

## Get Back to the Real World of Security

### *Ensuring Proper Physical Data Security and Destruction Throughout The e-Discovery Process*

By Christy Burke

Properly securing physical data before, during and after litigation often can be eclipsed by concerns about online “virtual” security issues. Agreed — firewalls, data encryption and password protection are vital safeguards. But another part of the story is how to properly secure and dispose of your hard drives, CDs, backup tapes, and obsolete hardware such as laptops, PCs, PDAs and thumb drives.

Ignoring physical data-security considerations is not only careless and irresponsible — it is just plain dangerous. Data exposures can lead to severe consequences from public relations, legal and financial standpoints, and can be especially precarious issues for law firms entrusted with safeguarding clients’ electronic data, along with their own. From a legal standpoint, allowing data to fall into the wrong hands can mean loss of claim to privilege or lead to malpractice allegations.

Even Fortune 500 companies with huge security budgets have dropped the ball on the physical security of electronic media. A nightmare can result from misplacement of a single media-storage item like a CD or backup tape.

#### **CAUTIONARY TALES**

In May, telecom giant Alcatel-Lucent (“Alcatel”) suffered a crushing blow when a CD went missing in transit between two vendors. The CD included 200,000 confidential employee records, detailing salaries and Social Security Numbers. The company involved the U.S. Secret Service and New Jersey State Police to find the missing CD.

Shortly before Alcatel’s incident, an IBM contractor lost multiple tapes containing identification information about current and former employees. Out of desperation, Big Blue ran ads in newspapers offering a reward for the missing tapes.

What would you say to Alcatel or IBM if they were your clients? Imagine the exposure to potential litigation they would have if the missing data were posted or sold on the Internet. It’s a thought of exponentially magnifying scariness.

As a legal-services provider, ask yourself whether you are instructing your clients on the best practices for physical data security to prevent such debacles. And then ask yourself whether your firm’s IT department and computer-forensics vendors are applying that same rigorous standard for you.

Compliance regulations such as Sarbanes-Oxley, HIPAA and the amended Federal Rules of Civil Procedure (“FRCP”) each dictate the required retention, protection and disposal guidelines to follow in business, and in e-discovery. To complicate matters, because the destruction of physical data involves not only managing abstract information but also discarding concrete physical materials, conscientious company officers must choose responsible disposal methods compliant with U.S. Environmental Protection Agency (“EPA”) guidelines.

#### **FRCP RULE 37(F) SAFE HARBOR PROVISION**

The FRCP’s Rule 37(f) Safe Harbor provision dictates that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information (“ESI”) lost as a result of the routine, good-faith operation of an electronic-information system. The rule addresses the routine modification, overwriting and deletion of information that applies to normal use of electronic-information systems. Under the 37(f) rule, the court is required to examine whether the loss or alteration of data occurred as a result of “routine, good-faith operation” of the system — and the rule gives courts wide discretion.

To comply with 37(f), corporations and law firms are authoring and refining document-retention policies that set processes of data stewardship. The policies can range from a few pages to a few hundred, depending on the level of detail provided. Don’t forget that providing explicit instructions on how the data is to be secured and disposed of is as important as describing how it should be retained and stored.

#### **SECURED PHYSICAL DATA TRANSPORT AND DESTRUCTION**

On the plaintiff and defense side of litigation, discovery data must be physically secured during the discovery phase and then must be properly disposed of. Security in transporting data is essential, as seen in the Alcatel CD loss. A track-

able and trustworthy transport method is essential to protecting the data. Use of armored-car services, secured couriers and professional security companies to guard the shipments or storage can be appropriate, given the sensitivity of the data and the client's financial resources to cover the costs. Physical data-security handling and purging must be managed in a disciplined, consistent way.

### **Physical Data-Destruction Options**

Under the Safe Harbor rule, a company or law firm is entitled to destroy data that it is no longer required to keep. Purging this data can be part of a routine business operation. But the electronic-discovery materials (hard drives, server drives, backup tapes) can't be simply discarded as trash. Not only does this risk data exposure, but it's environmentally irresponsible to send that material to a landfill.

Acknowledging these needs, numerous vendors have surfaced to provide effective, efficient and safe physical data-destruction or data-erasure. The new methods dramatically improve on Neanderthal approaches of old, such as destroying hard-drive platters with hammers, or cutting the platters with scissors. Software-based and physical-destruction "shred and melt" methods are available — but which is more effective?

### **Data-Erasure Software**

*Data-erasure software* is a slightly misleading term. These products don't erase data, per se — but overwrite or "wipe" the data on the disk many times so that underlying original information is rendered unrecoverable by most methods available to the general public.

*The National Industry Security Program: Operating Manual* (DoD 5220.22-M) has set the standard for electronic-media sanitization and

**Christy Burke** is a New York City writer who covers law and technology. She is president of Burke & Company LLC which provides media services for a variety of clients, including Back Thru The Future, a data-media destruction company mentioned in this article. Reach her at [cburke@burke-company.com](mailto:cburke@burke-company.com).

destruction. It's generally accepted that seven to 31 passes will render data unrecoverable. Some products far exceed these government requirements.

Sonja Robinson, FTI Consulting's director of forensics-lab management says: "You can buy software which does DoD (Department of Defense) wipes with seven to 31 passes. Software-based data-erasure products may be very good and reliable, but their accuracy and thoroughness may depend on how they are configured. The issue really is (the) potential for future recovery based on current and future technologies. What was good software five years ago might not stack up against today or tomorrow's modernized data-recovery tools and techniques."

Rather than using software-based methods, FTI sends its electronic media to a third-party vendor that shreds hard drives and melts the contents to preclude any chance of recovering the data.

"If physical destruction is done properly, it's the best because you can't put it back together again — you can't unmelt or unshred a properly destroyed drive," Robinson says.

### **Physical Data Destruction: Shredding and Melting**

Bob Johnson, executive director of NAID (the National Association of Information Destruction) — the international trade association for companies providing information-destruction services that consists of 845 members, approximately 5% of which are primarily involved in electronic media destruction — explains that about 300 NAID members have achieved NAID certification, a handful of which are electronic data-destruction providers. The NAID certification process is rigorous, consisting of planned and random audits to ensure that certified vendors understand the data-destruction business and are highly quality, fully compliant service providers. Johnson points to Back Thru The Future as an example of an NAID-certified electronic-media destruction company.

Back Thru The Future ("BTTF") is a New Jersey-based data-destruction

and computer-recycling company that has developed a secure data-destruction process specifically designed to comply with the FRCP and environmental statutes, and to satisfy NAID's certification requirements. BTTF's process is called safe harbor data-destruction, or SHDD, so named for its compliance with FRCP Rule 37(f).

"Data-destruction needs to be handled as a *process*, not as a project, and it needs to be supported by auditable records," BTTF Vice President and CFO Dan Bayha says.

BTTF maintains a 40,000-square-foot facility in Ogdensburg, NJ, that houses a custom-built electronic media-shredding machine that grinds hard drives, PDAs, backup tapes and other media into paper-thin shreds that are then sent to be melted down. The entire process is auditable. It is documented with paperwork, digital photos and an online tracking-service portal provided for compliance. Bayha says that law firms, corporations and government entities choose media-shredding because it complies with legal and environmental regulations, and is cost-effective.

Bayha adds that many clients initially come to BTTF needing to shred boxes of loose defective hard drives that have been sitting on IT staff desks or in storage closets. Because IT personnel are always putting out the fires of the day, defective hard drives tend to stack up and become a dusty little secret that always falls to low priority. Bayha refers to these defective hard drives as "EDD Trojan Horses" because although they appear harmless, they contain pure data and are exciting finds for forensics teams because they often contain unpurged material.

"Failure to destroy data when the time comes can have heavy financial consequences," Bayha cautions. "Imagine if the company was sued and that data from unpurged drives and tapes was all discoverable. Processing that data could cost clients thousands or millions of dollars in consulting fees. Whatever isn't destroyed can be discoverable, so having a destruction regimen is critical to law firms and their clients."

Clients ship boxes of hard drives, CDs, PDAs, backup tapes and other materials to data-destruction facilities by various secure methods. Many law firms and forensics shops keep secure, locked storage containers on site and fill them as media items accumulate. The containers are then shipped or sent by secure transport to the shredding facility, where the locked container is photographed on receipt to prove that the shipment wasn't tampered with in transit.

"Prior to having the drives shredded and melted, we used to reformat our hard drives and demagnetize them with a large magnet," says Michael Chung, IT director of Lester Schwab Katz & Dwyer, LLP, who uses the Back Thru The Future SHDD service for hard-drive destruction. "That procedure was time-consuming and inconsistent — sometimes a hard drive would still (work) even after we 'erased' it."

Chung elaborates on the advantages of using SHDD.

"Before we started physically destroying the drives, there was no way of guaranteeing that all the data was gone from previous usage," he says. "Also, physical shredding is ten times more cost-efficient than our previous method since I don't have my staff spending 20 to 60 minutes reformatting each hard drive."

## ENVIRONMENTAL CONSIDERATIONS OF DATA DISPOSAL

Data-destruction companies like BTTF are certified by the EPA and by state environmental-protection departments ("DEPs"). Once the media are shredded, the fragments are sent to a smelter. The melting phase is environmentally important because the resulting metals and plastics can be recycled.

Reenee Casapulla is coordinator of recycling for the Sussex County (New Jersey) Municipal Utilities Authority. (BTTF's facility is in Sussex County.)

"The smelting process is environmentally friendly," Casapulla notes. "Because the aluminum is reused, it reduces the requirement for new mining of raw materials. Consumer electronics represent so much metal. The more we can reuse it, the more successful we can be at protecting the environment."

Casapulla adds that businesses, law firms and corporations must realize their level of responsibility for the waste they generate.

"Businesses think that they don't make a difference with their waste numbers," Casapulla says. "As residents, the companies' executives and employees recognize their responsibility to recycle, but they often fall short in developing recycling programs for their businesses."

No federal legislation governs how electronic data should be disposed of — all existing laws are state and municipal. NAID's Bob Johnson, though, foresees national law becoming reality very soon.

"Information-destruction will increasingly get the attention of high-level executives because they are now being held accountable for it," Johnson says. "Many data-protection bills are being circulated in Washington, DC, right now that address this. Within the next two years, or sooner, I believe that this legislation will definitely materialize on a federal level."

Physical data-security concerns aren't going away; if anything, they're escalating as fast as the digital world expands into terabyte hard-drive territory. Law firms, forensics shops, litigation-support vendors and their clients can all learn from the mistakes of blue-chip companies. Unless you do, you might make the next "Have you seen my data?" headline — and see how true the old adage *not all press is good press* is!



The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.