TRIAL REPORTER

Spring 2009

Workers' Compensation

Improving the Workers' Compensation System

What to Expect At Your First Workers' Compensation Hearing

How to Avoid Malpractice in Workers' Compensation Cases

Workers' Compensation: A View from the Bench

Workers' Compensation: The Defense Perspective

Workers' Compensation Jury Instructions

www.marylandassociationforjustice.com

by John J. Cord

Protecting Your Data: Backup or Bow out

We see lessons every day that failure to implement a data protection plan can lead to the irretrievable loss of data. However, it frequently takes a personal disaster before we create a plan to protect ourselves and our clients from the perils of the information age. With a few precautionary measures, you can save your data, your clients' data, and your sanity.

Personal Backup

It happened to me one sunny afternoon. I was sitting in the partner's office, laptop on my lap, when out of nowhere it appeared: *The Blue Screen of Death*. I'd never seen one before, but I'd heard stories about it.[1] The first thing that happens is you freeze. Then you vainly search for help. But you know—deep down,

_____
[1] Interestingly enough, the Blue Screen of Death has its own page on Wikipedia. http://en.wikipedia.org/wiki/Blue_Screen_of_Death.

you know that there is nothing you can do. Because, you may lose some of your data. You may lose all of your data. My Dell computer, less than 6 months old, suffered a fatal hard drive error.

Fatal doesn't describe it well enough—catastrophic is really a better word. Unrecoverable. Everything on my hard drive—my wife's iTunes (which we didn't backup), any work I had done while at home or on travel which was saved to the hard drive and I never got around to transferring to our firm's network, and some personal files (okay,

a lot of personal files). All gone. That was the catalyst for me to change my ways. There are a number of ways to backup data from your personal computer or laptop. The key is do it regularly—use your case management program or firm's calendaring system to remind you every other week (or more frequently, depending on your needs) to create a backup. Here are a few methods:

External Hard Drives/Flash Drives: These are convenient storage devices for your data. *Flash drives* (also known as thumb drives) are typically about one to two inches in length, and plug into your computer's USB port. They can hold anywhere from about 64 megabytes (MB) to 128 gigabytes (GB).16 GB drives are available for about $50.00.[2] On the other hand, *external hard drives* are slightly larger (usually ranging from about the size of a large cell phone to small paperback novel), and can hold much more. I recently purchased a 500 GB external hard drive for $75.00.

About once every other week, I copy all documents on my laptop hard drive (everything is kept in one folder for convenience), and paste them onto the external hard drive into a new folder called with the description and date (for example, "Laptop Backup 04-15-09"). There's no reason to worry about deleting old backups if your data storage unit is large enough. This is a convenient method to backup data; however, if the hard drive or flash drive is kept at the same location as the computer, they are vulnerable to the same types of damage (theft, fire, water damage, etc…).

_____
[2] There are many different estimations of how many pages a gigabyte can hold. It depends on the size and type of the documents, but if we assume a single page .PDF document is 55 kilobytes, then a 1 gigabyte hard drive could hold 19,065 pages of .PDF.

Personal Servers: If you don't want to be bothered with remembering to backup your data on a regular basis, you can automate the process with a *personal server*. The personal server continuously backs up data as your work, and can even create a working copy of the data on your network. It is a piece of equipment stored with your computer, and as such is vulnerable to the same types of damage as external hard drives and flash drives.

On-line Backup: This has become popular in recent years. With o*n-line backup*, the user signs up with a data storage company, and the data on the computer will be saved on a regular schedule, often at night when it will cause the least disruption. The advantage of this method is that the data is stored off-site, which protects data in the event something happens to your office (i.e., fire or water damage).

Firm Network Backup

Backup of firm data is another important component to your data storage plan. Recent disasters, including Hurricane Katrina, emphasize the need for a solid backup plan. The frequency with which your firm backs up its data depends on a number of factors, including the firm size and the firm's reliance on computer data. A good policy for backing up firm data is to do it every day, so you do not lose more than a day of work in the worst case scenario. There are two components to a good firm data storage plan: on-site and off-site backup.

On-Site Backup: Like external hard drives, on-site backup is basically a process whereby changes to the firm network are copied every day at a certain time to backup "tapes." The tapes should be manually rotated every day, and stored in a secure location (possibly a fire-safe). Typically, daily backup tapes are saved for a week to ten days, and you should have monthly backup tapes for about the past year.

Off-Site Backup: Like on-line backup, this is a process whereby the information on your network is saved daily to a remote server, allowing access to data if disaster strikes your network or if you need to access a prior version of documents you've updated. Your vendor will make an exact copy of your total data, called a "seed," and will store it on their data center. Then, once a day (typically at night), the changes made to your firm's data are uploaded over the internet, modifying the vendors data. Your vendor will keep a regular rotation of information, so they can recreate the data as it existed in your network at specific points in the past. If you need to pull individual files, or backup the entire system, they can facilitate the process.

MAJ Sponsors who perform network backup services include **Choice Technologies, Inc.** (MAJ Gold Sponsor), **Byte Right Support, LLC** (MAJ Silver Sponsor), and **Cobalt IT Consulting** (MAJ Bronze Sponsor). Regardless of your choice of vendor, it is imperative that you and your firm implement a data storage plan to protect your work product. ∎

Biography

John J. Cord (Miller & Zois, LLC) graduated from the University of Colorado School of Law in May 2003. Mr. Cord concentrates his practice on assisting victims of birth trauma and other serious injuries of medical negligence. He is licensed to practice in Maryland, the District of Columbia, Pennsylvania, Georgia and Minnesota. He is a member of the American Association for Justice and is the past chair of the Maryland Association for Justice Technology Committee.