Business Continuity

Business Continuity Planning (BCP)

- Identifying exposure to threats
- Creating preventative and recovery procedures
- Testing them to see if they're sufficient

consists of 3 factors:

- Business Recovery Planning
- Crisis Management and Communications
- Disaster Recovery

Business Impact Analysis (BIA)

> Identifies business functions and quantifies the impact of loss

Impact on:

- property (tangible assets)
- finance (monetary funding)
- safety (physical protection)
- reputation (status)
- life (well-being)

Derivations

- *mission-essential function* - activity that serves as the core function of the enterprise
- *critical system* - the support of the mission-essential function
- *single-point of failure* (SPOF)
- *privacy impact assessment*
- *privacy threshold assessment*

Disaster Recovery Plan (DRP)

> Document focusing on protecting and restoring IT functions, and updated regularly

Most DRPs:

- Have a common set of features
- Cover specific topics
- Require testing for verification

Typical Outline:

1. Purpose and Scope
2. Recovery Team
3. Preparing for a Disaster

4. Emergency Procedures
5. Restoration Procedures

- What systems have priority to be restored over others?
- What should be done if a disaster makes the current location no longer available?
- *Failback* - resync data back to primary location

Disaster Exercises

Objectives:

- Test interdepartmental planning and coordination
- Test current DRP procedures
- Determine response strengths and weaknesses

Vocab:

- Tabletop Exercises - Simulate emergency situation informally and stress-free environment
- Fault Tolerance
- Mean-Time to Recovery (MTTR) - Average time it takes for a device to recover from non-terminal failure
- Mean-Time Between Failures (MTBF)
- Redundant Array of Independent Devices (RAID)
- Redundancy Planning - Servers, Storage, Networks, Power, Sites, Data
- Asymmetric Server Cluster - data oriented
- Symmetric Server Cluster - service oriented

RAID

- RAID 0 - Data is striped across drives - no redundancy, only increased performance
- RAID 1 - Data is mirrored across drives - all redundancy, no performance
- RAID 5 - Data has error parity across drives - no redundancy, no performance, increased error checking
- RAID 01 - Mirrored Stripes
- RAID 10 - Striped Mirrors

Networks

- Software Defined Networks (SDN)
- Backup ISP

Power

- Uninterruptible Power Supply (UPS)
  - Offline vs Online - Boots vs. Always Running
  - Can ensure proper shutdown occurs

- Backup Generators

Recovery Sites

- Hot - Everything's good to go, just need the data
- Cold - Just the office space
- Warm - All equipment, just no telecom

Data

- Recovery Point Objective (RPO) - Max time between backups
- Recovery Time Objective (RTO) - Length of time it will take to recover backed-up data
- *Full Backup* → only full is needed
- *Differential Backup* → full + latest diff
- *Incremental Backups* → full + sum incrementals
- *Continuous Data Protection* (CPS)
- *Automatic Continuous Backup*
- *Universal Access*
- *Delayed Deletion*

3-2-1:

- Three different copies
- Two different mediums
- One stored elsewhere

Environmental Controls

- Fire suppression
- Electromagnetic Disruption suppression
- HVAC

Incident Response Plan (IRP)

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Forensic Procedures:

- Secure the Crime Scene
- Preserve the Evidence
- Establish a Chain of Custody
- Examine the Evidence
- Enable Recovery