



150 Main Street
Ogdensburg, NJ 07439



973-823-9752
www.cdrecyclingforfree.com
www.backthruthefuture.com

The Physical Security Side of Electronic Data Discovery: From Preservation to Destruction

By Dan Bayha, VP of [Back Thru The Future](http://www.backthruthefuture.com)

In November 2007, it will be a full year since the amended Federal Rules of Civil Procedure were laid down, carrying with them a whole new vocabulary containing terms such as “Safe Harbor” and “Litigation Hold.” In the past year, law firms and other entities have been struggling to get on top of their record retention and disposal practices, as mandated by FRCP and other compliance requirements such as Sarbanes-Oxley.

On one hand, there has never been a higher value placed on prompt and efficient destruction of unnecessary stored data. On the other hand, inappropriate destruction can land you in jail for several years. 18 U.S.C. Section 15.19 Sarbanes-Oxley states, “Whoever knowingly destroys or conceals a document with the intent to impede an investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States may be imprisoned up to 20 years.” Law firms and corporate counsel have to walk this tightrope even more carefully, since they are stewards of their clients' sensitive data as well as their own.

Many major law firms have spent considerable time and effort on the systematized purging of online electronically stored information (ESI). However, their processes are often incomplete, flawed, time-consuming or all of the above.

Law firms can't assume that just because their firm has an internal data destruction practice, that this practice will be permanently sufficient. Most disposal practices were developed years ago, using techniques that were adequate at the time. Today, we have a whole new ball game. The amount of ESI is increasing exponentially. An average hard drive's storage capacity increases 50% annually. Terabyte (1 trillion bytes) capacity hard drives are available today at a cost of around \$500.00 each. That works out to a cost of fifty cents per gigabyte (1 billion bytes). Storing data electronically is dirt-cheap.

Because data storage is so inexpensive, we find all types of office electronics capable of storing massive amounts of data. Each one of these devices requires different data erasure tools to “clean” it for possible reuse. So not only is the amount of data to be destroyed expanding rapidly, but the devices storing the data are proliferating. All of these devices could contain highly sensitive data, at risk both from a data security standpoint and an EDD standpoint. As one lab manager of a major forensic data recovery firm states, “new forensic techniques are being constantly introduced. A data destruction



technique that is adequate today may be inadequate tomorrow. It's a constantly evolving world.”

In addition, little attention has been given to data stored on static, obsolete or defective data storage devices. Forgotten or misplaced back-up tapes have repeatedly done significant legal harm. In the *Coleman v. Morgan Stanley* lawsuit, mismanaged back-up tapes cost Morgan Stanley a \$1.2 billion judgment. Virtually nothing is more dangerous than an obsolete or defective data storage device containing pure historic data. Also, the cost to discover a large quantity of old hard drives or tapes could reach six figures.

Data recovery forensics are so sophisticated that devices that have been “erased” by software-based tools are now at risk. Even if the erasure effort is effective, you can be challenged later as to why you erased the device. The appearance of a cover-up is often more damaging than exposure of the destroyed data would have been. The bottom line is that not only should you promptly destroy data stored on obsolete storage devices and media; you should also immediately dispose of the devices themselves.

Proper disposal of data storage devices and media is just one aspect in the protection of the information stored on these devices. “Chain of custody” is a component critical to the collection of data during the electronic discovery process. The forensic data discovery credo of “If you miss a bit, you must acquit,” testifies to the importance of preserving and protecting the authenticity of the discovered data.

Preservation, Protection and Proper Destruction of ESI

Law firms can learn from the ESI handling procedures developed by the forensic data discovery industry to protect discovered data. They set the standard for all organizations charged with protecting highly-sensitive information. Forensic data recovery is a serious effort, performed by highly trained professionals using state-of-the-art data recovery tools. Today, there are over 1,000 companies in the data forensic/electronic data discovery business. It is a multi-billion dollar industry primarily focused on supporting the legal profession's electronic data discovery efforts. If you have not had an opportunity to attend a conference where data forensic techniques are presented, you have missed a real eye-opener. You'll think about what you save on your computers and PDAs in a whole different light.

Data handling procedures used by forensic data recovery specialists constitute quality groundwork for all parties handling EDD. Their guidelines include the following:

1. The technology of both the hardware and software used in the forensic discovery process has been specifically designed to image or copy data in its exact form. That way, there can be no question as to the authenticity of the data.
2. The recovered data never leaves the possession of the forensic expert while being searched through or when in transit.

3. Once the recovered data is delivered to its secure storage location, tight auditable records are kept of who accesses it, when and why.
4. Upon completion of the litigation, the data storage media and its recorded data are physically destroyed in an auditable manner.

What can we learn from these EDD procedures that will aid us in the improvement of our own physical data security procedures?

Internal “Chain of Custody” Concerns to Protect Data Devices in Your Possession

Knowing where a storage device is, who is responsible for the device, and maintaining an audit trail of this information significantly improves security accountability within your firm. It is the responsibility of your firm's security and/or IT department to regularly confirm and verify control and location of the devices. This confirmation reminds all employees of their responsibility to protect the firm's sensitive information. Unchecked failure of individuals to follow procedures is one of the most significant weaknesses in most data security processes, so compliance should be monitored and spot-checked frequently.

Two recent security breaches highlight the importance of internally protecting data devices from a physical standpoint.

First, our country's nuclear laboratories in Los Alamos, N.M. lost two hard drives containing nuclear secrets in a single year. One of the hard drives was eventually found in a local used computer store. The head of security at Los Alamos was quoted as saying “the best security procedures in the world are worthless if people don't follow procedures.”

In a second example, VeriSign, one of technology's highest profile security companies, announced the theft of a company laptop computer containing highly sensitive information. The company said the laptop was stolen from an employee who failed to follow company policies, which were in place to prevent these types of occurrences. Clearly, though there was a policy, it wasn't effective enough to prevent this disaster. Highly secure procedures need to be redundant. You must always assume that a single procedure may fail. Human error is a given. Redundant physical security procedures should be varied and should be performed by different people.

External “Chain of Custody” – Securely Transporting Data Devices

Transporting of data storage devices containing sensitive data requires strict protocols. Lost or stolen data storage devices and storage media are among the most commonly-reported causes of significant data security breaches.

- Alcatel-Lucent recently reported that a CD was lost in transport between two vendors. 200,000 confidential employees' records, including salaries and social security

numbers, were compromised.

- The State of Ohio announced the theft of a single backup tape from the car of a summer intern who was delivering it to a vendor. The device contained tax records including social security numbers of 860,000 Ohio taxpayers.

Legal chain of custody techniques are available to law firms and should be chosen according to the data's sensitivity. Imagine shipping a back-up tape or a CD containing information that a firm has spent literally millions of dollars creating, collecting and protecting through your firm's mail room via UPS or FedEx - which then goes directly to a vendor's unsecured mail room. Although more expensive, there are definitely more secure methods of transport than UPS or FedEx. For example, the armored car industry has been providing ultra-secure "Chain of Custody" transportation services for decades. Also, using secure locked shipping containers for shipping devices and media containing sensitive information should be a minimum standard when sending sensitive data devices.

Data Destruction Best Practices – Evaluating Destruction Methods

When disposal of sensitive data is required, your disposal process must be absolute and auditable. Under no circumstances should destroyed data be recoverable by any method. It is not good enough to be 99 percent confident in your process. You need to be 100 percent sure, 100 percent of the time.

As discussed earlier, data forensic techniques are constantly being improved to subvert technology-based data destruction methods. A reminder of this reality is recent news concerning a police department in N.J. A computer from the police department was sold at auction and was purchased by a local activist. Using freeware data recovery software found on the web, he was able to recover both sensitive police department information and the officers' embarrassing illicit Internet usage. This information was then posted to the Web and became a state-wide scandal. This data recovery and Internet distribution of the data was accomplished by a non-technical person who used easily-available data recovery tools to harvest remaining data from a hard drive supposedly "erased" using software tools.

- **Software Erasure Tools**

"Software erasure" is in fact a misnomer. Software data destruction is actually performed by recording or "wiping" meaningless data over the surface of the data to be destroyed. Between 7 and 31 DoD (Department of Defense) wipes is the generally-accepted standard for electronic-media sanitization and destruction, as set out by the National Industry Security Program: Operating Manual (DoD 5220.22-M). The more secure the destruction process, the more times the surface must be "wiped." However, even if the software did 1,000 wipes, the data would still remain intact underneath layers of code. One would think that data so carefully buried would be unrecoverable. Unfortunately, the above-mentioned N.J. police department found out that this is not always the case.

There are several significant limitations to the software-based erasure process:

1. In order to be wiped using software tools, the “to be erased” device must be operational. You can’t apply this tool to a defective device.
2. A second concern is what is technically known as “flagged” tracks on hard drives. As part of a hard drive's error-detection and correction routine, the recording surface of the disk is self-monitored for marginal recording areas. If a questionable recording area is identified, the recorded data in the area is copied and moved to another location on the drive. The questionable area is then “flagged” and no further recording is permitted on that spot. The recorded data in the flagged area still remains on the drive, but it is no longer accessible by software. All hard drives over time will accumulate “flagged” tracks; software erasure tools cannot wipe over these areas. However, the data in the flagged areas is recoverable by forensic data techniques, so it is a potential data exposure risk.
3. Software tools must be applied by trained technicians, which means that their effectiveness is subject to human error. One of the reasons you rarely find extensive software warranties is that manufacturers know that the correct use of their technology depends on the correct installation and operation of their product across widely-varying hardware and software configurations. Even the manufacturers of software erasure programs qualify the expected results based upon variables of operator thoroughness and accuracy.
4. The fourth problem with software erasure tools is that they require an inordinate amount of time to securely overwrite high-capacity hard drives. For example, it takes several hours to apply a highly secure software erasure tool to a 20 gigabyte hard drive. A terabyte hard drive will take over a week to erase via software, even if the erasure tool is running 24 hours a day. IT staff applying these tools are generally highly-paid computer technicians. Because they are spending time on software erasure, their attention is drawn away from supporting the firm's software and user base. The overhead cost of applying software erasure is increasing in direct correlation with the increase of drive storage capacity.
5. The final problem with software-based erasure methods is that data recovery software is being advanced and developed at an alarming rate. Even if your firm were to purchase software erasure tools today, they may be obsolete within a matter of weeks, months or years as the data recovery tools and techniques may evolve beyond it. As such, software erasure tools are not a one-time purchase and expense. Instead, they need to be continually maintained and updated, another burden for your IT staff and budget to bear.

- **Degaussing**

Another data destruction technique primarily used by government agencies is degaussing.

Degaussing uses a strong magnetic field to erase magnetically-recorded information on hard drives and tapes. It cannot be used on non-magnetically recorded media such as CDs and optical disks.

The single biggest problem with degaussing is that in order for the process to work, the degausser's magnetic field must be stronger than the magnetic field of the recorded data. The higher the storage capacity (the denser the recording) of the storage device, the greater the magnetic strength of the recorded data.

Newer high capacity hard drives require extremely strong degaussing fields. You constantly need to upgrade your degaussing equipment in order to erase newer media. Degaussers are mechanical and require regular recalibration.

Also, the ultra-strong magnetic fields created by a degausser require that they have a proper operational environment. Any electrical device in proximity is subject to damage and there are health considerations for employees, especially for those who have a pacemaker.

- **Physical Data Destruction**

A third destruction technique is physical destruction. A major challenge to this process is that hard drives are designed to physically protect the recording surfaces. The outside cases are made with thick aluminum, not a material easily breached. Hitting a hard drive with a hammer may make the drive nonoperational but the recorded data can easily be recovered by forensic data recovery tools. The same can be said about drilling holes in hard drives. Most of the data can still be recovered.

Physical Data Destruction by Shredding

Physical data destruction by shredding—a recently introduced service—is the only 100 percent absolute data destruction method available. In theory, the process is very similar to paper shredding but the machines used to destroy data media are “paper shredders on steroids.” Because of the immense size of the necessary equipment, hard drive shredding is usually provided by a vendor off-site rather than internally.

Selection of a hard drive shredding vendor should be done with the same caution and criteria used when selecting a forensic data recovery firm. The vendor's handling of your data storage devices to be destroyed should have the same meticulous care applied during the entire process. The destruction path ought to be tightly controlled with detailed, auditable records.

Because data media shredding is a relatively young service industry, confirming the vendor's experience and obtaining references is essential. The National Association for Information Destruction (NAID) screens and vets potential secure destruction vendors. NAID evaluates and certifies qualifying hard drive shredding vendors as AAA secure

data destruction facilities. NAID's certification process is rigorous, ensuring that certified businesses understand secure data destruction and provide high-quality and regulatory-compliant services.

Physical destruction has the additional benefit of being “technology indifferent.” To the destruction machine, shredding a hard drive or backup tape is no different than shredding a Blackberry PDA. Once a decision has been reached to physically destroy by shredding data storage devices and media, there is no need to revisit the process because of recent software advances or upgrades.

Physical data destruction is a permanent solution. After the data media is shred, it is sent to a smelting facility where the resulting fragments are melted down into source metals and plastics. For law firms with “green” and environmental priorities, this shred-and-melt process means that no remnants of the data media end up in a landfill.

Absoluteness and Auditability of Destruction Methods

Whichever destruction method you choose, auditable records of your destruction process are essential. Auditability or the ability to prove that you destroyed data in the normal course of your ESI management is a core principle of the Federal Rules of Civil Procedure's Rule 37(f), the “Safe Harbor” rule. This rule states:

“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.”

ESI destruction in any form must be part of a documented and regularly-monitored record retention and disposal policy. Casual, undocumented data destruction events are simply too risky to be permitted. Destruction must be part of a continuing disciplined process. Systematized repeatability is the principal characteristic of a qualifying “Safe Harbor” destruction event.

Conclusion

Law firms are on the bleeding edge of ESI's new reality. There are huge risks and liabilities associated with the ever-expanding storage capacity of today's myriad data devices.

Law firms have unique exposure to the protection of sensitive and privileged client information. The intimate understanding of the risks associated with electronic data discovery provide incentive to introduce new and more stringent physical security measures for the protection and disposal of data storage devices and media.

If physical security is not given its appropriate level of attention, you are compromising the integrity of your firm's entire security process. By taking physical data preservation,

handling and destruction seriously, putting sensible procedures in place, and updating procedures as needed, you can safeguard your firm's most important asset – your sensitive data and that of your clients.

About the Author

Daniel F. Bayha, is the Vice President and CFO of Back Through The Future. He is a graduate of the University of Pennsylvania and Harvard Business School. He has spent his entire 35-year business career in the technology field, starting in sales with IBM and progressing through various management positions before establishing his own computer leasing firm in 1980. Dan has been the lead investor and senior executive in a number of computer industry businesses. He was an early investor and consultant for Back Thru The Future before joining the firm in 1992 as CFO.

In addition to his financial duties, Dan is responsible for marketing and sales efforts for Back Thru The Future's computer recycling and secure data destruction activities.

Dan is a recognized authority on the rapidly emerging secure data destruction industry. He was selected by NAID (National Association for Information Destruction) as the 2006 NAID Member of the Year for his contribution to the NAID committee responsible for establishing the secure data destruction industry's certification standards, relating to the destruction of electronic media. He recently was invited by the New Jersey Department of Labor to participate in a panel discussion on the topic of Economic Development. Dan is a frequent speaker and has published several articles related to secure data destruction practices.