CONTINGENCY PLANNING

Learning Objectives

Upon completion of this part you should be able to:

- Understand the steps involved in incident reaction and incident recovery.
- Define the disaster recovery plan and its parts.
- Define the business continuity plan and its parts.
- Grasp the reasons for and against involving law enforcement officials in incident responses and when it is required.

- A key role for all managers is planning.
- Unfortunately for managers, however, the probability that some form of attack will occur, whether from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic factors, is very high.
- Thus, managers from each community of interest within the organization must be ready to act when a successful attack occurs.

Continuity Strategy

- Managers must provide strategic planning to assure continuous information systems availability ready to use when an attack occurs.
- Plans for events of this type are referred to in a number of ways:
  - Business Continuity Plans (BCPs)
  - Disaster Recovery Plans (DRPs)
  - Incident Response Plans (IRPs)
  - Contingency Plans

Contingency Planning (CP)

  - Incident Response Planning (IRP)
  - Disaster Recovery Planning (DRP)
  - Business Continuity Planning (BCP)

- The primary functions of these three planning types:
  - IRP focuses on immediate response, but if the attack escalates or is disastrous the process changes to disaster recovery and BCP.
  - DRP typically focuses on restoring systems after disasters occur, and as such is closely associated with BCP.
  - BCP occurs concurrently with DRP when the damage is major or long term, requiring more than simple restoration of information and information resources.

Components of CP

- An incident is any clearly identified attack on the organization‘s information assets that would threaten the asset‘s confidentiality, integrity, or availability.
- An Incidence Response Plan (IRP) deals with the identification, classification, response, and recovery from an incident.
- A Disaster Recovery Plan(DRP) deals with the preparation for and recovery from a disaster, whether natural or man-made.
- A Business Continuity Plan(BCP) ensures that critical business functions continue, if a

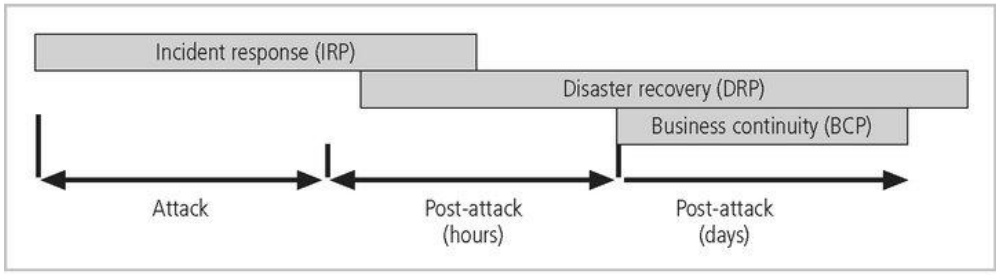


FIGURE 7-3 Contingency Planning Timeline

Contingency Planning Team

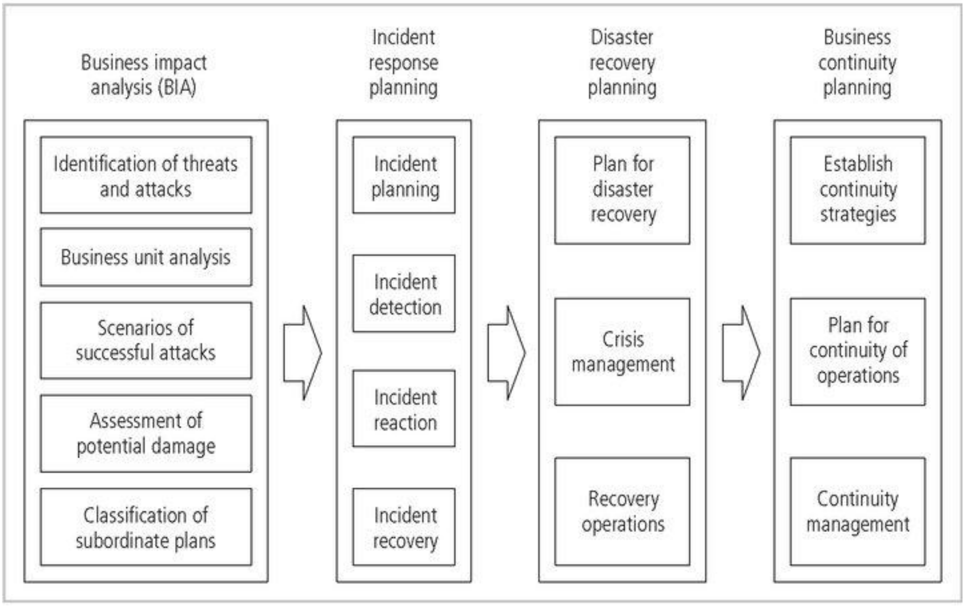
i. Champion: The CP project must have a high level manager to support, promote , and endorse

the findings of the project.

ii. Project Manager: A champion provides the strategic vision and the linkage to the power

structure of the organization.

iii. Team members: The team members for this project should be the managers or their representatives from the various communities of interest: Business, Information technology, and information security.



Business impact analysis (BIA)
Identification of threats and attacks
Business unit analysis
Scenarios of successful attacks
Assessment of potential damage
Classification of subordinate plans
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 operations
Continuity management

FIGURE 7-4 Major Steps in Contingency Planning

Business Impact Analysis

- The first phase in the development of the CP process is the Business Impact Analysis.
- A BIA is an investigation and assessment of the impact that various attacks can have on the organization.
- It begins with the prioritized list of threats and vulnerabilities identified in the risk management.
- The BIA therefore adds insight into what the organization must do to respond to attack, minimize the damage from the attack, recover from the effects, and return to normal operations.

- Begin with Business Impact Analysis (BIA)

  if the attack succeeds, *what* do we do then?

  Obviously the organization‘s security team does everything In its power to stop these attacks, but some attacks, such as natural disasters, deviations from service providers, acts of human failure or error, and deliberate acts of sabotage and vandalism, may be unstoppable.

- The CP team conducts the BIA in the following stages:

  Threat attack identification

  Business unit analysis

  Attack success scenarios

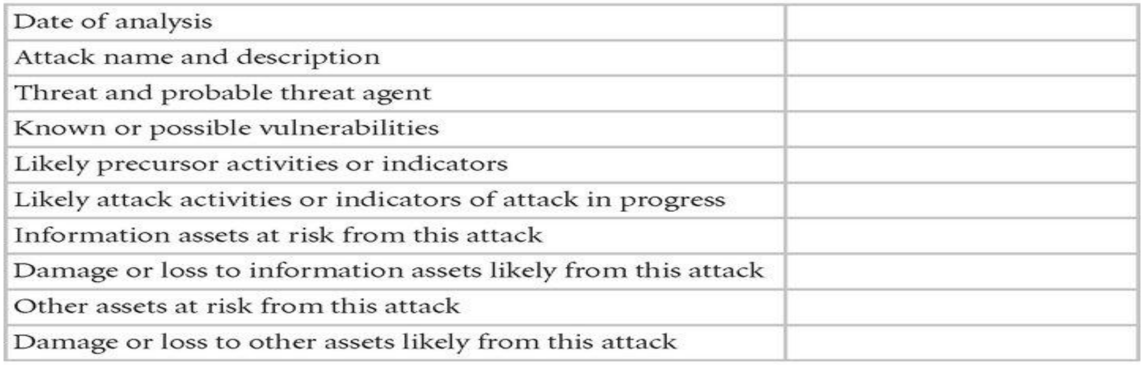
  Potential damage assessment

  Subordinate plan classification

Threat Attack Identification and Prioritization

- The **attack profile** is the detailed description of activities that occur during an attack
- Must be developed for every serious threat the organization faces, natural or man-made, deliberate or accidental.

TABLE 7-1 Attack Profile



Date of analysis	
Attack name and description	
Threat and probable threat agent	
Known or possible vulnerabilities	
Likely precursor activities or indicators	
Likely attack activities or indicators of attack in progress	
Information assets at risk from this attack	
Damage or loss to information assets likely from this attack	
Other assets at risk from this attack	
Damage or loss to other assets likely from this attack	

Business Unit Analysis

- The second major task within the BIA is the analysis and prioritization of business functions within the organization.

- This series of tasks serves to identify and prioritize the functions within the organization‘s units (departments, sections, divisions, groups, or other such units) to determine which are most vital to the continued operations of the organization.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf