

LAW.COM

LEGALTECHNOLOGY

February 21, 2008

Protect Yourself From Data Armageddon

Ari Kaplan
Special to Law.com

As I walked through the halls of LegalTech New York recently, I was struck by the fact that with so much focus on data discovery, management and review, there was little discussion of disaster recovery. In fact, there was only one program at the conference directly on the topic, "The Role of Mobile Remote and Wireless Technologies In Disaster Recovery." There is so much confidence in the power of forensic technology and the CSI-like retrieval of every byte of information that there is a risk that data protection is being overlooked.

Jeffrey Brandt, chief information officer at Cozen O'Connor in Philadelphia, was a panelist at the LegalTech program addressing this issue and comments that, to some, disaster recovery is old news. It was a hot topic following the tragic events of September 11, 2001, and then again post-Hurricane Katrina in 2005. Now, e-discovery is the topic du jour. Brandt cautions, however, that "disaster recovery is one of those items that people understand very well after they go through it once."

In fact, Waterloo, Ontario-based Research in Motion Ltd. recently reported a three-hour BlackBerry outage that crippled communication throughout the U.S. and Canada. Brandt, who is also the former vice president for the Mobile Remote & Wireless Peer Group and a member of the board of directors for the International Legal Technology Association, reports that the frenzy over the loss of service resulted in hundreds of messages on the ILTA listserv.

I hadn't really thought about data so personally until catastrophe struck in early November. I was in the midst of completing my first book, which had consumed me for months and was due to my publisher within days. My two year-old daughter was particularly excited to see me after a nap on a Friday afternoon. Running around my office, the cord to my laptop was obstructing her path. She tugged at it more than once, but for some reason I still set the computer down on the far corner of the table.

In a flash at around 4:30 p.m., my daughter won the tug of war and my notebook had literally crashed onto the painfully hard tile floor. I watched it fall in the surreal slow motion haze that accompanies any eyewitness experience, but could not imagine the potential damage. To my surprise, it worked for a minute and I thought nothing of the accident. I picked it up and breathed a sigh of relief.

When the colored pinwheel (rotating hourglass for PC users) locked up my computer, I tried to reboot. Alas, there was nothing. A gray screen. Game over. The support technician I called warned me that the drive was probably cracked and that I could have lost absolutely all of my data. Since I hadn't backed up in 4 months, I was noticeably bothered, but thought he had to be wrong. After all, it was 2007.

Two weeks and a refundable \$700 fee later, it was still all gone. Not a single item was recovered. Much of my work was backed up in some decentralized fashion through various e-mail accounts, but I was sad to have lost those items, like my family photos (many of Little Miss Sunshine herself), that had no quantifiable value.

With no luck at Tekserve in New York City, Greg Buckles, a corporate e-discovery consultant and analyst with Houston, Texas-based Reason-eD, suggested that I contact Rob Fitzgerald and Jason Dana of The Lorenzi Group in Manchester, N.H. I sent them the drive and they immediately attempted to make an image utilizing Hardcopy II from Lakeland, Minn.-based Voom Technologies. Without success, they tried SMART from Cedar Park, Texas-based ASR Data Acquisitions and Analysis, Helix from e-Fense and FTK Imager from Lindon, Utah's Access Data. No luck.

Since the hard drive did not even spin, Fitzgerald and Dana tried to create a mock-up by transferring the platters to an identical functioning drive. That actually made the disks spin, but they remained unreadable.

Brandt highlights that those making disaster recovery deliberations need to consider recovery point objectives, i.e., how old the data will be at the time of destruction and the recovery time objective, i.e., how soon one would need the data back. The recovery time objective is based on the tolerance of the organization. For critical segments, Cozen O'Connor's tolerance is under five minutes. The lower your tolerance for risk, the more expensive it becomes. I am told that Novato, Calif.-based DriveSavers Data Recovery, Inc. may be able to recover the data on my drive for anywhere between \$900-\$3,900, depending on what its technicians retrieve.

Brandt offers some simple steps to help your organization prepare for data Armageddon that include:

Centralize Contacts

At a minimum, one should have crisis contact information readily accessible. He carries 23 electronic staff directories, one for each office and the senior management group, in a Palm Treo. His list includes pictures of almost everyone alongside their home addresses, mobile phone numbers and emergency contacts.

Remote Data Hosting

Host your data center remotely, especially since external vendors usually have infrastructure facilities well beyond your financial means, such as feeds from three different power grids.

Duplicate Or Near-Duplicate Systems

Create a duplicate or near duplicate system at a remote location. Cozen replicates its data in Philadelphia and Chicago. The firm has five tiers of downtime. Tier zero never goes down and Tier 4 mandates recovery in less than a week. "You are making a business valuation because the further up you move out the tiers, the more expensive it becomes," says Brandt.

Secure Your Backups

At a minimum, keep backups off site at high-end records vaults. Even the managing partner of a smaller firm taking the tape home is better than doing nothing. Avoid placing them in a bank safety deposit box because you may need them at an odd hour when the bank is not open.

Test Regularly

Testing your backups and plans is essential. "After a disaster is a bad time to learn that nothing is retrievable," says Brandt. "Until you execute them, your plans are all theory," he adds.

There is a tendency to associate disasters with calamitous events so great that courts extend deadlines and suspend statutes of limitations. If, however, your office building floods and access is denied, or it is part of a suspected terrorist scare and the authorities prohibit entry (or if a two-year old destroys your hard drive), there will be little sympathy for your loss of data and continuity.

Buckles also recommends mapping and identifying information. A corporation that experiences a major

system crash with no recovery at all will need to explain in every subsequent litigation what happened and why it could not produce data for that specific date range, he says. More important than simply backing up is analyzing where critical data is created and maintained. "Whatever you do, there are certain things you have that will kill you if they disappear; those are things you want to map and identify," he adds.

Although planning and preparing is not cheap, contact someone who has lived through disaster recovery and he or she will convince you that it is priceless. If you need to scare yourself, just invite that person's kids into your office.

Ari Kaplan, the principal of Ari Kaplan Advisors, is a lawyer and a writer based in the New York area.

Copyright 2008 ALM Properties, Inc. All Rights Reserved.