5. Explain in detail about contingency planning.(May/June 2014, Nov/Dec 2012)

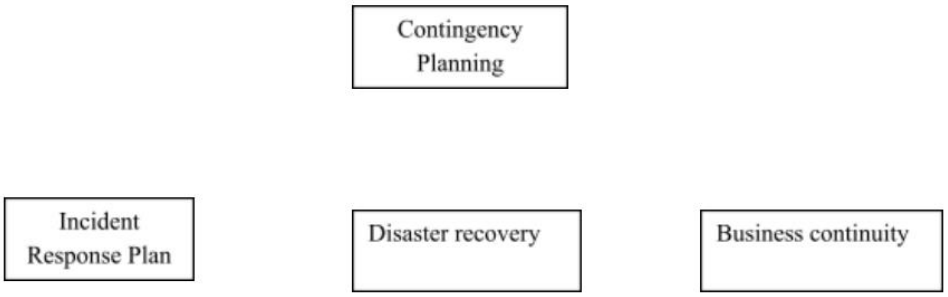
Contingency Planning

Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations. The organizations need to develop disaster recovery plans, incident response plans, and business continuity plans as subsets of an overall CP.

An **incident response plan (IRP)** deals with the identification, classification, response, and recovery from an incident, but if the attack is disastrous(e.g., fire, flood, earthquake) the process moves on to disaster recovery and BCP.A **disaster recovery plan (DRP)** deals with the preparation for and recovery from a disaster, whether natural or man-made and it is closely associated with BCP.

A **Business continuity plan (BCP)** ensures that critical business functions continue, if a catastrophic incident or disaster occurs. 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 Contingency Planning



There are six steps to contingency planning. They are

1. Identifying the mission-or business-critical functions,
2. Identifying the resources that support the critical functions,
3. Anticipating potential contingencies or disasters,
4. Selecting contingency planning strategies,
5. Implementing the contingencies strategies,
6. Testing and revising the strategy.

1. Incident response plan (IRP)

- It is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.
- IRP consists of the following 4 phases:
    1. Incident Planning
    2. Incident Detection
    3. Incident Reaction
    4. Incident Recovery

1.1. Incident Planning

- Planning for an incident is the first step in the overall process of incident response planning.
- The planners should develop a set of documents that guide the actions of each involved individual who reacts to and recovers from the incident.
- These plans must be properly organized and stored to be available when and where needed, and in a useful format.

1.2. Incident Detection

- Incident Detection relies on either a human or automated system, which is often the help desk staff, to identify an unusual occurrence and to classify it properly as an incident.
- The mechanisms that could potentially detect an incident include intrusion detection systems (both host-based and network based), virus detection software, systems administrators, and even end users.
- Once an attack is properly identified, the organization can effectively execute the corresponding procedures from the IR plan. Thus, **incident classification** is the process of examining a potential incident, or **incident candidate**, and determining whether or not the candidate constitutes an actual incident.

- **Incident Indicators-** There is a number of occurrences that could signal the presence of an incident candidate.
- **Donald Pipkin**, an IT security expert, identifies three categories of incident indicators:
    - **Possible Indicators**
    - **Probable Indicators**
    - **Definite Indicators**

Possible Indicators- There are 4 types of possible indicators of events ,they are,

1. Presence of unfamiliar files.
2. Presence or execution of unknown programs or processes.
3. Unusual consumption of computing resources
4. Unusual system crashes

Probable Indicators- The four types of probable indicators of incidents are

1. Activities at unexpected times.
2. Presence of new accounts
3. Reported attacks

4. Notification from IDS

Definite Indicators- The five types of definite indicators of incidents are

1. Use of Dormant accounts
2. Changes to logs
3. Presence of hacker tools
4. Notifications by partner or peer
5. Notification by hacker

1.3. Incident Reaction

- It consists of actions outlined in the IRP that guide the organization in attempting to stop the incident, mitigate the impact of the incident, and provide information for recovery from the incident.
- These actions take place as soon as the incident itself is over.
- In reacting to the incident there are a number of actions that must occur quickly, including notification of key personnel and documentation of the incident.
- These must have been prioritized and documented in the IRP for quick use in the heat of the moment.

1.4. Incident Recovery

- The recovery process involves much more than the simple restoration of stolen, damaged, or destroyed data files. It involves the following steps.
  1. Identify the Vulnerabilities
  2. Address the safeguards.
  3. Evaluate monitoring capabilities
  4. Restore the data from backups.
  5. Restore the services and processes in use.
  6. Continuously monitor the system
  7. Restore the confidence of the members of the organization's communities of interest.

Business continuity plan

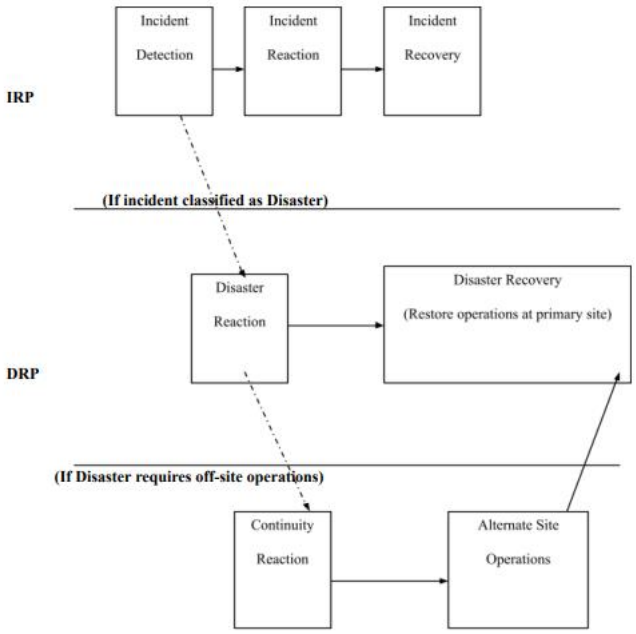
- It prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.
- If a disaster has rendered the current location unusable for continued operations, there must be a plan to allow the business to continue to function.

Developing Continuity Programs

- Once the incident response plans and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster.

- The development of the BCP is simpler than that of the IRP and DRP ,in that it consists of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy.

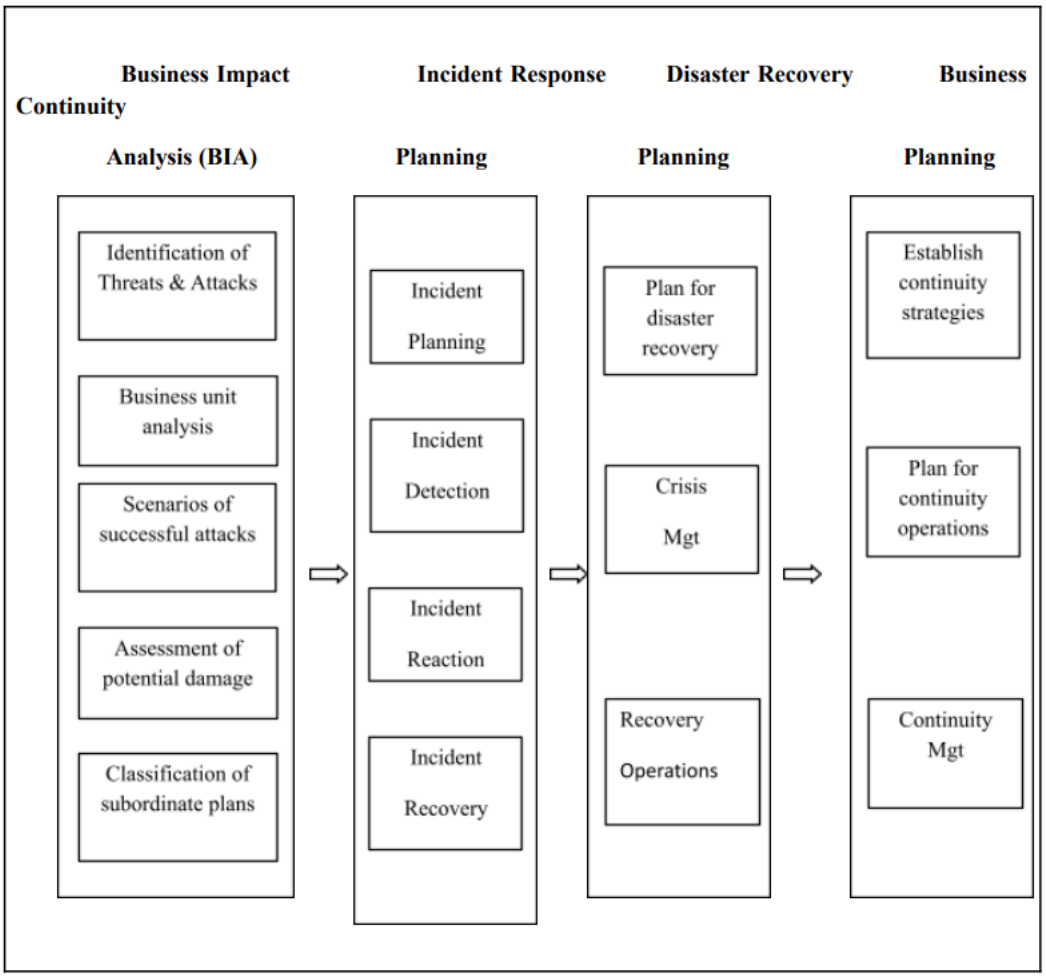
Contingency Planning Time line



BCP

Attack Occurs **Post – Attack (Hours)** **Post – attack (days)**

Major Steps in Contingency Planning


Business Impact Analysis (BIA)
Identification of Threats & 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 Mgt
Recovery Operations
Business Continuity Planning
Establish continuity strategies
Plan for continuity operations
Continuity Mgt

Continuity Strategies

- There are a number of strategies from which an organization can choose when planning for business continuity.
- The determining factor in selection between these options is usually cost.
- In general there are three exclusive options: Hot sites, Warm Sites, and Cold sites; and three shared functions: Time-share, Service bureaus, and Mutual Agreements.

 Hot sites:

A hot site is a fully configured facility, with all services, communications links, and physical plant operations including heating and air conditioning.

 Warm sites:

A warm site includes computing equipment and peripherals with servers but not client work stations. It has many of the advantages of a hot site, but at a lower cost.

 Cold Sites:

A cold site provides only rudimentary services and facilities, No computer hardware or peripherals are provided. Basically a cold site is an empty room with heating, air conditioning, and electricity. The main advantage of cold site is in the area of cost.

- **Time-shares**:

  It allows the organization to maintain a disaster recovery and business continuity option, but at a reduced overall cost. The advantages are identical to the type of site selected(hot, warm, or cold). The disadvantages are the possibility that more than one organization involved in the time share may need the facility simultaneously and the need to stock the facility with the equipment and data from all organizations involved

- **Service bureaus:**

  A service bureau is an agency that provides a service for a fee. In the case of disaster recovery and continuity planning, the service is the agreement to provide physical facilities in the event of a disaster. These types of agencies also provide off-site data storage for a fee. The disadvantage is that it is a service, and must be renegotiated periodically. Also, using a service bureau can be quite expensive.

- **Mutual Agreements:**

  A mutual agreement is a contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

Disaster Recovery Plan (DRP)

DRP provides detailed guidance in the event of a disaster and also provides details on the roles and responsibilities of the various individuals involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified. At a minimum, the DRP must be reviewed during a walk-through or talk-through on a periodic basis.
Many of the same precepts of incident response apply to disaster recovery:

1. There must be a clear establishment of priorities
2. There must be a clear delegation of roles and responsibilities
3. Someone must initiate the alert roster and notify key personnel.
4. Someone must be tasked with the documentation of the disaster.
5. If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization.