Chapter 3 - Networking and Group Computing

Disaster Recovery

Disaster recovery is a term given to the process of recovering and/or protecting your hardware, software and data from being damaged or destroyed. A disaster recovery plan is a method of restoring information-processing operations that have been halted by destruction or by accident. With the significant investment in technology and the critical role it plays in your firm's daily operations, it is essential that a disaster recovery plan be given top priority.

Backing up your data. The amount of critical electronic legal data piling up in law firms is staggering. Document management, calendars, e-mails, word-processing documents, multimedia, etc is causing backup and storage solutions to be a fast growing and critical issue in your practice. Your present backup servers may be adequate but what happens in case of a fire, theft and other problems? There are a variety of data storage solutions available to restore data lost or corrupted due to disasters. Please refer to Chapter 2, Data Storage Devices for further information on data storage options.

There are two primary goals of a well thought out backup plan:

1. The system must be invulnerable to fire, theft, corruption, etc.; and

2. You must have accessibility when you need to restore data. People often ask how much and often should you backup your data.

One response is: how critical to your practice would it be if you lost an entire day's data that was entered into your case management, word processing and other software applications on that day?

The best and most common approach is to backup your entire system everyday. Then, if you have a crash you can restore your entire system. Also, it is suggested that full backups of your data be done instead of incremental backups. It is difficult to restore a corrupted hard drive using incremental backups. Many firms use five sets of backup tapes, disks, or whatever other media they use one for each day of the week. However, a file deletion may not be noticed for a

few days or weeks. Therefore, backup everyday, one backup for each week, and one backup for each month for 3 months. Remember to retire tapes that are worn out. A fireproof safe provides little or no protection for magnetic tapes and other media since they can be damaged by heat. It is suggested that you take backup tapes off the premises and start backups late at night when people have left the office.

Web Storage - Web storage and backup capability is being offered that may now provide solutions to your back up issues. Web storage features to consider include:

- File security;
- Global access with a web browser;
- Relatively low cost;
- Ease of use;
- Encryption of data;
- Incremental backup available;
- Off-hour backup capability;
- CD-ROM backups are sent to you at selected intervals; and
- Restoration features.

On-line storage vendors include www.idrive.com and www.driveway.com . Below is a comparison of CD-ROM/DVD and On-line Storage. With CD-R's and DVD's drives, it is easy to "burn" your own optical disks for storage purposes. See Chapter 2, *Hardware and Software, CD-ROM.*

CD-ROM/DVD Document Storage	**ASP – Internet Storage**
Interface	Browser or client based	Browser based
Hardware	CD-ROM/DVD device - can be networked based	Access to the Internet
Access to new data	Must burn a new CD-ROM/DVD	Storage data can be easily and
Changeability of data	Read only access	Edit or read only
Media vulnerability	Can be damaged or lost	A file server at the ISP can be da
New users	Immediate if networked based	Can gain immediate access
# Of users	Depends on # of computers	Unlimited
Download time	Fast	Depends on connection

Hard Drive Backup

There are other backup options called mirroring and duplexing. Both options involve the use of backup hard drives. Essentially, both hard drives contain the same data, so if one hard drive fails the other automatically takes over. When two hard drives mirror the same data, they are running from one disk controller card. Duplexing is when two disks mirror each other but also run from two separate hard disks controllers. Duplexing is safer and faster. Fault tolerant drives are drives that mirror or contain the same data on a separate drive. In the case of failure of a drive, the other drive will take over and business can proceed as usual. In some cases, more than one drive will be mirrored so more than one backup drive is available. However, if the power supply goes down or the motherboard or memory chips fail, your system can still crash.

Other Considerations:

- *Archiving.* Archiving is intended as a long-term storage of important information. Make sure archived data can be read in 10-20 years with existing equipment, such as CD-ROM drives, etc.
- *Software*. Another restore option is using software that permits you to go back in time. If a problem occurs or you lose data, you can retrieve certain files or restore your whole hard drive. Both Windows XP and Vista have this capability. Whether the trouble is a virus, installation problems with new software, or another problem, you can go back and start over.

- *Data equipment racks*. These are used to keep your servers and other equipment off the floor and securely anchored in a central location. If you live in earthquake country, this additional bracing is needed.
- *Surge Protectors.* Guarding Against power fluctuations - Electricity is supposed to flow from an outlet at a steady voltage flow. However, fluctuations by either an increase or decrease in electricity can cause severe damage to your computer. An increase in electricity can be a spike lasting a fraction of a second or a surge lasting longer. A surge can burn out the circuitry in a computer system. A decrease can be a momentary lag or a brownout lasting longer. Sags and brownouts can produce a slowdown of the hard drive or system, or a system shutdown.A surge protector prevents a high voltage spike from seriously damaging your computer hardware. They run around $40 for a quality protector to protect computer hardware, generally worth thousands of dollars. Ensure that they have electrical certifications and a warranty that provides for product damage replacement if the protector does not work. However, you may want to consider buying a combination surge protector and uninterruptible power supply (UPS). The battery powered UPS unit will provide approximately 10 minutes of

time or more to save your data and properly shut down your system. They cost between $150 and $450. Check out the American Power Conversion site at www.apc.com
.

- *Uninterruptible Power Supply (UPS).* An UPS is a backup power supply for your computer system. An UPS has an internal battery that will activate when it senses a loss of power to your system. Generally, it will stay on for a specified number of minutes and advanced systems will alert the users that the system will be shutting down within that time frame. Users can then save their data and power off. Consider UPS devices on key workstations, such as the MIS director's and others, to allow them to continue or complete their work. Also, some UPS devices can be stacked to allow for the system to continue operating for hours in case of a power shortage or stoppage. Using a UPS or uninterruptible power supply can solve a lag or brownout. An UPS is essentially a standby battery.

- *Dial-in access protection.* If you are away from the office, then dial-in access may be critical for you. Ensure that UPS and surge protectors protect the dial-in access components of your network.
- *Maintenance and support contracts*. Have maintenance contracts in place to replace the critical components of your system in case of a disaster. In the contract, set out the response time (usually 4 hours) tolerated to repair your problems. Include penalties for non-performance. Consider contracting with a company to set up an off site LAN to handle critical projects if the system cannot be fixed immediately. "Smart" disaster recovery software. Software is available to monitor the components of your system and warn you of impending failures. You can then take affirmative action before disaster strikes.

- *Off site server or Intranet server.* If you have an off site server, then remote employees can have access to instructions or other material if the main system is out of order. Also, you may want to set up an off site LAN to handle mission critical tasks while the system is being fixed.