**Backup and Disaster Recovery**

1. A medium size criminal defense law firm in San Francisco.
There are five partners, 50 attorneys and 15 support staff including an administration manager and an IT administrator. The company specializes in cases of murder, racketeering, grand theft etc. It also works with private investigators and has a large database of very sensitive information on clients, suspects, law enforcement and judicial officers.

-Meeting place in the case of disaster
-Emergency communication devices
-Data backups

2. A stock broker and financial consultant.
There are 100 employees in three different locations, New York, Dallas and Seattle. Half of the staff is located on Wall Street in New York; the others are evenly divided between the two other locations. Remember the nature of business. When the markets are open, there is constant flow of transactions and trades happening. Also remember that they are keeping records of clients worth billions of dollars in total and any serious breach of security or data loss can put them out of business.

-Meeting place in the case of disaster
-Communication backups
-Evacuation procedures
-Emergency communication devices
-Data backups

**Disaster Recovery**

Disaster recovery involves creating, implementing, and testing disaster recovery plans. These plans typically include procedures to address redundancy and fault tolerance as well as data backups.

Disaster Recovery Plan (DRP): A written document that details the process for restoring IT resources following an event that causes a significant disruption in service.

The goal of an IT contingency plan is to ensure that the business will continue to function at an acceptable level in the face of a major IT incident or a disaster. Closely related is a disaster recovery plan (DRP), which is involved with restoring the IT functions and services to their former state.

All disaster recovery plans are different, but most address the common features included in the following typical outline:

| | | |
|---|---|---|
| Unit 1: Purpose and Scope | The reason for the plan and what it encompasses are clearly outline. Those incidences that require the plan to be enacted also should be listed. | -Introduction<br>-Objectives and constraints<br>-Assumptions<br>-Incidents requiring action<br>-Contingencies<br>-Physical safeguards<br>-Types of computer service disruptions<br>-Insurance considerations |

| | | |
|---|---|---|
| Unit 2: Recovery Team: | The team that is responsible for the direction of the disaster recover plan is clearly defined. It is important that each member knows her role in the plan and be adequately trained. This part of the plan is continually reviewed as employees leave the organization, home telephone or cell phone numbers change, or new members are added to the team. | -Organization of the disaster/ recovery team<br>-Disaster/recovery team headquarters<br>-Disaster recovery coordinator<br>-Recovery team leaders and their responsibilities |
| Unit 3: Preparing for a Disaster | A DRP lists the entities that could impact an organization and also the procedures and safeguards that should constantly be in force to reduce the risk of the disaster. | -Physical/security risks<br>-Environmental risks<br>-Internal risks<br>-External risks<br>-Safeguards |
| Unit 4: Emergency Procedures | The Emergency Procedures unit answers the questions, "What should happen when a disaster occurs?" | -Disaster recovery team information<br>-Vendor contact list<br>-Use of alternate sites<br>-Offsite storage |
| Unit 5: Restoration Procedures | After the initial response has put in place the procedures that allow the organization to continue functioning, this unit addresses how to fully recover from the disaster and return to normal business operations. | -Central facilities recovery plan<br>-Systems and operations<br>-Scope of limited operations at central site<br>-Network communications<br>-Computer recovery plan |

Test the Disaster Recovery Plan - Tabletop Exercise

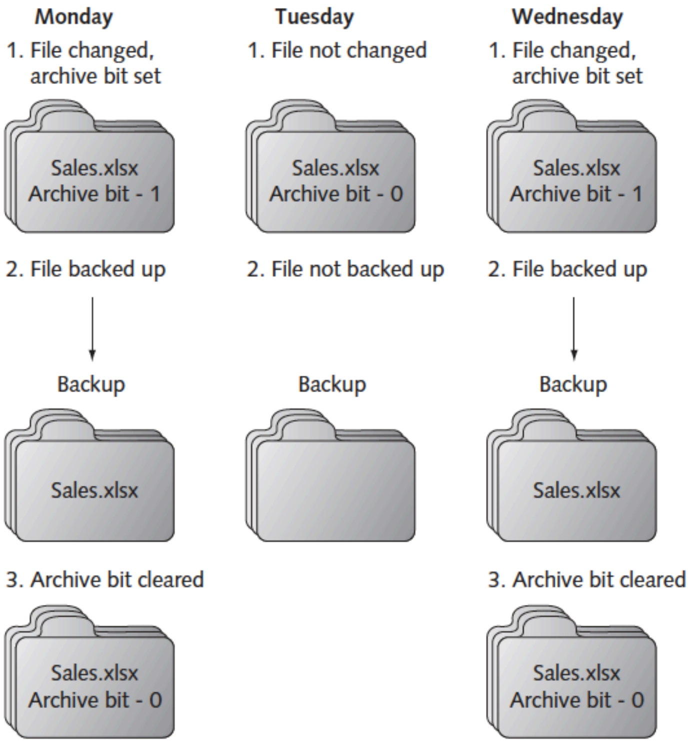
| Feature | Description |
|---|---|
| Participants | Individuals on a decision-making level |
| Focus | Training and familiarizing roles, procedures, and responsibilities |
| Setting | Informal |
| Fornat | Discussion guided by a facilitator |
| Purpose | Identify and solve problems as a group |
| Commitment | Only moderate amount of time, cost, and resources |
| Advantage | Can acquaint key personnel with emergency responsibilities, procedures, and other members |
| Disadvantage | Lack of realism; does not provide true test; |

**Data Backups**

Another essential element in any DRP is data backups. A data backup is copying information to a different medium and storing it (preferably at an offsite location) so that it can be used in the event of a disaster.

When creating a data backup plan or policy, five basic questions should be answered:
1. What information should be backed up?
2. How frequently should it be backed up?
3. What media should be used?
4. Where should the backup be stored?
5. What hardware or software should be used?

Example - Which files need to be backed up? - Archive Bit



There are three basic types of backups: full backup, differential backup, and incremental backup. The archive bit is not always cleared after each type of backup; this provides additional flexibility regarding which files should be backed up.

| Type of Backup | How used | Archive bit after backup | Files needed for recovery |
|---|---|---|---|
| Full backup | Starting point for all backups | Cleared (set to 0) | The full backup is needed |
| Differential backup | Backs up any data that has changed since last full backup | Not cleared (set to 1) | The full backup and only last differential backup are needed |
| Incremental backup | Backs up any data that has changed since last full backup or last incremental backup | Cleared (set to 0) | The full backup and all incremental backups are needed |

- CompTIA® Security+ Guide to Network Security Fundamentals