SCVdata
support@SCVdata.com
(661) 600-5333

. . . I have always found that plans are useless, but planning is indispensable.
— DWIGHT D. EISENHOWER

Backups and Disaster Recovery Planning

• Define the scope of your plan

- What is your tolerance for data loss?

- Which exactly are the critical systems and data files?

- What are the different scenarios to plan for? Loss of building (fire, collapse)? Public services (phone, electricity)? Damage to equipment (flood, vandalism, theft)?

Recover Point Objective (RPO) — the age, or "freshness," of the data available to be restored.

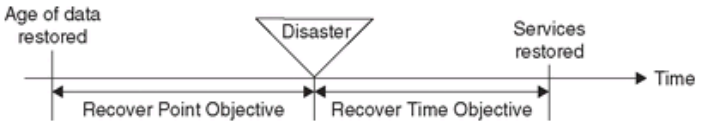
- Is last week's backup good enough, or do we need to be able to restore more current data?

Recover Time Objective (RTO) — The amount of time between the disaster, and when services are restored.

- How quickly do you have to recover those critical applications and services (Seconds? Minutes? Hours? Days?)

- How long of an interruption should be planned for? (Days? Weeks? Indefinitely?)

- How quickly do I need access to my data and systems?



• Create a Disaster Recovery Plan

Communication plan: A plan for contacting key personnel, customers, vendors, etc. Can you contact the necessary people after hours?

Documentation: Written material describing the existing environment, procedures for declaring a disaster, procedures for re-establishing services in a disaster recovery mode, duplicate copies in office and at home.

Real estate and IT facilities: Where will people meet if the facility is suddenly off-limits, inaccessible, or out of commission? Proximity to your location? Where can you set up servers and what are the costs associated?

Off-site storage of data: If your facility is destroyed, or inaccessible, you'll want to be sure you have an up-to-date copy of your data at an off-site facility. Backup hard drives? Data Replication?

Hardware availability: You want to make sure that you can get replacement hardware if yours is destroyed. This list could include workstations, servers, routers, switches, hard drives, etc. Entire environment or just select portions?

Regular updating and testing: Your environment changes regularly (technology, people, needs, organization, procedures, etc.). You need to regularly test and update your disaster recovery plan to make sure it retains its value.

• Assess the Cost of Implementing Your Plan

- Is your business valuable enough that you should spend some money to protect it? How much is reasonable?

- Which risks are the most important for you to plan for? How do they align with your budget?

- Is it reasonable that you could implement your plan immediately? Or should you roll it out over the next 5 years?