

Be Prepared

Law firms have to protect not only their own business documents but also records vital to their clients' businesses and personal lives. **By Mark Williams**

Beyond fire extinguishers, posted evacuation routes and computer backups, few law firms are truly prepared for natural or manmade disasters - ranging from earthquakes and floods to computer viruses and terrorist attacks.

The danger to the very survival of a firm is magnified by the extremely fast pace of today's business and commerce, which significantly reduces the recovery time window.

Law firms are in a highly critical position with respect to both digital and paper records because of their fiduciary responsibility to their clients. Thus disaster and recovery planning becomes doubly imperative because firms have to protect not only their own business documents but also records vital to their clients' businesses and personal lives as well. Because disasters cannot be put on hold until businesses are ready, don't put disaster planning on hold while you attend to "more urgent" matters.

There are ten key areas of disaster preparedness.

- Take stock of your assets. Begin planning by identifying your critical business assets, which can include your data, equipment and buildings. While the safety of employees may be paramount, consider what would happen if your financial data, client contracts and documents, both hard copy and digital, were destroyed.

Identify what you would need to take with you or restore. Pay particular attention to your information technology resources with regard to all types of disasters large and "small." With your and your clients' heavy dependence on digital records, the impact of a virus, hacker or network crash could surpass that of a fire or flood. Even "small" disasters such as power and telephone outages can have serious consequences in terms of lost records and wasted employee resources.

- Play "what if?" Brainstorm the full range of manmade and natural disasters that could happen in your area.

For example, what if a disgruntled employee was to wipe out your hard drive? What if a power outage caused

total hardware failure? What if ceiling sprinklers malfunctioned, flooding your building? Assess everything that could possibly happen and how it would affect personnel, records and operations.

- Put your recovery plan in place. Develop a plan for every type of disaster, from simple measures such as regularly backing up computers and storing backups off-site, to establishing a phone chain and training employees on what to do and where to call for messages.

Establish an exchange program with out-of-state firms that can act as emergency contact points to communicate information to clients, employees and other stakeholders. (While the lines calling into your area may be tied up in an emergency, calling out of state is usually not a problem.)

Schedule regular practice drills. Establish procedures such as having everyone- staff members and visitors- sign in and out upon entering and leaving the building. Make sure everyone knows how to get out, what records to take with them and where to report. Employees may walk past fire exits every day without registering their presence and so may not recall their location in an emergency.

- Where do we go? If you cannot access the building after a disaster, you'll need a preplanned meeting site. Locate another building, coffee shop or parking lot now and tell everyone. Establish procedures for communicating with employees so you can tell them what to do.

If the building has been destroyed or will be inaccessible for the long term, do you have a place where you can set up your computers? After the Sept. 11 terrorist attacks, many compa-

nies took over hotel ballrooms. After a disaster, space and equipment will be in great demand. You will be ahead of the game if you have prior reservations.

- Take stock of human capital, equipment and data. Take an inventory and list the types of computer systems, number of phone and data lines, employees' homes phone numbers, internet service provider contact information, office equipment, etc.

If you cannot get back into your offices, you will need to have accurate information for vendors so you can duplicate operations at another loca-



tion. To maintain employee communication, consider distributing laminated cards to keep in your wallet with key people's contact information.

- Plan how to restore operations. If you have data backup tapes but your computers are a total loss, you will require funds to purchase new systems and hire someone to set them up, load the information and restore your data.

If your corporate checkbooks and credit cards are destroyed, how will you actually pay for these services? Identify vendors outside the area for services and items you will need to resume operations and establish how they will be paid.

- Getting up and running. It is imperative that all firms regularly back up computer data and store the backups off-site. The frequency of backing up depends on the amount of data you enter on a daily basis.

Whether you rely on internal personnel or a vendor for backup, check the backup files frequently.

Once your computers are backed up, do you really have the data you need to resume operations? What

exactly are employees backing up? Is it just a snapshot of data or the entire database? Consider keeping backups from six-months to a year back in addition to incremental backups. If someone inadvertently deletes key files at 8:00 a.m. and you do a backup at 8:05 a.m., you've just cemented the deletion of what could be critical files. You'll need both incremental and full backups. Establish solid archiving procedures, including off-site archiving.

- Adapt timing and employee load. If you cannot be fully operational for some time and don't require all your employees, give them the option of taking early vacations or working in shifts so everyone can remain on the payroll.

- Resume business. The more quickly you can get back to the business of law, the better for you and your clients. If you're operational before other firms, you'll have a competitive advantage.

- Implement a plan to repair or rebuild. If you were forced to move to another area, would you lose valuable employees? Plan for relocation in advance by consulting with a real estate professional. In rebuilding your practice, don't forget the potential long-term effects of stress and trauma, particularly if the disaster is a terrorist attack. Because counseling professionals will be in great demand after a disaster, consider arranging now for psychological and pastoral services.

While most businesses have good intentions when it comes to disaster preparedness, getting around to it is another matter. And when the job is assigned to employees who have many other tasks, it doesn't always get the attention it requires. Law firms that are adequately prepared to protect themselves and their clients' vital records have a significantly shorter recovery time and a competitive advantage.

Mark Williams is president of Los Angeles-based Williams Records Management, which works with law firms to archive and protect critical hard copy and electronic data.