

Up Close and Personal: Leo's Office Disaster



By [Leo Wrobel](#)

Date: Apr 20, 2010

[Return to the article](#)

Following a record snowfall, Leo Wrobel discovered what it's like to learn that you're not quite as prepared for disaster as you thought you were. Learn from his experience, or you may be bound to repeat.

February 12, 2010: On that memorable Friday, the Dallas/Ft. Worth area of Texas received a whopping *14 inches* of snow, doubling the previous record of 7 inches, which had stood for over 30 years. North Texans are comical when anything other than rain falls from the sky, especially when it lands on the highways. In this part of the country, if snow or ice falls, you *stay at home*. School is canceled here when someone even *predicts* snow or icefall.

When Preparations Pay Off

Speaking of 30 years, that's about how long I've been writing articles on preventing and recovering from catastrophic events, so you'd think that mine would be the best-prepared small office in the face of such a disaster. Indeed, we thought that was the case. While over a foot of the white stuff was falling right at the end of the work week, we were here in the office, marveling at Mother Nature. Then, just at close of business, the power went off. No problem: The office had a backup generator. We also had taken logical precautions in the form of an uninterruptible power system (UPS) for each individual workstation, as well as for key components in the telephone closet. We finished up the week's tasks and never missed a beat. So far, so good, right?

The power stayed off until late Saturday night, but all the while we maintained electricity and heat in the office by virtue of the generator. Even after leaving the office, we enjoyed the weekend, because our home also has a generator (Snowstorms are rare in this part of the country, but thunderstorms are common. Since we often work from home, investing in a generator made sense.) We had recently shopped for groceries, so we had plenty of food and beer in the house. Life was good. How wonderful that we had outfoxed Mother Nature.

Or so we thought.

Not Quite Prepared Enough?

You've probably heard that old expression about what happens when you *assume* it makes an ass out of *u* and *me*. We had made some basic assumptions that didn't pan out well for us.

- Since all of our data was backed up on a RAID server, we assumed that it was safe and inviolable. [1] If something happened to a disk drive, the other redundant drive should take over.

NOTE

First defined by David A. Patterson, Garth A. Gibson, and Randy Katz at the University of California, Berkeley in 1987, RAID is an acronym for *redundant array of inexpensive disks*. Generally speaking, RAID refers to any technology that allows computer users to achieve high levels of storage reliability by arranging hard drives into arrays for redundancy. Using special hardware or software, RAID combines two or more physical hard disks into a single logical unit. In case one drive fails in a two-drive RAID system, the data is designed to remain safely on the second drive, in an accessible, redundant copy.

- We assumed that if something happened to a power supply or logic board, we could simply pop out the redundant disk and drop it into a spare computer to resurrect the data.
- We assumed that *surge protectors* do exactly what their name implies.

- We underestimated the cost of resurrecting even relatively small quantities of data in a worst-case scenario
- We underestimated how long data-resurrection takes, and the impact it has on even relatively small office.

For us, the disaster began unfolding at about 8 p.m. on Saturday when the power came back on. Until that time, we were warm and happy on backup power. When we went back to commercial power after about 28 hours on the generator, the power company (as is often the case) was still attempting to restore steady power. The power flicked on and off two or three more times on Saturday night.

During one of those times, there was a surge or spike in the commercial power.

Here's what happened in each vital service area of the company:

- Our phones stayed up. In the event that phone service would fail, we had subscribed to the [Telecom Recovery](#) voice-recovery system, a versatile and affordable service. If the phone company or our telephone system had failed, our calls would have been redirected instantly to our cell phones. So we were well prepared for voice communications.
- Our Internet access stayed up. We use two separate wireless Internet service providers (WISPs) and a dual wide-area network (WAN) router. In fact, one of the two Internet feeds actually *did* fail, since the tower that provided it was affected by the same power outage. However, the other diverse link ummed right along without our even noticing.
- Most of the workstations in the office did fine, since they were on UPS for the brief period of time after the power failed and before we started the generator. (This is a manual process, but you can't have everything in a small office!)

So what's the problem? We didn't realize that, when the power came back on, the spike killed the RAID server, erasing *four years* of our data!

Go ahead and lecture us now on the importance of backup copies. But golly, isn't that why you buy a RAID server in the first place? The RAID server by its nature *is* a backup copy. Or so we assumed. (Remember what I said about what happens when you *assume*?)

Errors and Costs

In hindsight, we can see that we made some subtle errors in judgment. Perhaps we had unrealistic expectations for what we referred to as a RAID "server." It was actually a Fry's Electronics retail store special. (In this case, perhaps *fried electronics* is a better name. Sorry, I couldn't help myself!) The actual nomenclature for the thing is an Iomega StorCenter ix2 network-attached file storage unit. A terabyte of storage and a gigabit Ethernet connection, all in a cool and compact little package. It worked well for us until that fateful weekend, may rest in peace.

Now let's talk about what it cost us in terms of lost productivity (albeit courtesy of the power company), what it really costs to fix a problem like this, and how it could happen to you. Solving the problem wasn't as simple as just buying another \$400 RAID server. After we determined that the spike was fatal (the server wouldn't boot), we began stepping through the process for dealing with the aftermath:

- **Plan A.** Remove one of the two redundant SATA drives and slap it into one of the office computers. This action quickly exposed the first flaw in our carefully conceived backup plan. Iomega uses a proprietary file system, and none of the office PCs could read it. On to plan B.

NOTE

Please, no nasty email or letters. This isn't a shot at Iomega or any other vendor. It's just a few tips for you, in case you ever have to recover from a similar event.

- **Plan B.** Tough it out and call Iomega's data-recovery people. We had six months' worth of data backed up on other servers, so kind of a belt-and-suspenders approach, given the fact that the RAID server had two redundant drives. The data was also stored offsite periodically, on an online basis. At Iomega, the help line was answered on the third ring by someone with a good command of English and a pretty good idea of the situation. When asked about the procedure, he explained that we simply had to ship the unit to Iomega, which would perform a free assessment of the problem and call back with a quote to fix the unit and/or resurrect the data. If we didn't want to take any further action, we could simply ask for the unit to be returned to us. Then

asked for a range of costs associated with such a task. The quote? From \$700 for a minor issue, up to \$3,000 or more for something more complicated.

The original Fry's Electronics price tag on the box showed \$249.99. Spending \$3,000 was obviously a different kind of proposition. Lesson learned: The price to fix something isn't based on the dollar value of the unit itself; it's based on the value *you* place on the data it contains. I've written about this topic for 30 years, but it's another thing altogether to live it firsthand.

In a small office, a \$3,000 hit is a big deal. Losing four years of archived data that we thought was safe was even worse to contemplate. Think about a law firm or CPA in a similar predicament. *Idle:* Why did the CPA cross the road? Answer: Because he looked in the file and that's what he did last year. Many professions use the same data again and again. My company is one of them.

- **Plan C.** Being somewhat of a cheapskate, I searched eBay and the factory outlets for the same unit. I reasoned that I could find a good used unit, swap the drives, restore the data, and then drop-kick both units out the back door. I even found one on Iomega's website for \$137, but was still unsure whether it would be compatible with the proprietary file structure.
- **Plan D.** The final answer was "None of the above." I solved the problem myself. Here's how: When we first installed one of the drives in a Windows XP machine (plan A), it didn't show up as a drive letter. It did show up as an unknown drive, however, when we brought up the Administrative Tools > Disk Management function under Windows and looked at the drive layout. Having heard that many manufacturers of these units use the Linux file management system, I pulled out a CD of Slax Linux purchased from an electronics flea market three years ago. Bingo! Not only did it find the Iomega drive, but it read the file. However, it wouldn't create a directory or write to a Microsoft Windows hard drive, perhaps since it was an evaluation copy. Not to be deterred, I pulled out a copy of Xandros Linux. Xandros' claim to fame is as a bridge between Linux and Microsoft environments. That did the trick. Once Xandros was installed, it was a simple matter to copy all of the files from the Linux partition to a Microsoft partition that could be read by the other computers in the office!

Bullet dodged, office saved, Leo was the hero. Or was he?

What did this "minor" disaster really cost? First, I had to do the work myself. That meant pulling me off of \$250+ per hour assignments for clients for two full days. Total cost: \$4,000 (sort of! I caught up on some of my work by putting in overtime for the rest of the week). My best guess is that we broke even on what Iomega would have charged to do the job. But I now have a new appreciation for the costs. When executives in small and medium-sized offices are working on IT problems instead of their jobs, that fully internalizes the scope of the problem. It happens much more often than people imagine. So I learned a valuable lesson, but I also got some great material for this article.

Moral of the Story

It boils down to what we've said for 30 years:

- Expect the unexpected.
- The value of disaster recovery has little to do with the price of the equipment, and everything to do with the value of the data it contains.
- The value of the restoration process corresponds linearly with the hourly rate of the people called to restore it. It was more expensive for me to do the work than to hire a technician. That might be the case with every profession, but if you're a lawyer, CPA, or other high-dollar, data-dependent knowledge worker, take heed.

We survived, but only after two days of the proverbial wailing and gnashing of teeth.

We hope that this situation strikes a resonant chord with you, and that you take a second look at even the small systems that support you and your organization. Happy planning!
