Computer News for Law Firms

No. 20 | Heckman Consulting llc | October 2001

Small to Medium Firm Disaster Recovery

In the wake of the terrorist attack on the World Trade Center, many firms have felt the need to come to grips with the grisly subject of disaster recovery. In the past this topic has been evaded as either unnecessary or too costly. For example, a major law firm in downtown Manhattan was put out of business for nearly a week in the early 1990s in the wake of a power outage in lower Manhattan because it had rejected installing Uninterruptible Power Supplies for its mainframe computers as too expensive.

Disaster recovery plans fall into the same category as various kinds of insurance: you have it because you cannot afford not to. There are other similarities as well. Like an insurance plan, for more money you can have higher liability coverage (=more thorough recovery) as well as a lower deductible (= less time you are out of operation). There is no reason that firms should not perform the same analysis for disaster recovery that they do when purchasing any other type of insurance, be it car insurance, malpractice insurance, key man or business interruption insurance. The main difference is that disaster recovery does not depend on how "likely" something is to happen, because if a disaster does happen, it could put you out of business.

About This Newsletter

Heckman Consulting is a systems integration firm specializing in the legal market. John Heckman has over 18 years experience in the legal community and is featured as a "Top Tier Technologist" on www.lawcommerce.com. This newsletter is published periodically as a service to our clients and others. It contains items we find of interest.

Contact Heckman Consulting at:
One Fencove Court
Old Saybrook, CT 06475
Tel: (860) 395-0881
Fax: (860) 395-0386
e-mail: heckman@heckmanco.com

Electronic Disaster

The lowest level of disaster is a server crash of some sort. This has a very high likelihood of happening some time within a 5-10 year period. It can be either physical (the server dies) or inflicted from the outside, by a virus or disgruntled employee. Your goal in this case is to recover your data rapidly. The most common protection is a tape backup. However, there are several caveats you need to be aware of.

- You need to test your backup regularly to make sure it is "really" backing up. You can do this by copying the files from some random directory to somewhere else and then restoring that directory. Chances are that if you can restore a random directory, your tape backup is good.
- Many older backup systems do not back up open files. Most database-based programs (such as e-mail or case management programs) keep their databases open all the time. If your database is not being backed up, the tape is worthless for recovery. Determine whether your programs can be "suspended" during a tape backup (as Worldox can) or can automatically generate their own backups during the day (as Amicus can) so that even if the main database is not backed up at 2 am, the program backup made at 6 pm *is* backed up. Given the current state of backup drives, there is no reason to do anything but a full system backup (and CD backups are definitely totally inadequate).
- Tape backup drives and software become obsolete as quickly as other hardware and software in the computer industry. Therefore, even if you have a good tape, you may not be able to read it if your three year old tape drive/PC dies, because nobody makes or has that model any more. Yes, there are companies that specialize in recovering obsolete tapes or damaged hard drives, but they are quite expensive. The best solution is to buy a duplicate PC/server with duplicate tape backup and software, to be located outside the office. At today's prices, for a small office this could cost as little as $2,000-$3,000. This will ensure that you can actually restore the information in the event of a disaster.

Physical/Natural Disaster

What about a physical disaster to your office (fire, flood, etc.)?

- Have some form of off-site storage for your tapes (in addition to the backup machine). A fire safe is essentially worthless: while it may protect your tapes for an extra 15 minutes in the event of a fire, they will still melt down. Off-site storage does not need to be high-tech. For example, if an IT person or senior partner takes a weekly backup tape home, it provides off-site storage on a weekly basis.
- Even smaller firms may maintain a "convenience office" at a different location or in a different part of the state. Frequently, this is used simply for meeting clients. However, you might consider installing a "backup PC," loaded with all the standard firm software, at this location (including appropriate security precautions such as boot passwords).
- Most attorneys have some sort of "computer space" at home. Consider putting your backup PC in a den or spare bedroom and expanding your overall setup so that you have a phone line (for a modem) and perhaps a better printer. In short, consider making a "mini-office" at home. In the event of catastrophe, you could either work from there or move the entire setup to new space. Independent of the tape backup, you should also keep (and periodically update) copies of key items such as the firm's rolodex on this computer

How Much Down Time?

The second main question relating to disaster recover is how much of a "deductible" do you want, that is, how much data are you willing to reconstruct in the event of a disaster and how long can you afford for your firm to be inoperable? Banks, for example, cannot afford to be forced to "reconstruct" any data and their backup systems reflect this. However, for a

(Continued over)

Recovery *(Continued)*

small law firm the price of being able to recover *all* your data at any given point in time may be prohibitively expensive. In that case, you need to assess: am I willing to reconstruct 1 day of lost work; 2-3 days; 2 weeks? Two or three days would be onerous but not prohibitive, two or three weeks would probably be unacceptable.

Document Everything

For small firms, it may not be practical to image everything or have large off-site storage facilities. However, you should plan to store copies of essential business documents: leases, insurance policies, various licenses, etc. off site. This is the kind of thing you might want to keep in a bank safety deposit box anyway.

In addition, you should make copies of all your key software CDs (together with the serial numbers/ license numbers and similar information) and keep them off site. You will need a CD Writer, but these ship with many new PCs. You may want to get a scanner to image at least critical documents. Recovery of damaged paper can be impossible or extremely expensive (and is beyond the scope of this article).

Develop a Plan

You need to create a plan for what to do first if disaster strikes. What operations need to be restored first? For example, it is probably more important to continue to get documents out than focus on restoring your time and billing software. How do you deal with the loss of information concerning court/calendar dates? As a preliminary, you might establish relationships with various vendors, computer rental companies, disaster recovery specialists. Think of it as having an attorney on retainer in case of need.

Other Resources

You should set up a file containing printouts of some of the on-line help that is currently prominent in the wake of the WTC disaster. None of this information will fit your future situation exactly, but virtually all of it will have some points that are useful, and they were drawn up by people who have been through major disasters or who specialize in this field. Particularly good sites are run by the Tennessee Bar Association (www.tba.org/tnbarms/disaster.html) and the LawNet, an association of large law firms (www.peertopeer.org). Www.disasterrecoveryworld.com focuses on general business scenarios and examines many issues beyond the scope of this article.

Summary

Each firm needs to assess its comfort level in terms of disaster recovery planning and the budget required. However, for a small to mid-size firm, guaranteeing the ability to be back up and functioning within a matter of days of a major disaster is neither technologically overwhelming nor inordinately expensive. It is a matter of taking some basic precautions and keeping your recovery systems and documentation up to date as a basic element of doing business. ■

Worms and Viruses

The recent spate of viruses and worms (Code Red, Nimda) has again focused attention on virus protection. The Microsoft-sponsored view that users have only themselves to blame is at best irrelevant and at worst irresponsible. The issue is what can you do to prevent your users from being infected.

There is no substitute for user awareness and updating your anti-virus software regularly (once a week or more often if a new virus strikes). *Never ever* open an unknown file, even if it appears to be from someone you know. Many viruses propagate by sending themselves to the address list of the email client they have infected. What else can you do?

Apply security patches religiously. This sometimes seems like practically a full-time job, but it must be done. It is worth noting that the influential Gartner Group recently recommended dropping Microsoft's Internet Server (IIS) due to the difficulty of maintaining its security patches.

Turn *on* file extensions. Many viruses have hidden behind a double extension (e.g., *.jpg.vbs). Change your file associations so that anything with a *.vbs extension is opened by Notepad.

Disable (rename) wscript.exe and cscript.exe (in the Windows and windows/command directories respectively). This is the most drastic step, and may reduce functionality, so you have to watch for problems after doing this. But if you can get away with it, it will be effective. ■

Heckman Consulting llc
One Fencove Court
Old Saybrook, CT 06475

Stamp