

# Physical Data Security, Management and Destruction for Legal IT Professionals

By Michael Chung

Lester Schwab Katz & Dwyer, LLP (“LSK&D”) is a 65-attorney insurance defense firm based in New York City. As IT director, I oversee all information systems for the firm, managing a relatively lean staff to cover our employees’ needs. Our firm’s management expects my team to properly manage, backup and destroy information at the appropriate times with effective methods. They are kept informed periodically, but the bulk of the responsibility falls to me and my IT staff to get the job done right.

One of our major concerns has always been the security of our clients’ sensitive data. Recently, there have been stories in the news about data media getting lost or exposed, often with damaging or embarrassing consequences. Backup tapes, hard drives, CDs and other sources contain exponentially more data than a box of paper, so we have had to become very focused on how these data storage devices are tracked, stored, managed and disposed of when the time comes. Now that storage is so inexpensive, more data is sitting on a single disk or drive. New terabyte disk drives are setting a new standard for capacity — but they also send up a huge red flag for risk. What if one terabyte hard drive was to fall into the wrong hands? Imagine the fallout and liability to which a law firm could be vulnerable.

Also, since our firm does insurance defense, we are frequently handling

**Michael Chung** is IT Director of Lester Schwab Katz & Dwyer, LLP, a law firm with offices in New York City and Millburn, NJ. Based in the firm’s New York headquarters, Chung is a member of ILTA (International Legal Technology Association) who has worked in the IT field for 15 years, 11 of which have been in the legal vertical. He can be reached at [mchung@lskdnylaw.com](mailto:mchung@lskdnylaw.com) or 212-964-6611.

our clients’ confidential medical records. Our main compliance consideration with these files is HIPAA (the Health Insurance Portability and Accountability Act of 1996), which requires that we keep the information for seven years to allow for recovery of data; then we need to make sure that the data is destroyed. In addition to medical information, we often have access to private information for defendants, such as Social Security numbers and personal details. In order to comply with HIPAA’s “due diligence” clause and its privacy requirements, we need to erase the data when it’s no longer needed.

## LOCKING DOWN THE DATA

Because of the inherent risks that go along with handling confidential data, we lock down our technology — both from a virtual and physical standpoint. For example, we lock the users’ workstations down tightly. Users cannot save locally to their machine’s hard drive.

However, we know that this level of virtual security still leaves a few loopholes. When a user opens a document, a copy is opened and saved on the local machine as a temporary file. When the user saves that file back to the server, the temporary files on the local machine *should* be deleted, but sometimes that doesn’t happen. Also, if people are surfing the Internet, the cached information still remains on their local machines. Again, the temporary files should be deleted, but aren’t always.

As for physical data security, we have really woken up to the need for it. We keep an official inventory list of each piece of technology equipment at the firm. The list contains the equipment serial numbers and lease duration data. We lease equipment for three years and we generally have six months’ lead-time to replace old equipment with newer models. When we are ready to replace equipment, we take an inventory of all equipment that has been collected and compare it with the leasing company’s manifest from when they first leased it to us.

## DATA DESTRUCTION

Another area we have paid sharp attention to lately is the proper destruction of data and computers that we no longer need. Every year,

we replace and upgrade workstations and other equipment for several users, and disposing of data-bearing or defective hard drives has always been a concern. Also, our department must continually discard used backup tapes and obsolete handheld devices such as Blackberrys.

Like many firms, our biggest problem was to figure out how to properly erase or destroy information that resided on our employees’ hard drives and on backup tapes. Most law firms simply reformat the tape or hard drive and then consider that they are clean and reusable. We used this reformatting method, using a Norton software application to do a DOS-level format on the hard drive. As an extra measure, we would then run a magnet over the hard drive to make sure that it was data-free.

The bad news about the reformat and demagnetizing process was that it was inconsistent. At times, we would boot up some drives and still find data on them. In addition to being an unreliable erasure method, the reformat and magnetize process was extremely time consuming for my staff. Each hard drive would take between 20-60 minutes to reformat — my staff did one drive manually and would then test to make sure the erasure was complete. For a mass cleanup of machines, if we wanted the process to be done efficiently with good concentration, it would take one of my people a whole day to reformat and test the disks. With a lean staff, it was a real hardship to lose a person for an entire day, but we didn’t have an alternative to this method at the time.

Realizing that this method was neither efficient nor effective, I went looking for a better solution. I asked some of my fellow legal IT colleagues about their data media destruction methods. Most of them were doing a process similar to ours. Some of them were using more physically aggressive approaches such as smashing the drive plates with a hammer or drilling holes in the drives. Those approaches were worrisome to me — especially with the rising tide of forensic data recovery specialists who could have probably extracted pure data from the remains left by the smash or drill methods.

*continued on page 8*

---

## Physical Data Security

continued from page 7

### HARD DRIVE SHREDDING

The solution for this problem came from an unusual source — an IT consultant who was working for Tiffany's, the internationally known jewelry company. The consultant told me that Tiffany's was using a company called Back Thru The Future ("BTTF") ([www.backthruthefuture.com](http://www.backthruthefuture.com)) to recycle their old and obsolete computer equipment. Apparently, BTTF would accept the computer equipment, remove the hard drives, and shred them to eliminate any risk of the data getting into the wrong hands. I was intrigued by this report and wanted to find out more.

My first thought was that this would solve our computer-recycling dilemma. In the past, we had been donating our used computers to a non-profit organization. After the charity picked the machines up from our office, we had no idea what happened to them, which was a definite risk for our firm to be taking. And New York laws prohibited us from throwing the hardware in the trash, so that was not an option either.

### WITNESSING THE SHREDDING PROCESS

As part of my due diligence, I visited Back Thru The Future's headquarters, which is a 40,000 square foot facility in northwestern New Jersey.

While at BTTF, I witnessed the hard drive shredding process, which was done by a massive, custom-built machine that pulverized drives, backup tapes, CDs, Blackberrys and other data media. After the shredding process, which happened in seconds, the hard drives were transformed into small scraps of metal and plastic — completely unrecognizable compared to their previous identities as tapes or drives.

The shreds were collected in boxes, weighed and then shipped to a smelting location where they were melted and separated into metals and plastics, mostly aluminum, which is then reusable. The process was 100% guaranteed to completely destroy the data so there was no chance of exposure. Also, the shredding process was relatively inexpensive so it would not expand our budget significantly.

BTTF called this shredding process Safe Harbor Data Destruction due to its compliance with the amended

Federal Rules of Civil Procedure that govern data storage and electronic discovery. The company maintains a strict audit trail on all shipments, using lock boxes, digital photos and both paper-based and online tracking methods to assure law firms that the shipment has been received, processed and completely destroyed.

From an environmental standpoint, I wanted to make sure that the hard drive shredding was going to be "green." Our firm is very intent on recycling and other environmentally friendly methods. I was relieved to find out that BTTF has been approved by the EPA, New Jersey Department of Environmental Protection and county authorities. Since the shredded materials are recycled, nothing needs to end up in a landfill.

### FUTURE PLANS

We have been shredding hard drives with BTTF since April 2007, and so far the process has gone smoothly. At this time, we are just shredding hard drives, although we will probably start shredding backup tapes and Blackberrys in the future. Also, we will consider shredding printer and fax drives as well, when our equipment leases are up.



---

## Data Mapping

continued from page 6

High on the storage list are thumb drives that today can also host applications as well as data files (U3 and PortableApps.). Less common, but rising fast, is the use of Internet-based storage hosted by sites such as iBackup, Xdrive (a service of America Online) and GlobalDrive which offer online storage for all types of data. Finally, social networking sites such as MySpace.com and blogging sites often contain enormous amounts of data, communications and commentary.

- *Leverage Existing Processes to Keep the Map Current.* Business and the technologies that support it are a constantly moving target

and a data map needs to accommodate that. IT departments already have a wealth of pre-existing systems and frameworks that deal with change management and could facilitate data map maintenance without initiating new systems and initiatives. For example, the existing documentation and processes for adding more licenses, or new hardware, or sun setting and decommissioning systems would only need an "extra step" added to the process to update the appropriate information in the data map.

In the end, data mapping provides a vital tool for educating and communicating the state of an enterprises' electronically stored information as a foundation for both corporate litiga-

tion preparedness and corporate data security. Working together, corporate counsel and IT can create a comprehensive, clear and updateable catalog of the company's ESI, data mapping represents a readily accessible resource of the sources, locations, formats and uses of the business' records and the corresponding written and unwritten retention policies and practices. This mapping will add value to the business enterprise for data security programs by helping the business understand its ESI in order to fashion secure access and ensure privacy. This mapping will also help the business and its outside counsel to navigate the often-treacherous waters of e-discovery, yield e-discovery savings, and protect against sanctions.



To order this newsletter, call:  
1-877-ALM-CIRC

On the Web at:  
[www.ljnonline.com](http://www.ljnonline.com)