

Disaster Recovery and Electronic Document Management

By: Andrew Bailey

Nearly 18,000 businesses were dislocated, disrupted or destroyed by 9/11. Thousands more were affected by Hurricane Katrina. According to research by the University of Texas, only 6 percent of companies suffering from a catastrophic data loss survive, while 43 percent never reopen and 51 percent close within two years.

If you come into work one morning to find your office has been destroyed, would your business recover?

- Would you lose all of your paper documents?
- Are electronic documents that are scattered across many different workstations now useless?
- Have you lost valuable email messages?
- Where are your customer, vendor and employee records?
- What would you do?

Paper documents stored in file cabinets are susceptible to fire and flood. You cannot recover a paper document that has been destroyed by a fire or a flood. But the problem goes beyond your paper files. Electronic documents stored on hard drives on workstations and servers across your operation are equally vulnerable to catastrophic loss.

Nobody wants to think they might need to implement a disaster recovery plan, but proper planning could enable your company to survive a disaster.

What processes does your business have in place for backing up critical data? Consider where and how your paper documents are stored. Think about important electronic documents within your network. Now, lock the doors and walk away. How would your company re-establish operations? If you take that thought process and expand it and begin thinking about what you would need to resume operations then you have the beginnings of a disaster recovery plan. This paper addresses specific ways to ensure that your documents can be recovered. But keep in mind, there are many other aspects to your overall recovery plan.

Let's tackle the issue of centralized document management first. If you currently don't have an **Electronic Document Management System (EDMS)**, then electronic documents are most likely not consolidated in your organization and fragile paper documents are stored on desks and in filing cabinets on-site.

By definition, EDMS is software that controls and organizes documents. This involves scanning paper documents, filing them accordingly, and making them available to view across your business. In

addition to paper documents, electronic documents and email can also be stored in the EDMS. An EDMS will provide consolidation of all important documents within an organization regardless of the type of document. This consolidation creates a centralized electronic repository that not only improves operational efficiency, but also makes it possible to create and implement a successful disaster recovery plan.

The first level of disaster recovery is to have the EDMS installed on a RAIDⁱ drive array to prevent a single point of failure within the system. Regardless of how efficient and robust the EDMS is, without a comprehensive disaster recovery plan you could potentially lose valuable documents. After document centralization using an EDMS, the next step is to create a disaster recovery plan to ensure access to those important documents in the event of a disaster.

The data backup schedule is perhaps the most important consideration when planning for disaster recovery. It is critical to plan backups around restoration requirements.

There are different types of backup plans, which have pros and cons associated with them. Here are explanations for a few of the common types of backup processes.

Full Backups

One possible backup scenario is to store your entire system to a tape or other backup media at the end of each work day. The benefit of this scenario is that in a recovery situation, you only need to handle one backup media set. The disadvantage is that, since all files (including those that have not changed), are backed up every day, the amount of time and media needed to complete the backup increases greatly.

Cumulative Backups

Another strategy is to perform a full backup once per week (typically on the weekend) and partial cumulative backups on all other work days. This strategy reduces both the time required to perform the backup and media usage. In a cumulative backup, you are always backing up everything since the date of the last full backup.

Following a cumulative backup strategy, you will need to have only two tapes or other medium to perform a full system recovery: the most recent full backup and the most recent partial (cumulative) backup.

Incremental Backups

In an incremental backup strategy, you perform a full backup once per week (typically on the weekend) and partial backups on all other days. However, since the date of each partial backup is the date of the last partial backup (not the date of the last full backup), only those files which have changed are copied to the tape or other medium.

The principal advantage to the incremental backup strategy is that it uses the smallest amount of time and backup media. The disadvantage is that, in the event of a system recovery, you must restore each backup set from the most recent full backup through the most recent partial backup.

All of these backup plans are viable and you will need to determine the best approach based on your requirements, personnel, hardware and software. Regardless of which plan you implement it's also critical to ensure that your backup medium is stored off-site. You may elect to implement your backup strategy across the internet and there are many options available for this choice. This ensures that your valuable data is backed up to an off-site location without having to physically remove the backup medium from your office location. A simple internet search will return a wealth of companies that offer this service.

A backup plan presumes a restore plan; your backup plan should always be based on your requirements for restoring data. You should carefully test and document all of the processes and time required to fully recover your servers from backup data. Use the results of this testing to establish the requirements for your backup schedules.

Now that we have covered document consolidation and backup strategies we are well on our way towards creating and implementing a disaster recovery plan.

Summary

In the event of a disaster, the goal is to be able to quickly procure a temporary office, install computer systems and restore all required documents and information to enable a business to function. The biggest differentiator between a backup plan and a disaster recovery plan is maintaining a copy of your critical documents in an off-site location. By following the steps listed below and utilizing what we have learned in this document, this should be a manageable process.

- Consolidate documents of all types into an EDMS
- Create a backup strategy
- Implement your backup processes
- Test your restore capabilities
- Ensure your backup medium is stored at an off-site location

Definition:

ⁱ Wikipedia: "RAID" is now used as an umbrella term for computer data storage schemes that can divide and replicate data among multiple hard disk drives. The different schemes/architectures are named by the word RAID followed by a number, as in RAID 0, RAID 1, etc. RAID's various designs involve two key design goals: increased data reliability or increased input/output performance. When multiple physical disks are set up to use RAID technology, they are said to be *in a RAID* array. This array distributes data across multiple disks, but the array is seen by the computer user and operating system as one single disk. RAID can be set up to serve several different purposes.