DAMAGE ASSESSMENT AND DISASTER RECOVERY PLANNING

Damage Assessment

- There are several sources of information:
  - including system logs.
  - intrusion detection logs.
  - configuration logs and documents.
  - documentation from the incident response.
  - results of a detailed assessment of systems and data storage.
- Computer evidence must be carefully collected, documented, and maintained to be acceptable in formal proceedings.
- Recovery

In the recovery process:

- Identify the vulnerabilities that allowed the incident to occur and spread and resolve them.
- Address the safeguards that failed to stop or limit the incident, or were missing from the system in the first place. Install, replace or upgrade them.
- Evaluate monitoring capabilities. Improve their detection and reporting methods, or simply install new monitoring capabilities.
- Restore the data from backups.
- Restore the services and processes in use.
- Continuously monitor the system.
- Restore the confidence of the members of the organization's communities of interest.

- Conduct an after-action review.

Disaster Recovery Planning

- Disaster recovery planning (DRP) is planning the preparation for and recovery from a disaster.
- The contingency planning team must decide which actions constitute disasters and which constitute incidents.
- When situations are classified as disasters plans change as to how to respond - take action to secure the most valuable assets to preserve value for the longer term even at the risk of more disruption.
- DRP strives to reestablish operations at the 'primary' site.

DRP Steps

- There must be a clear establishment of priorities.
- There must be a clear delegation of roles and responsibilities.
- Someone must initiate the alert roster and notify key personnel.
- Someone must be tasked with the documentation of the disaster.

Crisis Management

- Crisis management is actions taken during and after a disaster focusing on the people involved and addressing the viability of the business.
- The crisis management team is responsible for managing the event from an enterprise perspective and covers:
  - Supporting personnel and families during the crisis.

- Determining impact on normal business operations and, if necessary, making a disaster declaration.
- Keeping the public informed.
- Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties.

Business Continuity Planning

- Business continuity planning outlines reestablishment of critical business operations during a disaster that impacts operations.
- If a disaster has rendered the business unusable for continued operations, there must be a plan to allow the business to continue to function.

Continuity Strategies

There are a number of strategies for planning for business continuity

- In general there are three exclusive options:
  - hot sites
  - warm sites
  - cold sites
- And three shared functions:
  - timeshare
  - service bureaus
  - mutual agreements