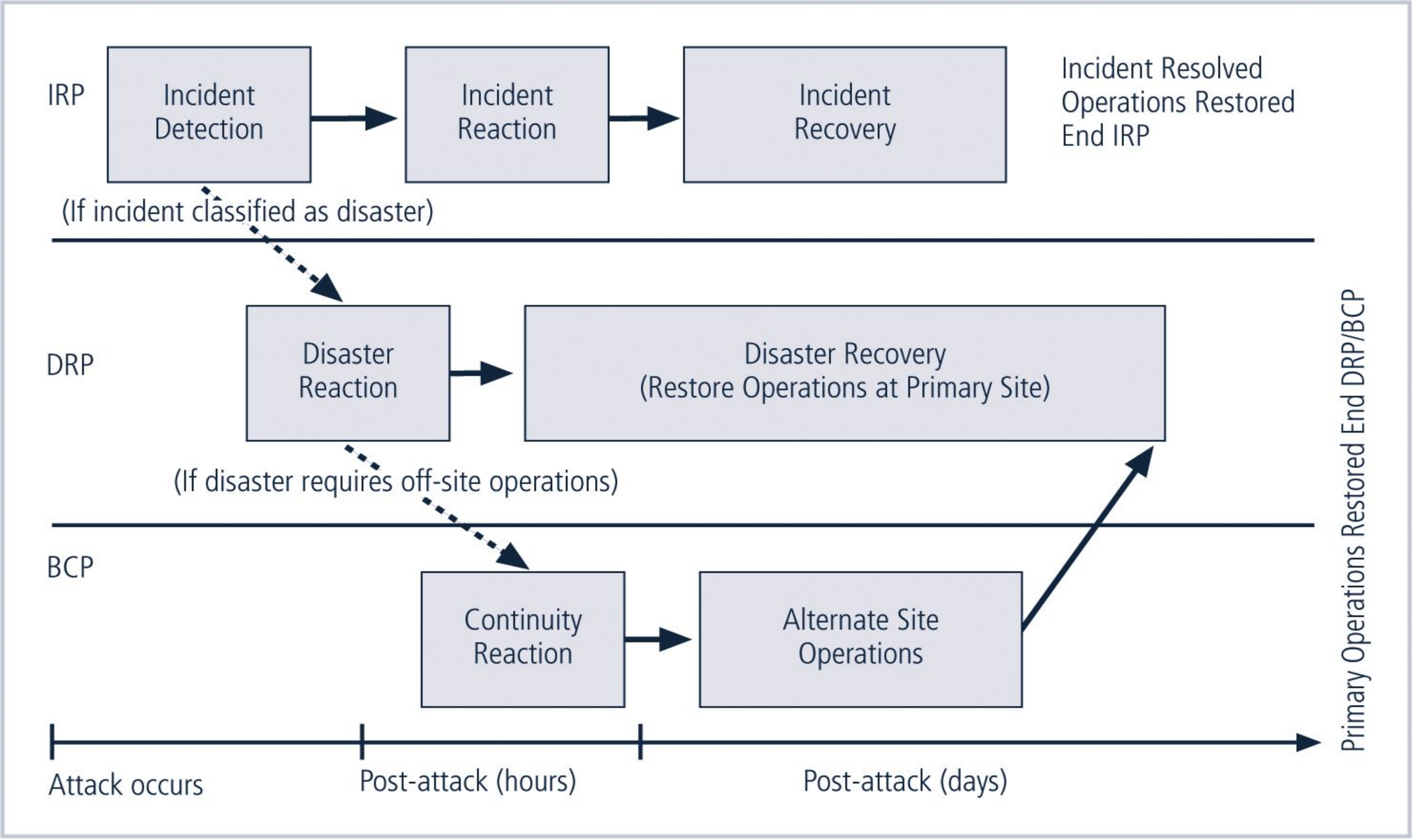


**FIGURE 3-5** Contingency Plan Implementation Timeline

# Putting a Contingency Plan Together

- The CP team should include:
  - Champion
  - Project Manager
  - Team Members
    - Business managers
    - Information technology managers
    - Information security managers

# Major Tasks in Contingency Planning (for CP team)

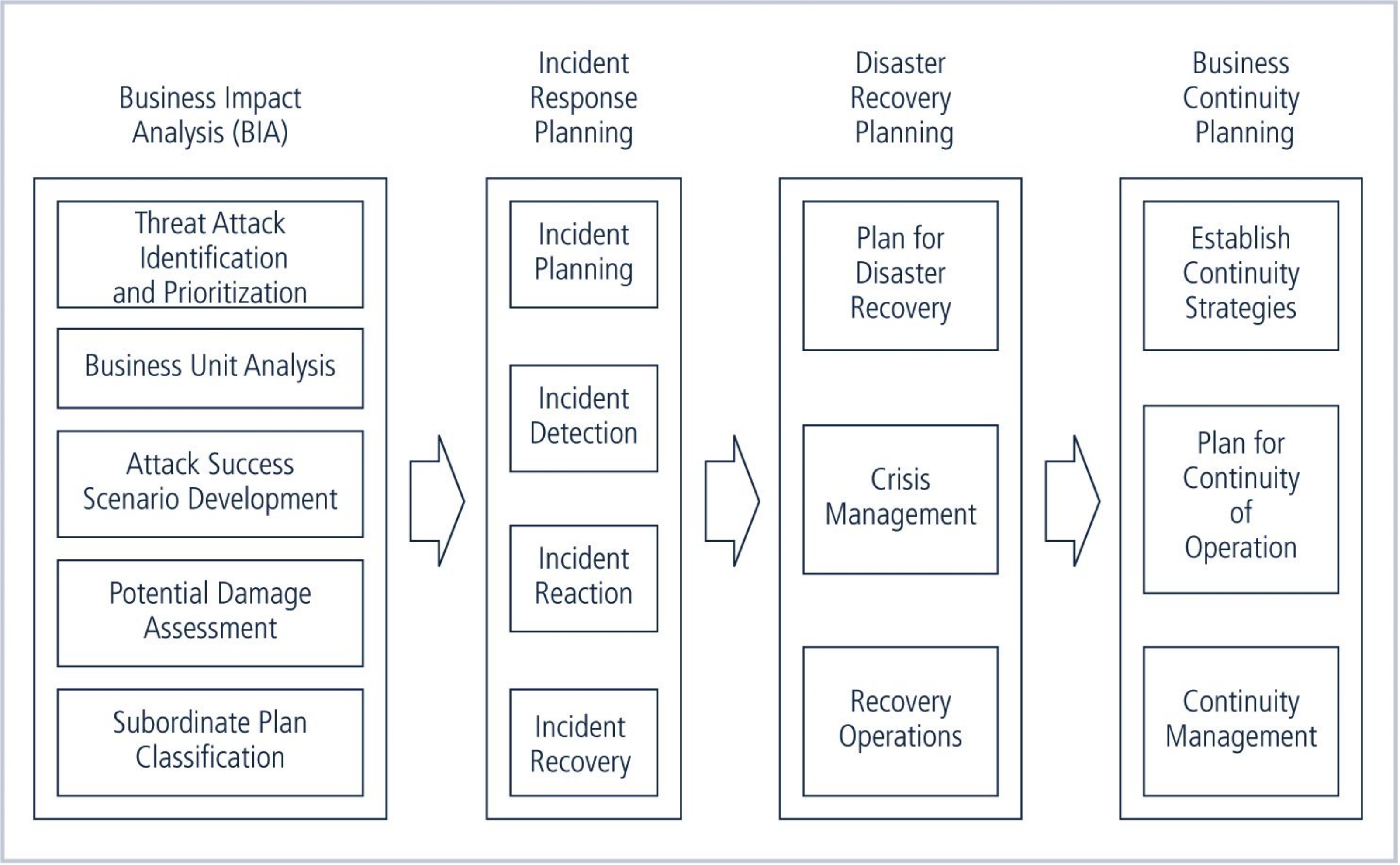

Business Impact Analysis (BIA)
Threat Attack Identification and Prioritization
Business Unit Analysis
Attack Success Scenario Development
Potential Damage Assessment
Subordinate Plan Classification
Incident Response Planning
Incident Planning
Incident Detection
Incident Reaction
Incident Recovery
Disaster Recovery Planning
Plan for Disaster Recovery
Crisis Management
Recovery Operations
Business Continuity Planning
Establish Continuity Strategies
Plan for Continuity of Operation
Continuity Management

**FIGURE 3-6** Major Tasks in Contingency Planning

# Business Impact Analysis (BIA)

- BIA
  - Provides information about systems/threats and detailed scenarios for each potential attack
  - Not risk management focusing on identifying threats, vulnerabilities, and attacks to determine controls
    - Assumes controls have been bypassed or are ineffective and attack was successful
- CP team conducts BIA in the following stages:
  - Threat attack identification
  - Business unit analysis
  - Attack success scenarios
  - Potential damage assessment
  - Subordinate plan classification

# Threat/Attack Identification and Prioritization

- An organization that uses risk management process will have identified and prioritized threats
  - Add the attack profile to it
- Attack profile:
  - detailed description of activities that occur during an attack
  - (handout page)

# BUA and ASSD

- Business Unit Analysis
  - Analysis and prioritization of business functions within the organization
  - Each unit should be considered separately
- Attack Success Scenario Development
  - Create a series of scenarios depicting impact of successful attack on each functional area
  - Attack profiles should include scenarios depicting typical attack including:
    - Methodology
    - Indicators
    - broad consequences
  - More details are added including
    - alternate outcomes—best, worst, and most likely

# Potential Damage Assessment

- From detailed scenarios,
  - the BIA planning team must estimate the cost of the best, worst, and most likely outcomes by preparing an attack scenario end case
  - Allow identification of what must be done to recover from each possible case

# Subordinate Plan Classification

- From existing plans, a related plan must be developed or identified from among existing plans already in place
- Each attack scenario case is categorized as disastrous or not
- Attack cases that are disastrous find members of the organization waiting out the attack and planning to recover after it is over

# Combining the DRP and the BCP

- DRP and BCP are closely related,
  - Most organizations prepare them concurrently and may combine them into a single document
  - Such a comprehensive plan must be able to support reestablishment of operations at two different locations
    - Immediately at alternate site
    - Eventually back at primary site
  - Although a single planning team can develop combined DRP/BRP, execution requires separate teams

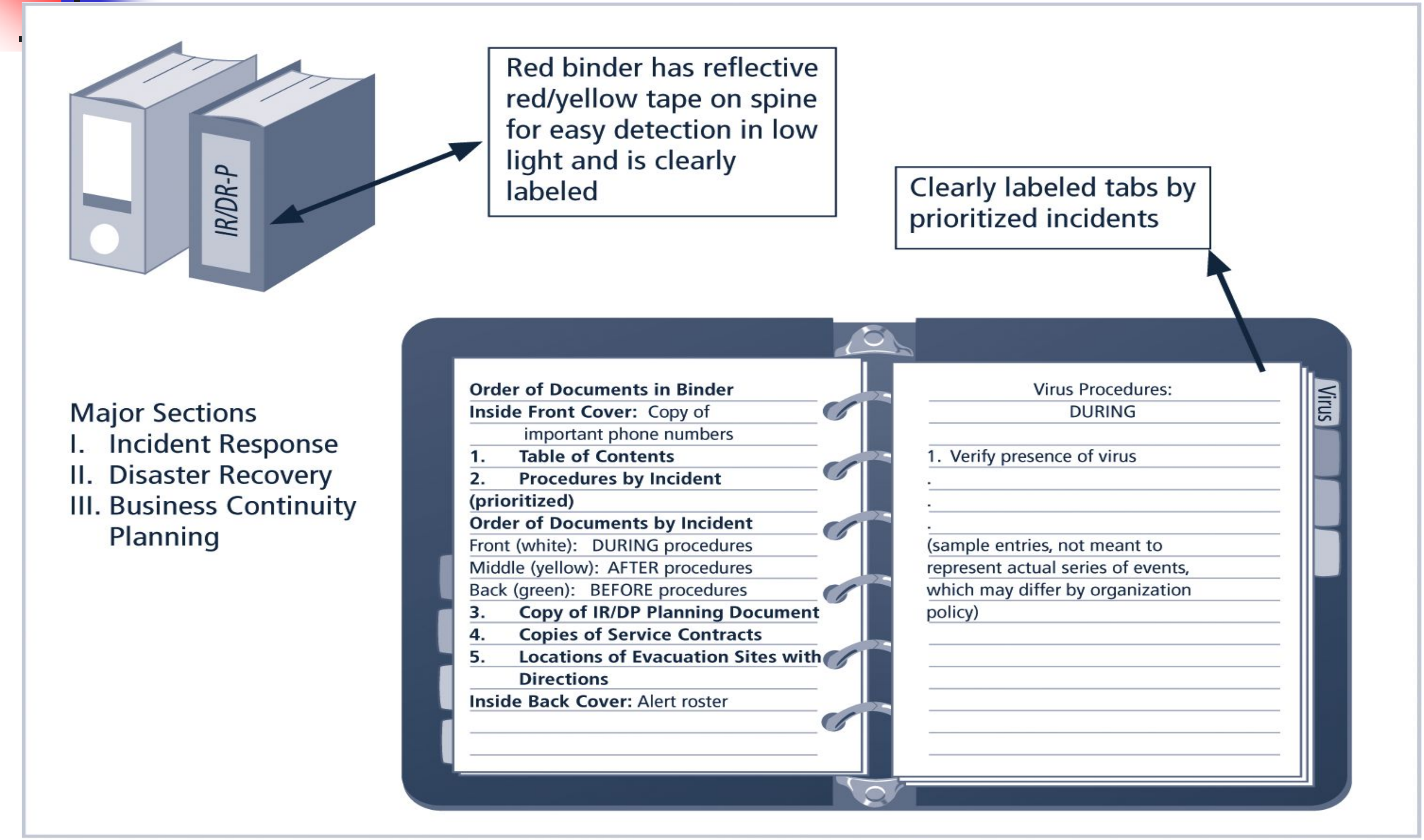
# Sample Disaster Recovery Plan

- Name of agency
- Date of completion or update of the plan and test date
- Agency staff to be called in the event of a disaster
- Emergency services to be called (if needed) in event of a disaster
- Locations of in-house emergency equipment and supplies
- Sources of off-site equipment and supplies
- Salvage Priority List
- Agency Disaster Recovery Procedures
- Follow-up Assessment

# Testing Contingency Plans

- Once problems are identified during the testing process, improvements can be made, and the resulting plan can be relied on in times of need
- There are five testing strategies that can be used to test contingency plans:
  - Desk Check
  - Structured walkthrough
  - Simulation
  - Parallel testing
  - Full interruption

# A Single Contingency Plan Format



Red binder has reflective red/yellow tape on spine for easy detection in low light and is clearly labeled

Clearly labeled tabs by prioritized incidents

Major Sections
I. Incident Response
II. Disaster Recovery
III. Business Continuity Planning

**Order of Documents in Binder**
**Inside Front Cover:** Copy of important phone numbers
1. **Table of Contents**
2. **Procedures by Incident (prioritized)**

**Order of Documents by Incident**
Front (white): DURING procedures
Middle (yellow): AFTER procedures
Back (green): BEFORE procedures

3. **Copy of IR/DP Planning Document**
4. **Copies of Service Contracts**
5. **Locations of Evacuation Sites with Directions**

**Inside Back Cover:** Alert roster

Virus Procedures:
DURING

1. Verify presence of virus
.
.
.

(sample entries, not meant to represent actual series of events, which may differ by organization policy)

FIGURE 3-8 Contingency Plan Format

# Continuous Improvement

- Iteration results in improvement
- A formal implementation of this methodology is a process known as continuous process improvement (CPI)
- Each time plan is rehearsed, it should be improved
- Constant evaluation and improvement leads to an improved outcome