**Chapter 18: Disaster Recovery Planning**

Natural disasters reflect the occasional fury of our habitat—violent occurrences that result from changes in the earth’s surface or atmosphere that are beyond human control.

Earthquakes are caused by the shifting of seismic plates and can occur almost anywhere in the world without warning.

Some flooding results from the gradual accumulation of rainwater in rivers, lakes, and other bodies of water that then overflow their banks and flood the community. Other floods, known as flash floods, strike when a sudden severe storm dumps more rainwater on an area than the ground can absorb in a short period of time.

Pandemics pose a significant health and safety risk to society and have the potential to disrupt business operations in a manner unlike many other disasters.

Human-Made Disasters

* Fires
* Act of terrorism
* Bombing / Explosions
* Power Outages

A single point of failure (SPOF) is any component that can cause an entire system to fail.

System resilience refers to the ability of a system to maintain an acceptable level of service during an adverse event.

Fault tolerance is the ability of a system to suffer a fault but continue to operate. Fault tolerance is achieved by adding redundant components.

High availability is the use of redundant technology components to allow a system to quickly recover from a failure after experiencing a brief disruption. High availability is often achieved through the use of load balancing and failover servers.

RAID - Redundant Array of Independent disks

RAID-0 This is also called striping. It uses two or more disks and improves the disk subsystem performance, but it does not provide fault tolerance.

RAID-1 This is also called mirroring. It uses two disks, which both hold the same data. If one disk fails, the other disk includes the data so that a system can continue to operate after a single disk fails.

RAID-5 This is also called striping with parity. It uses three or more disks with the equivalent of one disk holding parity information. This parity information allows the reconstruction of data through mathematical calculations if a single disk is lost.

RAID-6 This offers an alternative approach to disk striping with parity. It functions in the same manner as RAID-5 but stores parity information on two disks, protecting against the failure of two separate disks but requiring a minimum of four disks to implement.

RAID-10 This is also known as RAID 1 + 0 or a stripe of mirrors, and it is configured as two or more mirrors (RAID-1), with each mirror configured in a striped (RAID-0) configuration. It uses at least four disks but can support more as long as an even number of disks are added. It will continue to operate even if multiple disks fail, as long as at least one drive in each mirror continues to function.

Fault tolerance is not the same as a backup. If a catastrophic hardware failure destroys a RAID array, all the data is lost unless a backup exists.

Both software- and hardware-based RAID solutions are available

A failover cluster includes two or more servers, and if one of the servers fails, another server in the cluster can take over its load in an automatic process called failover.

Fault tolerance can be added for power sources with a UPS, a generator, or both. UPS ensures uninterrupted power supply and provides up to 30 minutes of time to turn on the generator for long term power supply.

Trusted recovery provides assurances that after a failure or crash, the system is just as secure as it was before the failure or crash occurred.

Quality of service (QoS) controls protect the availability of data networks under load.

* Bandwidth - The network capacity available to carry communications.
* Latency - The time it takes a packet to travel from source to destination.
* Jitter - The variation in latency between different packets.
* Packet Loss - Some packets may be lost between source and destination, requiring retransmission.
* Interference - Electrical noise, faulty equipment, and other factors may corrupt the contents of packets.

Cold sites are standby facilities large enough to handle the processing load of an organization and equipped with appropriate electrical and environmental support systems. The time to activate a cold site is often measured in weeks, making a quick recovery close to impossible and often yielding a false sense of security.

A hot site is the exact opposite of the cold site. In this configuration, a backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities. The servers and workstations are all preconfigured and loaded with appropriate operating system and application software. The data on the primary site servers is periodically or continuously replicated to corresponding servers at the hot site, ensuring that the hot site has up-to-date data. Switchover times for most hot sites are often measured in seconds or minutes.

Warm sites occupy the middle ground between hot and cold sites for disaster recovery specialists. Unlike hot sites, warm sites do not typically contain copies of the client’s data and/or application softwares pre-configured. Activation of a warm site typically takes at least 12 hours from the time a disaster is declared.

Mobile sites are non-mainstream alternatives to traditional recovery sites. They typically consist of self-contained trailers or other easily relocated units. These sites include all the environmental control systems necessary to maintain a safe computing environment. Mobile sites are usually configured as cold sites or warm sites.

Many organizations now turn to cloud computing as their preferred disaster recovery option. Companies wishing to maintain their own data centers may choose to use these IaaS options as backup service providers.

Mutual assistance agreements (MAAs), also called reciprocal agreements, are popular in

disaster recovery literature but are rarely implemented in real-world practice. Under an MAA, two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources. Many drawbacks inherent to MAAs prevent their widespread use such as difficulty to enforce, Confidentiality concerns, etc.

Database Recovery Techniques

* In an electronic vaulting scenario, database backups are moved to a remote site using bulk transfers. The entire database backup files are transferred periodically in a few days to the backup site.
* With remote journaling, data transfers still occur in a bulk transfer mode, but they occur on a more frequent basis, usually once every hour and sometimes more frequently. Unlike electronic vaulting scenarios, only the database transaction logs since the previous bulk transfer are transferred.
* Remote mirroring is the most advanced database backup solution. A live database server is maintained at the backup site. The remote server receives copies of the database modifications at the same time they are applied to the production server. Therefore, the mirrored server is ready to take over an operational role at a moment’s notice.

There are three main types of backups:

Full Backups - As the name implies, full backups store a complete copy of the data contained on the protected device. Full backups duplicate every file on the system regardless of the setting of the archive bit. Once a full backup is complete, the archive bit on every file is reset, turned off, or set to 0.

Incremental Backups - Incremental backups store only those files that have been modified since the time of the most recent full or incremental backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated. Once an incremental backup is complete, the archive bit on all duplicated files is reset, turned off, or set to 0.

Differential Backups - Differential backups store all files that have been modified since the time of the most recent full backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated. However, unlike full and incremental backups, the differential backup process does not change the archive bit.

The most important difference between incremental and differential backups is the time needed to restore data in the event of an emergency. Differential backup takes less time to restore but requires more storage and time to create. Incremental backup on the other hand, takes less time and storage to create but requires more time to restore.

DRP Testing

* Read-Through Test - In this test, you distribute copies of disaster recovery plans to the members of the disaster recovery team for review.
* Structured Walk-Through - In this type of test, often referred to as a tabletop exercise, members of the disaster recovery team gather in a large conference room and role-play a disaster scenario.
* Simulation Test - In simulation tests, disaster recovery team members are presented with a scenario and asked to develop an appropriate response. This may involve the interruption of noncritical business activities and the use of some operational personnel.
* Parallel Test - Parallel tests represent the next level in testing and involve relocating personnel to the alternate recovery site and implementing site activation procedures. Operations at the main facility are not interrupted.
* Full-interruption tests operate like parallel tests, but they involve actually shutting down operations at the primary site and shifting them to the recovery site. These tests involve a significant risk and are therefore extremely difficult to arrange.

Once a disaster interrupts the business operations, the goal of DRP is to restore regular business activity as quickly as possible. Thus, disaster recovery planning picks up where business continuity planning leaves off. The goal of business continuity is preventing business interruption.