Information Security Management

Chapter 3
Planning for Contingencies

Webster University
Scott Granneman

“Things which you do not hope
happen more frequently
than things which you do hope.”

-- Plautus (c. 254–184 BCE),
in Mostellaria,
Act I, Scene 3, 40 (197)

Upon completion of this chapter,
you should be able to:

Understand the need for contingency planning

Know the major components
of contingency planning

Create a simple set of contingency plans,
using Business Impact Analysis

Prepare and execute a test of contingency plans

Understand
the combined contingency plan approach

This chapter focuses on
planning for the unexpected event,
when the use of technology is disrupted
& business operations come to a standstill

Procedures are required
that will permit the organization
to continue essential functions
if IT support is interrupted

Over **40%** of businesses
that don’t have a disaster plan
go out of business after a major loss!

Contingency Planning (CP):
planning for unexpected events

It is how organizational planners
position their organizations
to prepare for, detect, react to, & recover from
events that threaten
the security of info resources & assets

Main goal: **restoration**
to normal modes of operation
with minimum cost & disruption
to normal business activities
after an unexpected event

CP Components

✓ Incident response planning (IRP)
focuses on immediate response

✓ Disaster recovery planning (DRP)
focuses on restoring operations
at the primary site after disasters occur

✓ Business continuity planning (BCP)
facilitates establishment of operations
at an alternate site

To ensure continuity across
all CP processes
during planning process,
contingency planners should:

✓ Identify mission- or business-critical functions

✓ Identify resources supporting critical functions

✓ Anticipate potential contingencies or disasters

✓ Select contingency planning strategies

✓ Implement selected strategy

✓ Test & revise contingency plans

Four teams are involved
in CP & contingency operations:

✓ CP team

✓ Incident recovery (IR) team

✓ Disaster recovery (DR) team

✓ Business continuity plan (BC) team

NIST describes the need for this type of planning as:

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

Components of CP

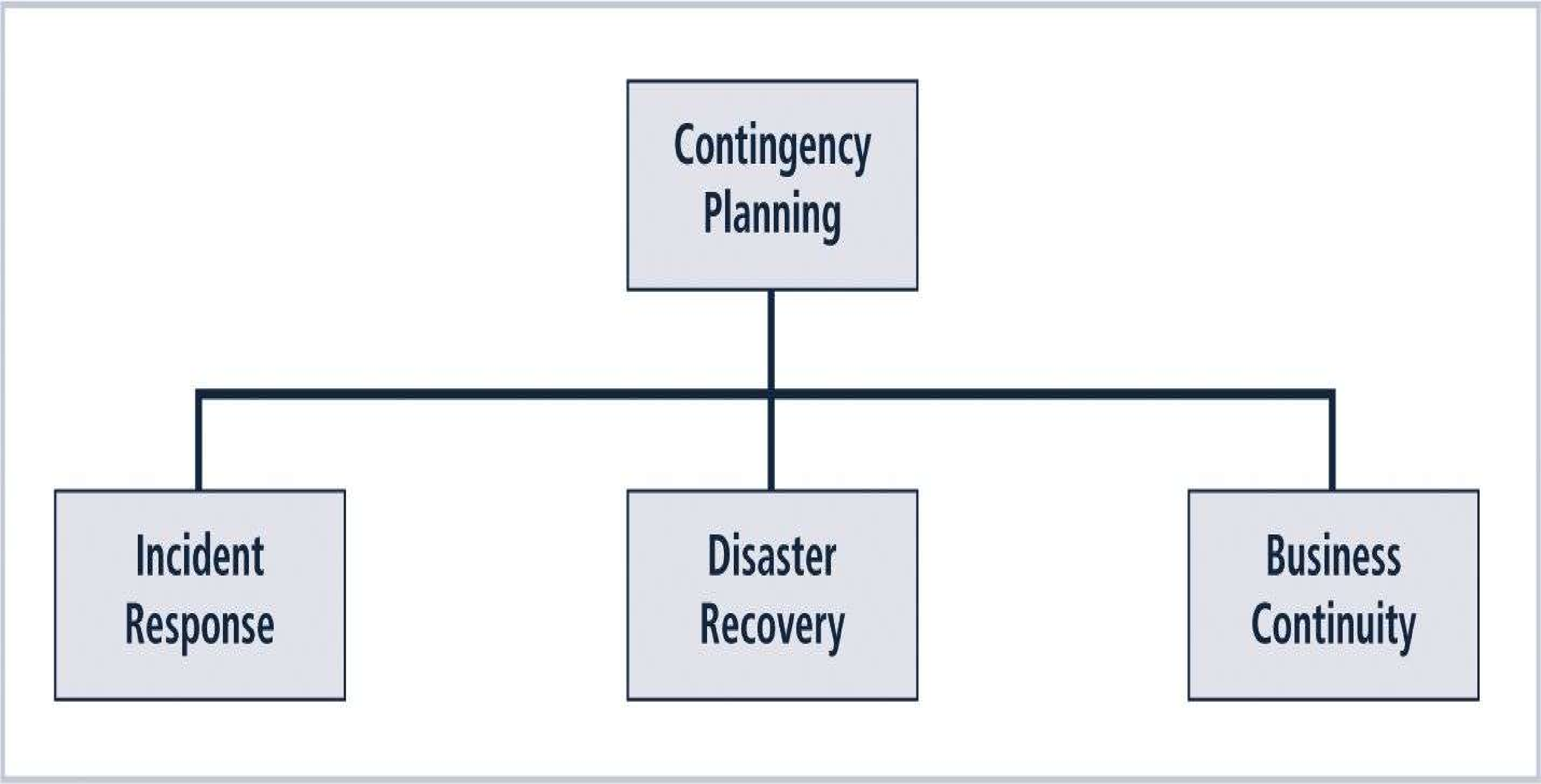


FIGURE 3-1 Contingency Planning Hierarchies

Incident Response Plan (IRP):
Detailed set of processes & procedures
that anticipate, detect, & mitigate
the impact of an unexpected event
that might compromise
information resources & assets

Incident response (IR):
Set of procedures that commence
when an incident is detected

When a threat becomes a valid attack,
it is classified as
an information 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

It is important to understand that
IR is a reactive measure,
not a preventative one

During the incident …

✓ Planners develop & document
the procedures that must be performed
during the incident

✓ These procedures are
grouped & assigned to various roles

✓ Planning committee drafts
a set of function-specific procedures

After the incident …

✓ Once the procedures
for handling an incident are drafted,
planners develop & document
the procedures that must be performed
immediately after the incident has ceased

✓ Separate functional areas
may develop different procedures

Before the incident …

Planners draft a 3rd set of procedures,
those tasks that must be performed
in advance of the incident, including:

✓ Details of data backup schedules

✓ Disaster recovery preparation

✓ Training schedules

✓ Testing plans

✓ Copies of service agreements

✓ Business continuity plans

Planning requires a
detailed understanding of info systems
& threats they face

IR planning team seeks
to develop 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 & effort

IR team consists of
professionals capable of
handling info systems & functional areas
affected by an incident

Each member of the IR team must:

✓ Know their specific role

✓ Work in concert with each other

✓ Execute the objectives of the IRP

How do you detect an incident?

Is an event routine system use
or an actual incident?

Incident classification:
process of examining a possible incident
& determining whether or not
it constitutes actual incident

Initial reports from ...

✓ end users,
✓ intrusion detection systems (IDS),
✓ host- & network-based anti-virus software,
✓ sysadmins

... are all ways to track & detect
incident candidates

Careful training
allows everyone
to relay vital information to the IR team

Incident Indicators

Possible Indicators

- ✓ Unfamiliar files
- ✓ Unknown programs or processes
- ✓ Unusual consumption of computing resources
- ✓ Unusual system crashes

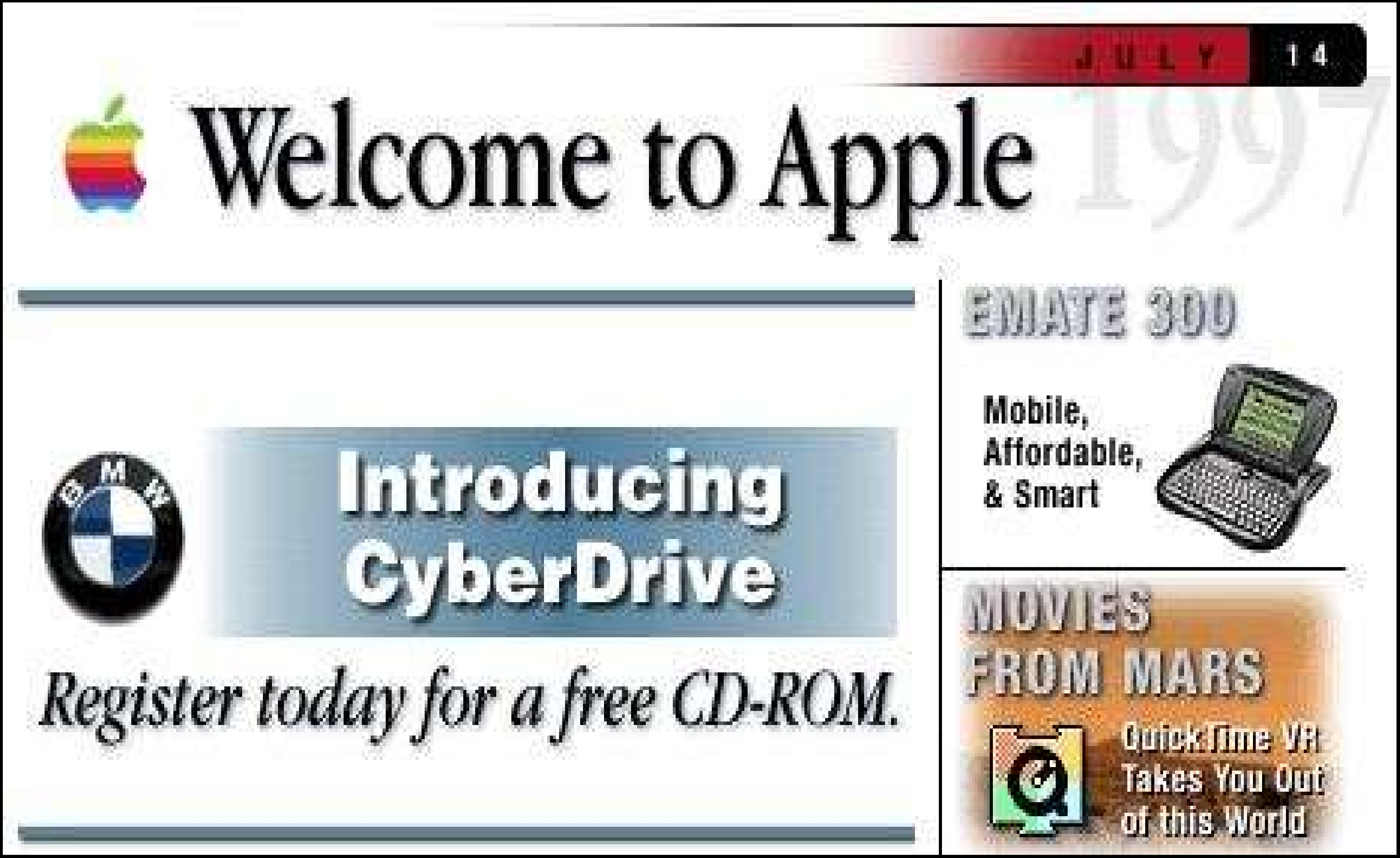
Probable Indicators

- ✓ Activities at weird 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

Apple home page, 1997



JULY 14

Welcome to Apple 1997

EMATE 300

Mobile, Affordable, & Smart

Introducing CyberDrive

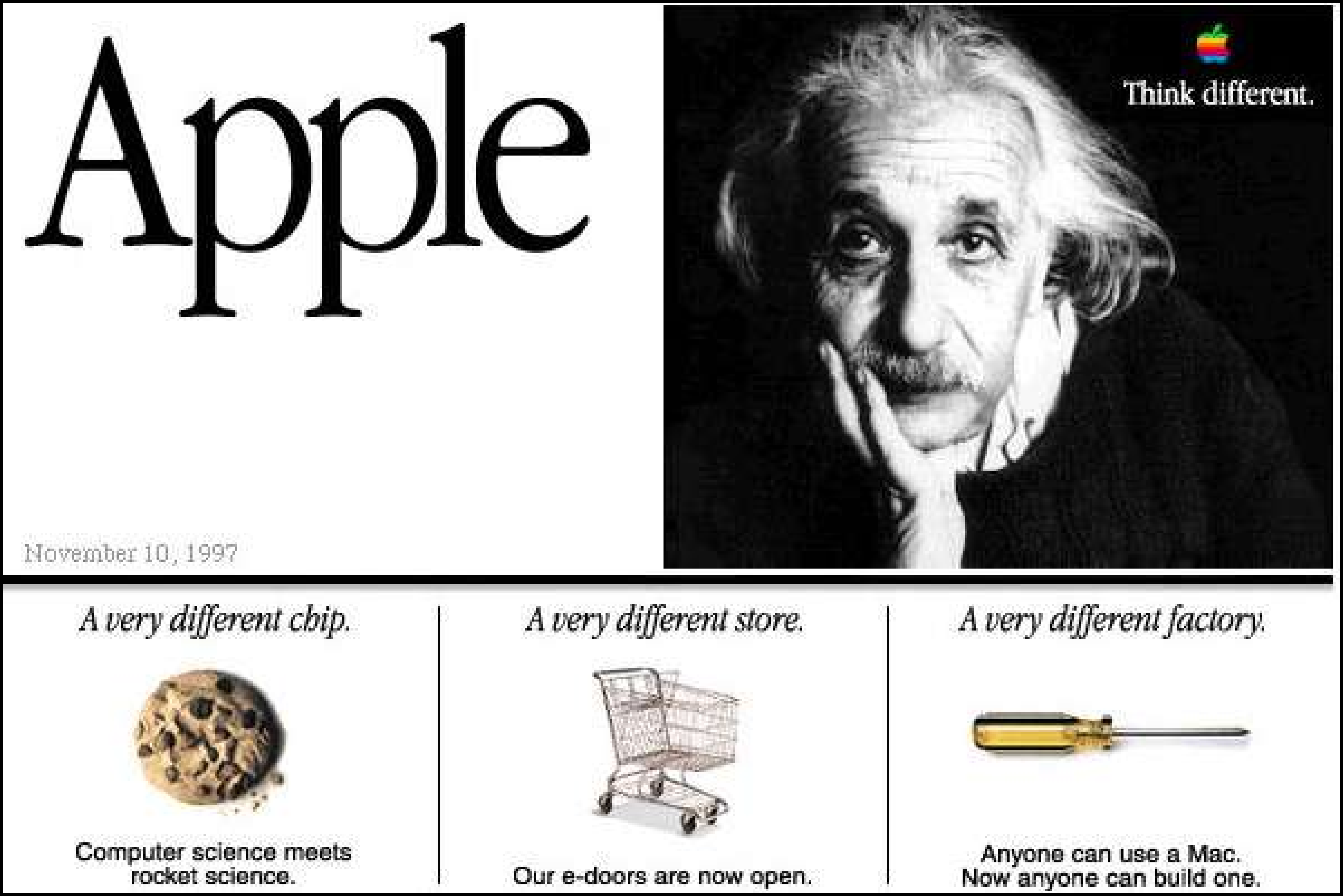
Register today for a free CD-ROM.

MOVIES FROM MARS

QuickTime VR Takes You Out of this World

http://www.flickr.com/photos/kernelpanic/sets/283374/

Apple home page, 1997



Apple

Think different.

November 10, 1997

A very different chip.

Computer science meets rocket science.

A very different store.

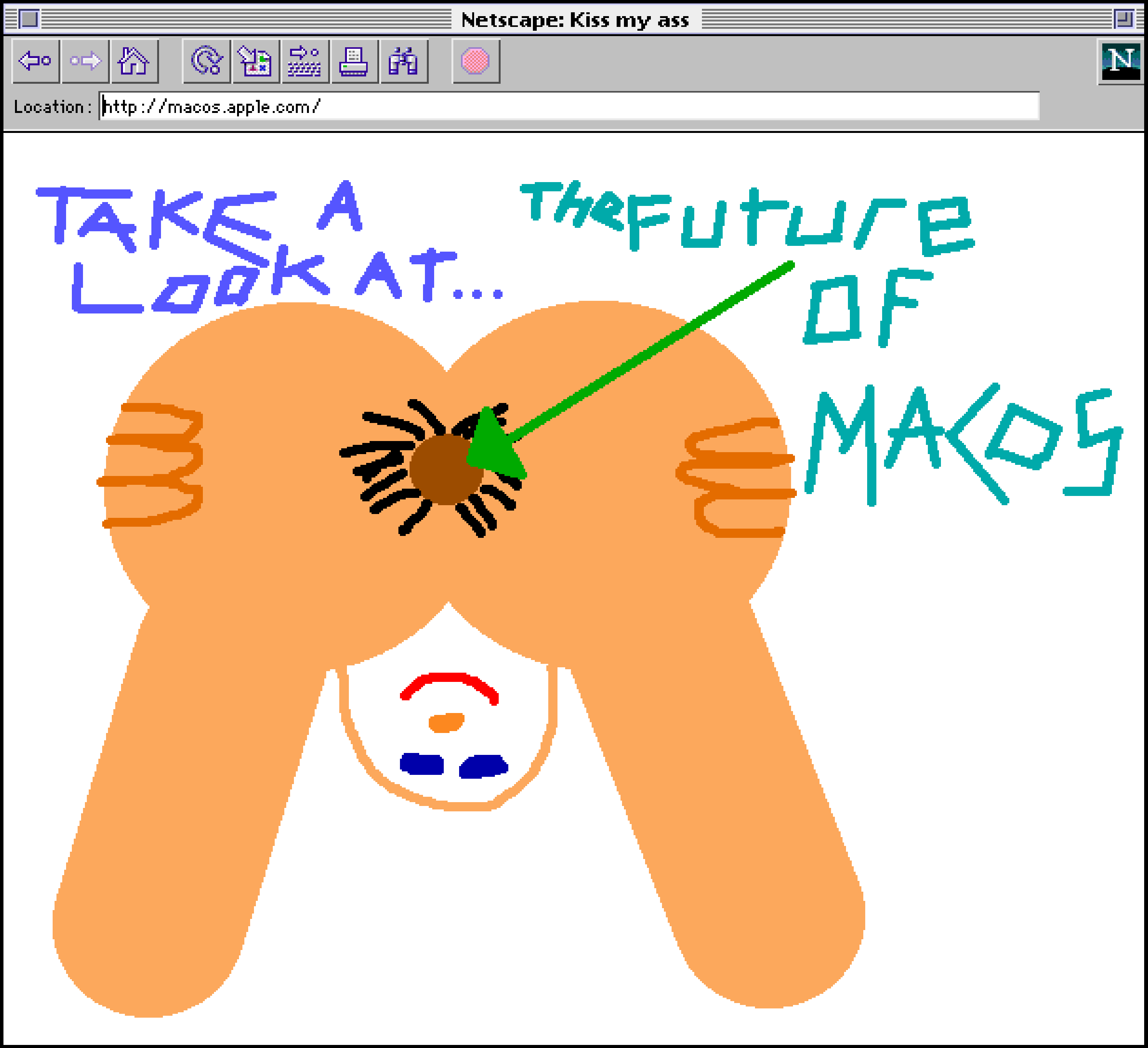
Our e-doors are now open.

A very different factory.

Anyone can use a Mac. Now anyone can build one.

http://www.flickr.com/photos/kernelpanic/sets/283374/

Apple home page for a few hours, 1997



http://www.flickr.com/photos/kernelpanic/sets/283374/

Occurrences of actual incidents:

✓ Loss of availability

✓ Loss of integrity

✓ Loss of confidentiality

✓ Violation of policy

✓ Violation of law

Once an actual incident
has been confirmed & properly classified,
the IR team moves
from detection phase to reaction phase

In the incident response phase,
a number of action steps
taken by the IR team & others
must occur quickly
& may occur concurrently

These steps include
notification of key personnel,
the assignment of tasks,
& documentation of the incident

As soon as incident is declared,
the right people
must be immediately notified
in the right order

Alert roster:
document containing 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,
but before media or other sources find out

As soon as an incident has been confirmed
& the notification process is underway,
the team should begin documentation

Should record the
who, what, when, where, why, & 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
& if they were effective

Can also prove the organization
did everything possible
to deter the spread of the incident

Incident Containment

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

IR team can stop the incident & 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 or service

✓ Take down conduit application or server

✓ Stop all computers & 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

Incident Recovery

Once the incident has been contained,
& system control regained,
incident recovery can begin

IR team must assess full extent of damage
in order to determine
what must be done to restore systems

Immediate determination of the scope of the
breach of confidentiality, integrity, & availability
of information & information assets
is called **incident damage assessment**

Those who document the damage
must be trained to collect & preserve evidence,
in case the incident is part
of a crime or results in a civil action

Once the extent of the damage
has been determined,
the **recovery process** begins:

✓ Identify & resolve vulnerabilities
that allowed incident to occur & spread

✓ Address, install, & 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 & reporting methods,
or install new monitoring capabilities

more ... →

✓ Restore data from backups as needed

✓ Restore services & processes in use
where compromised (& interrupted)
services & processes
must be examined, cleaned, & then restored

✓ Continuously monitor system

✓ Restore the confidence
of the members
of the organization’s communities of interest

Before returning to routine duties,
the IR team must conduct
an **after-action review** (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

When incident violates civil or criminal law,
it is an organization’s responsibility
to notify proper legal authorities

Selecting appropriate law enforcement
depends on the type of crime committed:

- ✓ Federal
- ✓ State
- ✓ Local

Involving law enforcement
has both advantages & disadvantages:

Usually much better equipped
at processing evidence,
obtaining statements from witnesses,
& building legal cases

However ...
involvement can result
in loss of control
of chain of events
following an incident

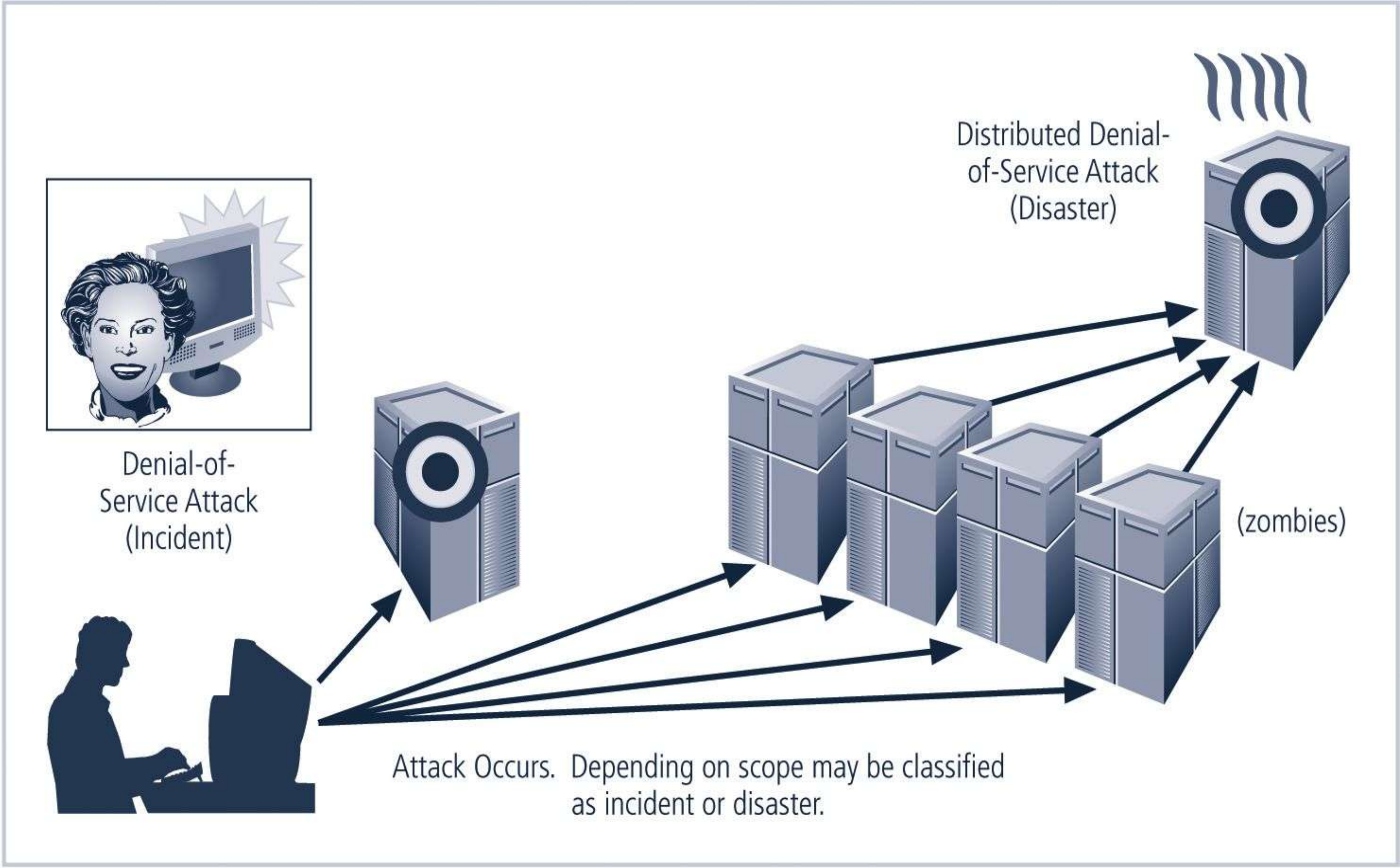

Distributed Denial-of-Service Attack (Disaster)
Denial-of-Service Attack (Incident)
(zombies)
Attack Occurs. Depending on scope may be classified as incident or disaster.

FIGURE 3-3 Incident Response and Disaster Recovery

Disaster recovery planning (DRP)
is the preparation for & recovery from
a natural or man made disaster

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,
organization is unable to quickly recover

Key role of DRP:
defining how
to reestablish operations
at location
where organization is usually located

A DRP can classify disasters
in a number of ways

Most common method:
separate natural disasters
from man-made disasters

Another method:
by speed of development
(rapid onset or slow onset disasters)

Scenario development & impact analysis
are used to categorize
the level of threat
of each potential disaster

DRP must be tested regularly

Key points in the DRP:

✓ Clear delegation of roles & responsibilities

✓ Execution of alert roster
& 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:
set of focused steps
taken during & after a disaster
that deal primarily with people involved

Crisis management team manages event:

- ✓ Supporting personnel & 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 laid 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 & executed
concurrently with the DRP when needed

Reestablishes critical functions at alternate site
(DRP focuses on reestablishment at primary site)

Relies on i.d. of critical business functions
& the resources to support them

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 & 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

To get any BCP site running quickly, organization must be able to recover data utilizing various options

✓ Electronic vaulting:
bulk batch-transfer of data to off-site facility

✓ Remote Journaling:
transfer of live transactions to off-site facility

✓ Database shadowing:
storage of duplicate online transaction data

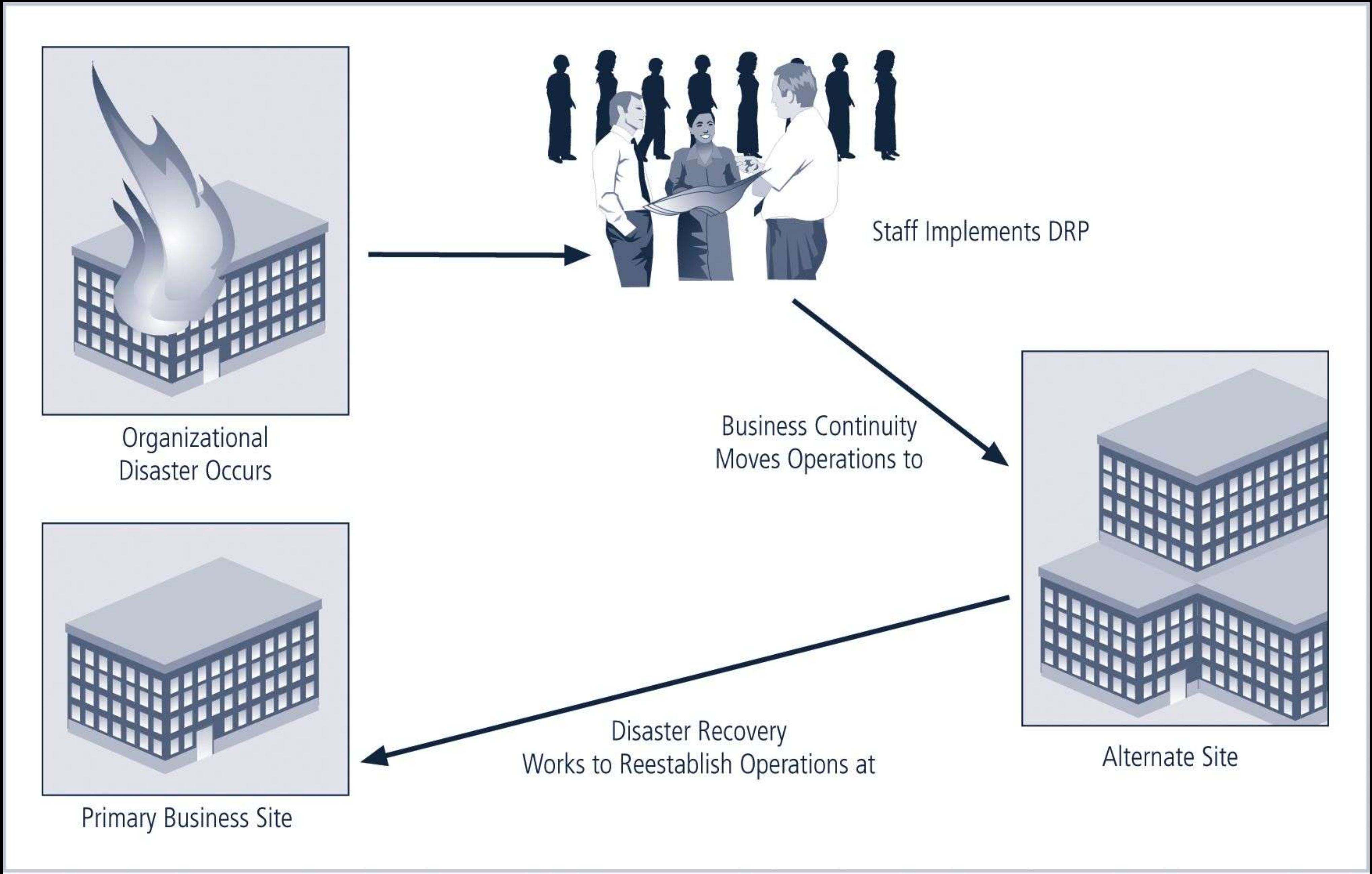

Staff Implements DRP
Organizational Disaster Occurs
Business Continuity Moves Operations to
Alternate Site
Disaster Recovery Works to Reestablish Operations at
Primary Business Site

FIGURE 3-4 Disaster Recovery and Business Continuity Planning

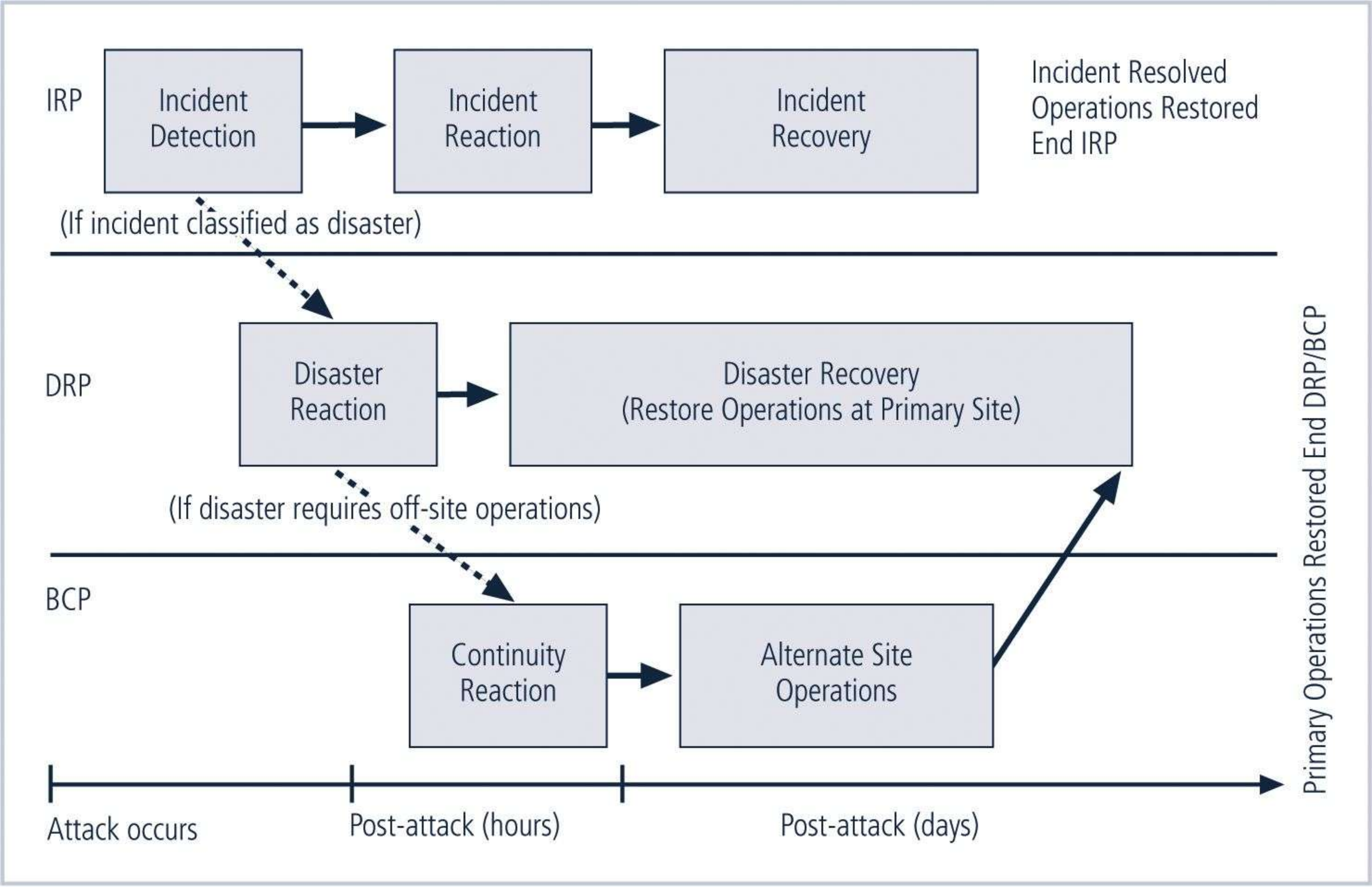


FIGURE 3-5 Contingency Plan Implementation Timeline

The CP team should include:

✓ Champion

✓ Project Manager

✓ Business managers

✓ IT managers

✓ InfoSec managers

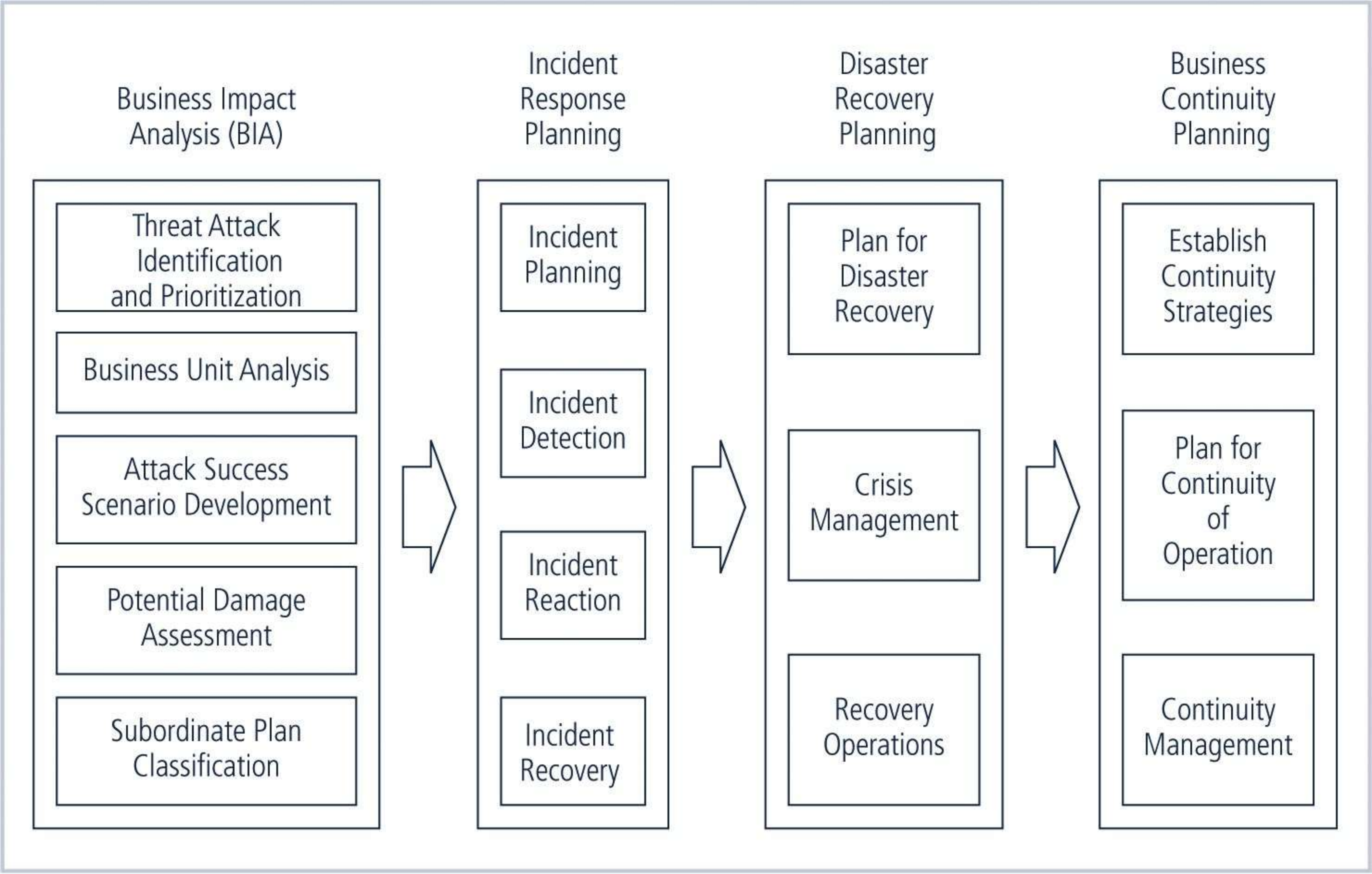

Business Impact Analysis (BIA)
Threat Attack Identification and Prioritization
Business Unit Analysis
Attack Success Scenario Development
Potential Damage Assessment
Subordinate Plan Classification
Incident Response Planning
Incident Planning
Incident Detection
Incident Reaction
Incident Recovery
Disaster 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

Provides information about systems/threats
& detailed scenarios
for each potential attack

Not risk management focusing on
identifying threats, vulnerabilities, & attacks
to determine controls

Assumes controls have been bypassed
or are ineffective & 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

An organization that uses
risk management process
will have identified & prioritized threats

These organizations update threat list
& add one additional piece of information:
the attack profile

Attack profile:
detailed description of activities
that occur during an attack

Second major BIA task
is business unit analysis:

analysis & prioritization
of business functions
within the organization

Next 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, & most likely

From detailed scenarios,
the BIA planning team
must estimate the cost
of the best, worst, & most likely outcomes
by preparing an attack scenario end case

This will allow identification
of what must be done
to recover from each possible case

Once the potential damage
has been assessed,
& each scenario
& attack scenario end case
has been evaluated,
a related plan
must be developed or identified
from among existing plans already in place

Each attack scenario end case
is categorized as disastrous or not

Attack end cases that are disastrous
find members of the organization
waiting out the attack
& planning to recover after it is over

Because DRP and BCP are closely related,
most organizations prepare them concurrently &
may combine them into a single document

Such a comprehensive plan
must be able
to support reestablishment of operations
at two different locations

1. Immediately at alternate site
2. Eventually back at primary site

Therefore, although a single planning team
can develop combined DRP/BRP,
execution requires separate teams

Sample disaster recovery plan:

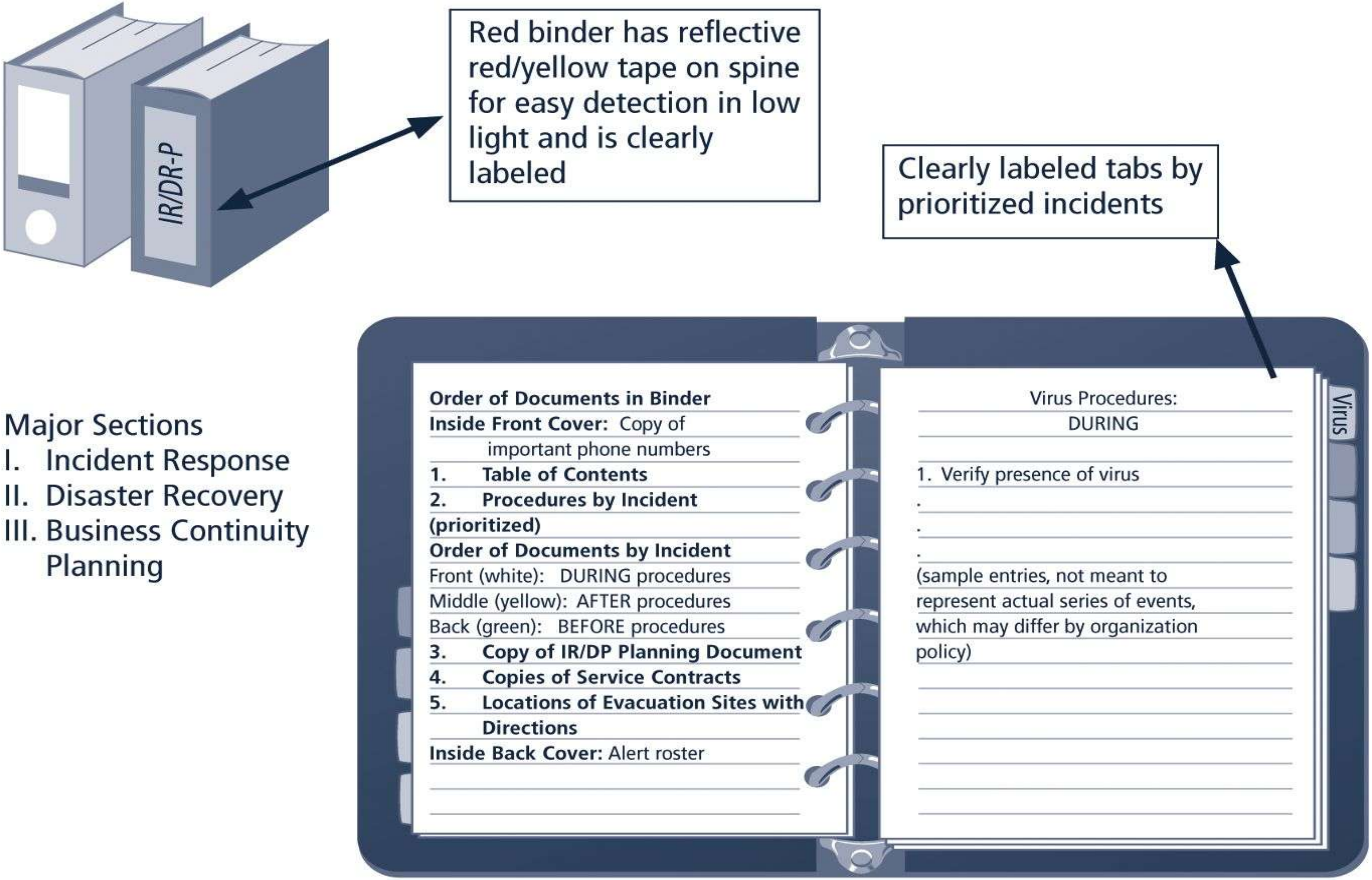
- ✓ Name of agency
- ✓ Date of completion or update of the plan & test date
- ✓ Agency staff to be called in the event of a disaster
- ✓ Emergency services to be called (if needed)
- ✓ Locations of in-house emergency equipment & supplies
- ✓ Sources of off-site equipment & supplies
- ✓ Salvage Priority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

You must test your contingency plan!

Once problems are identified
during the testing process,
improvements can be made,
& the resulting plan can be relied on

5 testing strategies can be used:

1. Desk Check
2. Structured walkthrough
3. Simulation
4. Parallel testing
5. Full interruption



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

Practice & change

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 & improvement
leads to an improved outcome

Summary

What Is Contingency Planning?

Components of CP

Putting a CP together

Testing CP

A single Continuity Plan

Thank you!

Scott Granneman