

From the July 2009 issue of
The Lawyer's Competitive Edge: The Journal of Law Office
Economics and Management

Published by West, a Thomson/Reuters Company

Indecent Exposure - Most law firms are unprepared for computer calamities.

Kim J. Brand

www.FileEngine.com

Computers are cheaper, more powerful and ubiquitous in law firms. But ignorance about their operation continues to be excused up and down the management line. The risk of significant data loss from a variety of threats is similar to the morbidity of a major heart attack. The firm may survive, but the prognosis isn't pretty. As with your health, an ounce of prevention is worth a pound of cure.

The number of hardware and software products available to defend against these threats is an indication of how common data loss is. According to one vendor(1) 140,000 hard drives crash *every week* in the U.S. A Google study(2) estimates that over 2% of all hard drives (one in fifty) fail in their first year of operation; a rate that grows to over 6% (one in sixteen) per year. The issue was summed up nicely by Inspector Harry Callahan (Dirty Harry) when he suggested that a bank robber ask himself, before reaching for a gun as he was staring down the barrel of Harry's [possibly empty] .44 Magnum: "Do I feel lucky?"

Hard drive failure is only one of a myriad calamities that can terminate access to your firm's data in a heart beat. Your hard disk is part of a complicated system comprised of many components. Reliable as they are, they tend to fail at the wrong time. (Is there a good time?) The same Google study estimates that 90% of all new information is stored on hard drives – attorneys are probably responsible for a good part of it.

To understand how to defend yourself from the threats that affect reliable access to your data it is appropriate to understand what they are. As you will see, the steps to be taken are different depending on what sort of 'bad thing' can happen. You need a 'blended defense' to dodge this bullet.

Acts of God
Acts of Violence
Acts of Stupidity

These threats are probably obvious if you think about it. Bad storms roll through and lightning strikes. It is not uncommon for electrical problems to destroy computer equipment. Your first defense should be a quality surge suppressor; don't scrimp - spend \$40 or more. An uninterruptible power supply (UPS) is even better. They start at \$75. But a storm can literally blow the windows out of your office or pull the roof off. Water is just as dangerous. Other Acts of God include accidents and hardware failures.

When an Act of God occurs we just want 'yesterday' back. Here, a full system image of the affected computer stored offsite is the best defense – assuming we can get replacement hardware. Redundancy is also useful. Hard drives can be deployed in 'fault tolerant' arrays that can withstand the failure of a single drive without data loss. The problem is that most firms don't monitor these RAID (Redundant

Array of Independent Disks) arrays so the failure goes unnoticed until a second hard drive fails and the data disappears. (Note that redundancy is no defense against an Act of Stupidity: if you delete a file it's gone everywhere at once.)

Acts of Violence come in many flavors. Servers get stolen or vandalized by strangers or employees all the time. A recent case(4) involved a Florida woman, convinced she was being fired on Monday, went into her office on the weekend and erased all the files on her company's server causing an estimated \$2.5 million in damages.

One out of ten laptops are stolen.

Your backup tapes or disks are valuable too – or a thief might think they are – so store them away from your server and lock them up. Backup media should be password protected. Absconding with a backup tape or disks may be the easiest way to thwart an effective system of passwords and firewalls.

Virus attacks or hacker intrusions may be classified as Acts of Violence too. Either can cause trouble that might not be noticed for some time. The same is true with hardware or software failures that slowly 'eat' data or corrupt files. You might not become aware of a problem until significant damage has been done. Backup programs that fail and report 'corrupted data' might give an important warning – if only the backup logs were monitored.

These circumstances call for multiple generations of backups (the so-called Grandfather – Father – Son system) so recovery can be effected from a time period before the damage or infection occurred. But tapes, external hard drives and on-line storage space can be expensive so there is always some reluctance to keep too many. Also, with more backup generations, backup media management becomes a problem: rotating them offsite, identification, retirement and, as mentioned above, security.

Many firms use a one or two week cycle of daily backups. The disks or tapes are recycled so that the oldest backup media is reused after five or ten backup cycles. This results in a 'use it or lose it' race: If you don't notice something is wrong before your oldest backup is re-used you lose the chance to recover it. The development of a backup policy that respects business cycles, data retention requirements, data safety concerns and economic considerations can be complicated but is essential.

[Tip: If you only make a weekly backup do it on Thursday night. If Acts of God or Violence have an equal chance of happening on any day of the week, taking a Thursday night backup home on Friday makes more sense than leaving a Friday night backup tape at the office over the weekend where it can get stolen or destroyed for two days when nobody will be at the office.](#)

Over a quarter of data loss is caused by Acts of Stupidity(8). The classic case is when someone attempts to 'clean up' unused directories or files. Forgetting to use the 'Save-As' command when adapting an existing file to a new use is a popular mistake. More creative is the recovery of too much data from a backup which mistakenly overwrites newer versions of files with older ones.

Add to these acts of commission acts of omission. Failing to monitor the reports created by your backup program is almost as bad as not backing up at all. If you don't know what files and directories are included in the backup, *or that it worked at all*, you might as well not bother to backup your system. We have been handed many blank, unreadable and 'antique' backups after a server melt-down. The operator was horrified that despite diligently following the IT guy's instructions everything was gone. (A simple backup survey and audit procedure is included at the end of this article.)

Programs can be stupid too. Outlook 2002 has a known issue with PST files that grow beyond 2GB. If you exceed that limit, the program will prompt you to restore your PST file from a backup. No backup? Start over. The loss of critical e-mail has recently become another risk to which unprepared law firms are exposed.

Files stored on portable media like thumb drives and external USB connected hard drives can simply get lost. Over 10,000 laptops are lost(5) in U.S. airports *every week*. One source(6) estimates that the value of a lost laptop is nearly \$50,000 when liability for breach of data confidentiality is considered. New laws require owners of lost laptops to notify parties that may have had their personal information compromised. How do you know what data was lost unless you have a backup? Needless to say, making backups of mobile devices is more challenging than making backups of PCs and servers that never leave the office.

For Acts of Stupidity the best solution is a readily accessible copy. Here a simple archive folder works just fine and a nightly copy 'script' is a good alternative to a complex backup program. (Any IT consultant familiar with command line operations can create such a script in just a few minutes.)

Recovery Point Objective Recovery Time Objective

Firms concerned about recovering from a computer calamity should decide from what point in time they would be satisfied to start over and how long it is acceptable to be 'down.' The former ambition is known as Recovery Point Objective (RPO) and the latter is known as Recovery Time Objective (RTO.)

If you make backups once a week you are implicitly accepting a RPO of up to one week – a system failure on Thursday afternoon requiring restoration of data from the prior Thursday night represents the worst case scenario. Considering the lost productivity of even a solo practitioner, it is hard to justify not making a backup every night.

Many firms confuse backups with Disaster Recovery. If your server has been totally disabled or stolen you are faced with recovery of not just the data but also the hardware, operating system (OS), configuration details, application software, settings, licenses, etc. We call this the 'Value Stack' and each layer imposes a different recovery requirement. Having replacements at hand – and few firms do – is important but not enough. You'll also need the skill, (or the prompt attention of a qualified consultant,) to rebuild the system and recover the data.

Typically, firms begin to experience the pain of total system failure within just a day after the loss. Substantial costs (which can include direct costs and penalties, lost income, as well as loss of a firm's reputation and threat of malpractice claims,) can mount after just a few days. One source(7) indicated that 60% of businesses that suffer a major data loss go out of business within six months.

To achieve a RTO of one day or less after a significant system failure is expensive. Few small firms can afford 'Full Server Failover' technologies which generally start at \$15,000 and go up; and that doesn't include the cost of continual maintenance, monitoring and testing. More reasonable is a RTO of the next business day. Many hardware vendors offer that; but recovering the rest of the value stack can take additional time. We recommend imaging software that stores a complete image of a PC or Server for rapid recovery. The cost of software and hardware would be less than \$1000 for a server – under \$200 for a PC.

Summary

Dependence on computers has exposed many firms to threats – old and new – that few are prepared to defend. The best solution is to implement a blend of data safety strategies that include the following elements:

1. Engage competent help to identify data safety risks and appropriate recovery strategies
2. Operate PCs and Servers that are under warranty and that can be repaired quickly.
3. Establish a backup policy, train staff to implement the policy, and monitor compliance.
4. Take periodic images of important systems to multiple external hard drives. Take these hard drives offsite.
5. Create multiple backup generations of 'dynamic' data - that which changes frequently. Rotate backup media offsite and protect it locally. Assign responsibility for monitoring backup program results and monitor compliance.
6. Subscribe to an 'on-line' backup service for dynamic data.
7. Survey your network for data that should be backed up and backups periodically.

Backup Survey

Ask: What programs do you use?

Have your users point to the icons they click on or the programs they select. This should include word processing programs, e-mail programs, databases, accounting and other custom applications. If you notice icons or programs that weren't on the list, ask "What are these?" Sometimes people simply forget which programs they use.

Ask: Where does that program store its data?

Ask the user to demonstrate using the programs, opening or closing a file, database, etc. Most programs store and retrieve files. The trick is to make sure the user knows where that is, or to confirm that systems are in place to locate the data in a place where it can get backed up.

Ask: When/Where does that data get backed up?

Every user should be aware of how their "stuff" is backed up. They should know if it was last night or last week.

A Simple Backup Audit

STEP ❶ Create a "test" file and store it along with your other documents. That may be in "My Documents" or in some other folder on your PC or server. This file might only have one line in it; a quote like: "here today, gone tomorrow" is appropriate. You can also try adding a contact to your address book, login and password to a website, or sending yourself an e-mail message.

STEP ❷ Tomorrow, delete the file, contact or e-mail message. (This step adds drama.)

STEP ❸ Attempt to recover the file from your backup. PLEASE make sure you know what you are doing—you don't want to conduct this test if you are not familiar with your backup software. Recovering too much can be a disaster! If you need to ask someone else for help, let him or her know it is a test. Be patient, but be persistent.

References

- (1) <http://www.Mozy.com>
- (2) http://labs.google.com/papers/disk_failures.pdf
- (3) http://en.wikipedia.org/wiki/Dirty_Harry
- (4) <http://www.switched.com/2008/01/24/afraid-of-losing-job-florida-woman-deletes-office-files-worth/>
- (5) <http://www.itworld.com/security/53383/laptops-lost-hot-cakes-us-airports>
- (6) <http://www.physorg.com/news159730126.html>
- (7) <http://www.bostoncomputing.net/consultation/databackup/statistics/>
- (8) <http://www.ontrackdatarecovery.com/understanding-data-loss/>