



From the **Ross Ipsa Loquitur** blawg
November 28, 2007

By

Ross L. Kodner, Esq.
MicroLaw, Inc.
rkodner@microlaw.com

©2007 Ross L. Kodner, Esq. All Rights Reserved

On the Subject of Backup

On the subject of backup, which has reared its head for perhaps the 8000th time on various listserves I've been involved with over the years... it appears the subject once again should be addressed. So buckle your belts and hold on - it may be a bumpy ride. Note that this article is specifically directed at solo & small firms but the concepts are applicable to practices of all sizes.

As a veteran of many a late night restoring data from the failed systems of my clients over the years, and as a many-times author and speaker on PRECISELY this topic, I will make the following statements. It's important to understand my credentials on this subject. Since 1985 when I started consulting with law practices full time, I've made backup system/process recommendations to literally thousands of law practices of ALL sizes. I've had to sit and restore systems from backup media - more often than I'd like to think pulling all-nighters at client offices to nurse their systems back from the brink. I've seen it all.



On the Subject of Backup

Ross L. Kodner, Esq.

November 28, 2007

Page 2

From cassette tapes in the wild, wooly frontier days of the early 80's to floppies to the earliest backup tapes, through the Pre-Dark Ages (called the Colorado Memory Systems era) to the true Dark Ages (also called the "Travan Nightmare"), through Bernoulli disks, to Zip drives, through the weird writable CD period which morphed into the less weird but still somewhat delusional writable DVD period, to



Magneto-Optical drives, to DAT tape, into DLT tape, to LTO and VXA tape, to tape libraries and tape autochangers, to external hard drives, to modern D2D eSata systems, through the complete evolution of online options. I've really seen and experienced it all. Through failed systems that could only be restored through the miracle work of services like Ontrack and Drivesavers, eating thousands of dollars and slicing years off the lives of the partners of the firms involved. Through article after article on every aspect of the subject, including an epic 12,000 word two part tome in 2004 in "Law Office Computing" (RIP). Through dozens of live CLE programs on the subject coast to coast and even on other continents. Through literally hundreds of posts on various legal listserves.

But the subject still comes up. And dangerous ignorance, rampant tempting of the fates and taunting "nah, nah, nah, nah, nahs" to Mr. Murphy and his famous law still seem to be the order of the day. Until someone experiences total data loss because of their failure to accept data backup realities. So it needs repeating. And probably will need it again. And again. And again. Because ultimately, while nothing is as tedious and boring to talk about as backup, it's the one technology that will one day save your law practice and your entire ability to make a living from utter apocalyptic destruction.

Like it or not, agree or not, it's really besides the point - these are my:

Ross' Great Truths of Data Backup:

- 1) ***Why we do it.*** It's not about backing up, it's about restoring.
- 2) ***Tape is so 1990's*** - No one should be backing up to tape media anymore - doing "disk to disk" or "D2D" backup is the only sensible approach for your primary daily backups
- 3) ***Don't Tempt the Fates - Spread Out Your Protection:*** Your backup approach should have four layers of protection ideally - never put all your backup "eggs" in one basket
- 4) ***Bad things happen to good lawyers*** - expect and prepare for the the worst and be pleasantly surprised if it never happens
- 5) ***Primary Backup*** - full nightly automated backup of your primary server/system - that means EVERYTHING, not just your view of "data" and NEVER, EVER an incremental backup under any circumstances. Several of you have asked why - so here's my answer on avoiding incremental backups:

On the Subject of Backup

Ross L. Kodner, Esq.

November 28, 2007

Page 3

Because trying to stitch someone's system back together from a patchwork of miscellaneous incremental backups spread across multiple media is a nightmare that I would never want to live through ever again. I've never actually seen a system that was ever successfully restored from an incremental backup set.

And since full system backups should be done automatically in the middle of the night anyway, overwriting the previous backup set on the media, who cares whether it takes 20 minutes or 3 hours in a small firm where there isn't a graveyard shift? The only "advantage" of an incremental approach is "less time required." But it's completely non-sensical for the reason indicated.

For the best written explanation of full (or sometimes called "normal") backups v. incremental v. differential backups, read this article at TechRepublic: <http://articles.techrepublic.com.com/5100-1035-1048814.html>. It's very understandable and ultimately makes the key point. Full backups take the longest and require the most storage space to be sure . . . but they're also the fastest to restore and THAT'S consistent with rule no. 1 on my list.

6) **Primary Backup Part Two** - use actual data backup software suitable for either an individual PC or a network server and BE SURE if it is on a network, you include needed backup "agents" to properly backup open files, Exchange Server, and to provide you with a disaster recovery function to rapidly restore to a rebuilt system. Never use any backup software that comes built into any version of Windows. For networks using Windows 2003 Small Business Server my favorite is Symantec's Backup Exec for SBS, currently v. 11d (a great deal at \$289 when bundled with a new Dell server BTW). Be sure to add any needed backup "agents" to make sure open files are protected, as are Exchange databases and SQL databases. For individual PCs, I like NTI's Backup Now, Roxio's Backup My PC, and some versions of EMC Retrospect Pro. The product I am personally using to backup my laptops is Acronis TrueImage 11. Originally designed to be a "ghosting" product, it has morphed into an impressive complete backup/restore system.

7) **Alternate media each day** - a five (or more - more is better) disk rotation is what I would consider minimally adequate - with eSATA-connected internal or external removeable drive systems as inexpensive as they are and capacities as high per "cartridge" as they are, you can have a M through F set of five disks and keep cycling through them. More is better - two weeks worth plus a rotating "monthly" cartridge are better. An annual cartridge that never gets reused after being backed up to on 12/31 each year is best.

8) **Store the media out of the office** - in a different building. As far from the office as is practical each day. Another city at least 500 miles away is best. It does you no good if the backup media melts in the fire.

On the Subject of Backup

Ross L. Kodner, Esq.

November 28, 2007

Page 4

9) **Secondary Backup** - Offsite if ethically permissible in your jurisdiction. Data only backups, automated in real-time or after-hours to either Mozy.com (I like the interface for restoring and pricing) or Connected.com (because Iron Mountain isn't likely to go away any time soon)

10) **Tertiary Backup** - actually this level is all about downtime reduction while a failed or downed system is being restored to regular operation (which can take some time). Ignore this one and you could easily be down for a couple of days while your IT person waits for a replacement hard drive to be shipped. This involves a combination of simple approaches to make sure you can run on another PC if you're a standalone or peer to peer situation, or on another server or workstations if you're networked. The best approach for server-based systems is setting up a simple mirroring situation so everything happening on the primary server is mirrored in real-time to a secondary server - if main dies, secondary kicks in = zero downtime. OR... mirror data folders in real-time with a shadowing utility like NTI Drive Shadow or Second Copy to a NAS or another networked PC - then use that data in the event the server connection is lost = much less downtime. AND take advantage of the mirroring abilities of some software - for example, Worldox and other DMSes which can mirror documents in real-time to a designated local drive to use if the server connection is lost. Or TimeMatters with its local "clone and sync" process to keep a working copy available on a local hard drive . . . or PracticeMaster's Briefcase function with similar capability. All focused on cutting downtime when a server or primary machine is disabled or inaccessible.

11) **Image Backup - Protect Against OS Blowups on Workstations.** Use Acronis TrueImage or Symantec Ghost to keep an "image" backup of each class of PC setup so you can quickly restore a blown Windows system (or setup a nearly-identical new PC).

12) **TEST! TEST! TEST!** The most important point - exercise your backup systems. Do a "mini test restore" from your primary backup media at least weekly (randomly pick a couple of documents, restore them (move the originals to a safe place first), see if you can access them - it's a valid test of being able to restore everything if the chips were down). At LEAST weekly. Then at least monthly (more often is good, less often is not) test your secondary and tertiary systems, especially online systems. It's amazing how many people I know who backup online but have absolutely no idea whatsoever how to restore files (see item no. 1 on this point!)

13) **Protect against Liveware failure.** If you have enough people, make two responsible for backing up - one to do it, the other to confirm that and to ensure the steps are followed religiously.

14) **Dispose of old backup media intelligently** - when you dump your antiquated and unreliable tape-based system, either keep the media and the tape drive forever (in case you need to access something on the tapes) or physically destroy the media to prevent unintended/unauthorized recovery of your confidential info.

On the Subject of Backup

Ross L. Kodner, Esq.

November 28, 2007

Page 5

15) **Be Redundant!** Look for other, sometimes more subtle ways to protect your data or reduce the chances of expensive downtime. In servers, use RAID Arrays of hard drives. RAID 1 at least for mirroring or drives, or better, duplexing of entire drive systems. RAID 5 or 10 for adding smart error correction and online rebuild capabilities into the process. Use heavy-duty SAS (f/k/a SCSI) server-intended hard drives in your servers, not workstation-intended cheaper, lighter duty SATA drives. If there's a redundant power supply option available when you order a server, go for it. You can even use RAID Arrays in Windows workstations that you might be using as a quasi-server in a little P2P network.

16) **Think about Spot Backup** - what about critical stuff you can't afford to lose in between your four primary backup layers of protection. The Great American Trial Brief. A chapter of your long-awaited book. The greatest trust agreement in the history of the universe. Absolutely use your word processor's emergency backup function - I set mine to auto-backup every 7 minutes in both Word and WordPerfect versions. Know how to recover those BK files when you need to (before the disaster happens, eating your document in a puff of digital smoke). Consider emailing in process docs to yourself at your Gmail account for "spot offsite backup" purposes. Think about keeping a hefty 4 Gb flash drive plugged in and get used to double-saving key docs and emails to the flash drive as well as their regular folders. So think "spot."

I'm sure I can come up with more if I really thought about it but this should keep most out of trouble. Failure to follow these field proven, hard-fought, University of Hard Knocks learned lessons puts your entire practice in abject peril. No exaggeration or hyperbole intended.

Other helpful stuff - here's a link to a great online article that explains the differences between full backups, differential backups and incremental backups – a superb read on this not-so-obvious subject and somewhat fuzzy set of distinctions (<http://articles.techrepublic.com.com/5100-1035-1048814.html>).

Let me conclude by saying . . . no . . . BEGGING you to follow the advice in this post. Your practice depends on it.

Ross L. Kodner is the most-awarded legal technologist in history with an unprecedented five Technolawyer awards to his credit including a lifetime achievement award. He also is an active GP|Solo Division volunteer, founding and Co-Chairing the National Solo and Small Firm Conference. A "recovering lawyer," Ross is the founder of Milwaukee's MicroLaw, Inc., a 23+ year old international legal technology

On the Subject of Backup

Ross L. Kodner, Esq.

November 28, 2007

Page 6

and law practice management consultancy. He has delivered over 1400 CLE programs on practice management topics over the years and has held numerous leadership positions in local, state and national bar associations. He is also the developer of the widely-known Paper LESS Office(tm) process, which has been successfully deployed at law practices worldwide.