



Managing Legacy Data

Daniel F. Bayha, Vice President

Back Thru The Future Technology Disposal
150 Main Street
Ogdensburg, NJ 07439
973-823-9752
shred@backthruthefuture.com

April 21, 2009

“Managing legacy data is the most important thing an organization can do to reduce risk and cost associated with electronic data.”

Anne Kershaw, A.Kershaw PC // Attorneys & Consultants

Legacy data is stored data that is no longer a part of your active information systems.

It can reside on backup tapes, obsolete or defective hard drives, floppy disks, CDs, ZIP drives, obsolete or out of use cell phones and PDAs.

The vast majority of legacy data stored on these types of devices and media is data that you are no longer legally required to retain. It costs money to continue to store legacy data and the continued storage of legally disposable data represents significant legal risk.

- State and Federal privacy regulations discourages the retention of personally sensitive information.
- Unnecessarily retained data exposes you to information theft.
- The storage of data storage media and devices is expensive.
- Unnecessarily retained data significantly inflates litigation costs.

The principal challenge for most organizations is identifying what information must be retained and what may be defensibly eliminated. In many cases organizations have been accumulating legacy data for multiple years and the task of cataloging the legacy data appears overwhelming.

Failure to address this problem can result in huge litigation costs:

Gartner estimates that the average E-discovery event costs \$1.5 M

Osterman Research estimates that 50% of organizations with over 1000 employees have had to perform 3 or more litigation related searches of electronic records within the last 12 months.

Being sued and the cost of litigation is a cost of doing business. Reducing the costs of litigation is an essential financial tool for any organization. Proactively addressing the legacy data problem will result in immediate savings in the cost of storage and the future costs associated to electronic data discovery events.

- It costs \$.08/mo or \$.96/yr to store a single tape off site,
- It cost \$.25 to destroy a single tape resulting in an annual savings of \$.71/ tape,
- The storage savings in the 1st year for 10,000 tapes would be \$7100.00

Data restoration and cataloging:

Specialized data restoration firms such as National Data Conversion, New York, NY, offer services to inventory and statistically sample legacy data media.

From the sampling you can segregate media that can be immediately disposed of from media containing data that needs to be further evaluated to determine the need to retain. In many cases this initial cataloging effort can result in the immediate reduction of 40-60% of the stored data media.

- It costs \$25 - \$40 per tape to do an initial cataloging
- It costs \$250 - \$500 per tape to restore it for legal review in a litigation discovery event

Issues may arise as to the legality of destroying certain stored data. Anne Kershaw, of A.Kershaw PC // Attorneys & Consultants, states that such decisions should be made within the context of your firm's retention policies and current regulatory and litigation requirements. Firms such as A.Kershaw PC // Attorneys & Consultants can work with clients to inventory all their data caches, identify what must be retained and what can be disposed of, and most importantly issue a memorandum of disposition providing the legal authority for the methodology taken in disposal decisions.

Now that I know what to destroy, what should I do?

Follow the S-I-I handling rules:

- **Segregate** – Separate all “to be destroyed” data storage material from other to be disposed of material.
- **Inventory** – Initiate the chain of possession records. Uniquely identify the “to be destroyed” data storage devices and/or media in order to establish your possession of the material at a point in time.
- **Isolate** – Isolate the inventoried items in such a manner as to prevent any unauthorized removal of an item from the disposal process. Collect and store the items in secure containers or a locked and securely controlled area within your facility.

Follow the A-T-A secure destruction principles:

- **Absolute** - Destroy the materials in such a way as to prevent any possible recovery of the data including the utilization of sophisticated data recovery techniques.
- **Timing** - Do not accumulate quantities of “to be destroyed” material. Remove to be destroyed material promptly from your facility preferably on a scheduled basis. Random destruction events should be avoided.
- **Auditable** – Detailed records should be maintained of all electronic records destruction events that prove that you follow a written destruction policy.

What Constitutes Absolute Destruction?

Destroying recorded data on multiple types of media is addressed by the National Institute of Standards and Technology (NIST) special publication 800-88 Guidelines for Media Sanitization. This is a free publication available as a PDF at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

The NIST publication is considered the authoritative “how to destroy recorded data” source publication. It breaks down the tools available to destroy recorded data on each type of media into categories:

Clear = Good

Purge = Better

Destroy = Best

The “Best” category is absolute destruction, while the “clear “ and “purge” tools will vary according to media type, the “destroy” by shredding tool is consistent over all media types.

Shredding of data storage devices and media containing legacy data is not only an absolute destruction technique it is also typically the least expensive solution.

Outsourcing physical destruction:

Given the specialized equipment required to shred varying types of data storage devices and media, outsourcing this activity is generally your only option.

Outsourcing considerations:

Vendor selection: Given regulatory and legal issues associated to the destruction of any type of recorded data, vendor due diligence is essential. The simplest approach to due diligence would be to select a vendor that has already been certified by a recognized industry certification group such as the National Association for Information Destruction (NAID) AAA secure destruction certification standard.

The NAID standard requires adherence to a list of more than 40 specific security precautions including employee screening, physical plant security and handling procedures.

At a minimum a vendor should be able to show:

- Employee screening
- Controlled facility access
- A secure storage and destruction area including surveillance capabilities
- Auditable records of destruction activity
- Required regulatory certification such as EPA permits for electronic recycling and disposal.
- Adequate Insurance coverage's including professional liability, and employee dishonesty coverage.

Chain of Possession:

Outsourced destruction may take place as mobile shredding performed in a truck at your facility or at a remote plant based facility. In either case, it is necessary for the shredding activity to generate an auditable record of chain of custody and disposal.

Assuming you have properly isolated the to be destroyed material in secure containers, you should be able to match the inventory of to be destroyed material that you generated when you place the items in the container, with the items removed from the secure container at the point of destruction. This type of inventory reconciliation is best done with the utilization of bar code labels. If bar code equipment is not available, a hand written list of serial numbers will suffice. Once the outgoing and incoming inventories have been satisfactorily reconciled, permission to proceed with destruction can be given.

The actual destruction event should be documented with:

1. Certificate of destruction which confirms the date of destruction,
2. Quantities of devices or media destroyed, and
3. Statement as to appropriate disposal of the shredded material.

Ideally this documentation should be made available in both digital and paper form. These records should be retained for a minimum of three years.

Destroying data of any type has become a complicated regulatory and legal issue. All organizations should have a written policy for its data destruction practices and should also maintain records to support that it is routinely following its own policy. Addressing legacy data is an important first step in the proper management of the risks and cost associated to the storage of electronic records.