



Effectively Implementing and Managing Data Disposal and Destruction

WE2-1219 Proceedings Paper

ARMA International 53rd Annual Conference & Expo
Las Vegas, NV

August 13, 2008

***Dan Bayha, VP/CFO,
Back Thru The Future Technology Disposal
Anita Castora, CRM, Manager, Document
Management, American Eagle Federal Credit Union***

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

INTRODUCTION AND SCOPE

Information systems generate an ever-increasing stream of to be disposed data storage devices and media. It is fundamentally important to assure the removal of all residual data that may be stored on these devices. Data storage technology has sped ahead, providing us with multiple new data storage appliances while adding huge increases in storage capacity. Attach to this issue the recent significant increase in government regulations requiring the protection of sensitive personal information and the legal issues of managing electronic discovery events, the challenge of properly destroying this residual data has become very complex. New tools and services are emerging to address this challenge and the purpose of this presentation is to introduce you to these alternative solutions and hopefully assist you when deciding how your organization might best adapt its data destruction procedures to meet this changing environment.

Records managers have the responsibility of managing their organization's information through its entire life cycle. No one in your organization has a better understanding of the importance of absolute records destruction. Failure to properly destroy an electronic record can not only lead to the unintentional release of sensitive information, it can lead to very serious legal consequences including charges of spoliation of evidence.

Some assumptions to be made are:

1. All records contained on media have been approved for destruction.
2. All records including paper, electronic, and mixed media have been taken out of active filing systems per authorized retention policies.
3. The categorization of the relative importance of the records contained on the storage devices and media has been done.

The term "Sanitization" will be used to describe the process of removing recorded data from the media on which it is recorded. This should not be confused with the software overwrite process commonly used for data erasure that is often referred to as sanitization.

How do Records Managers manage their programs and efficient destruction of records?

A solid Records Management (RM) program includes a Records Management Policy, Records Management training and the loop is completed with a compliance audit.

Records Management Policy will include procedural guidelines and a retention schedule that is updated regularly to meet any new laws. It is important to note that the retention schedule sets the precedence for when a record, regardless of media, can be properly disposed. This includes all systems, cell phones, Blackberrys and other PDAs (Personal Digital Assistant), just to name a few. This means that regardless of media

and storage tool, an effective process must be in place to successfully purge the data to meet compliance of the company's policy that is based on business need and regulations.

Records Management training is necessary for a company's program to be effective and is a strongly recommended best practice as a result of recent litigation and past experiences. It has also proven that when employees are trained and understand the Records Management (RM) program and there is a strong commitment from executive management, there is less chance of records being mismanaged. When there is a RM program in place, employees are more cooperative of the management and disposal of records and focus on their work responsibility and leave records to RM.

Compliance Audit - No RM program is complete unless a compliance audit has been conducted. A RM compliance audit is based on the company retention schedule. The RM program is based on keeping records in compliance with an approved retention schedule that is created from current federal and statutory laws and the company's business requirements. Again, it is very important to stress that compliance of all records regardless of hardware or software is critical. A company must demonstrate to the courts that it is following its retention schedule and is purging its records when they have met their business need per the Retention Schedule. Morgan Stanley, for example, produced records during its case, but later discovered additional records that it didn't know it had. Morgan Stanley was given sanctions of \$1.2 billion dollars because of poor recordkeeping and non-compliance of their policy. (Coleman Holdings, Inc. v. Morgan Stanley & Co., Inc.)

Records Managers usually perform an annual record destruction on a scheduled basis using an approved records retention schedule. This works for business records in a controlled environment, but a different approach must be considered with data storage devices.

How many of you shred paper?

How many of you use an outside service to shred the paper?

If these questions were asked 4-5 years ago, only a few of you would have responded affirmatively. Today, paper shredding is a multi billion-dollar industry with literally thousands of companies offering services across the country.

Why do we shred paper?

There are regulatory requirements to protect sensitive information and internal security requirements to protect internal information.

Why use third party organizations to shred paper?

1. Using employee time - on a cumulative basis, the amount of time gets to be sizeable. Using a third party is a more practical use of employees' time.

2. When you shred paper, it generates clutter and you must also dispose of the shredded material. Today, you'd also like to have that material recycled.
3. Control factor: third party professional shredders provide containers, scheduled performance and good documentation, which is something you don't get when you shred internally.

The reason businesses spend billions per year? It saves employees' time, disposes of a by-product of your business in an efficient and environmentally appropriate manner and it provides you with a uniform, easily managed process with good documentation.

We may spend billions of dollars to do this, but today paper represents less than 10% of all business records. The other 90% plus are stored in electronic format. A single gigabyte of electronic storage has the capacity to store up to 75,000 typewritten sheets of paper. This electronic storage activity generates a constant stream of to be disposed of data storage devices and media that contain records that must be destroyed for all of the same reasons you shred paper, only magnified thousands of times. Historically IT departments have performed this destruction activity as a security precaution.

Recent regulatory requirements concerning the protection of personally sensitive information and litigation issues associated to electronic data discovery have placed significant new requirements on the entire destruction process. In December 2006, the federal courts amended the FRCP as it relates to electronic discovery. One of the provisions of this amendment was rule 37(d), (3), (e), the safe harbor data destruction rule. Under these new provisions, we have seen courts permit the utilization of forensic data recovery techniques and we've seen ad hoc data destruction activity be challenged as spoliation of evidence.

How is a records manager able to comply with the requirements of destroying electronic information as required under new regulations and under his or her own internal security requirements, but also deal with the issues of litigation hold?

One of the objectives of this presentation is to provide records managers with the tools and processes necessary to both protect your organization but also to be in full legal compliance with court rules relating to electronic discovery.

How do you destroy your hard drives and other devices that hold data?

Do you manage the destruction of hard drives, USBs, tapes, CDs, DVDs like you do paper?

Do you reformat the hard drive and leave it at that?

Do you donate used hardware to outside companies without removing the hard drive?

ATA principles of proper data destruction:

A – Absolute: When you have permission to destroy a record, you want to destroy it in a way that it can never possibly be recovered under any conditions, including forensic data recovery techniques.

T – Timely: Accumulation of data storage devices is a dangerous practice and should be minimized and all destruction events should take place on a scheduled basis avoiding ad hoc destruction activity that can lead to legal challenges as to the timing of the destruction event.

A- Auditability – Under the FRCP safe harbor data destruction provision, you must be able to prove that your destruction activity is “routine” and done in “good faith”. Detailed destruction records provide auditable proof that you “routinely” followed your own “good faith” destruction policies.

Issues of associated to absolute destruction and the alternative ESI (Electronically Stored Information) destruction methods:

We will be referencing, with permission, the work prepared by the “Computer Security Division of the National Institute of Standards and Technology (NIST)” publication 800-88 “Guidelines for Media Sanitization” This work was originally completed for the Office of Homeland Security and is the United States government standard for all government agencies and is considered the current authoritative source for all media sanitization issues.

(Refer to tables in handout.)

The “Clearing” or “Purging” technique may be chosen, but each type of media requires a different tool. The only consistent tool across all types of media is physical destruction by shredding and it is the “fail safe” alternative.

Timing of destruction events.

This is one of the most common problems with organizations’ current electronic data destruction procedures. Because electronic data destruction has been looked at as a security precaution, as long as the data storage devices remained within an organization’s security perimeter the timing of the destruction activity was not considered important. “Litigation hold” requirements have cast a whole new premium on promptly destroying information when permissible and the prompt removal of the devices and media from the organization’s facilities. Even if the media is promptly sanitized, the discovery of a sanitized storage device during a discovery process can lead to questions as to why the media was sanitized and what was on it. This can be an extremely time consuming and expensive question to answer. The average cost to forensically examine a single storage device is \$5000.

Detailed and auditable records for destruction activity are needed.

Here again we have a new requirement that is not typically addressed in current destruction procedures. All media should be segregated, inventoried and isolated in a manner that reasonably minimizes the chance of unauthorized access and diversion of the media from the destruction process - both at your facility and during transportation. This process is generally known as "chain of custody". The ability to track individual storage devices such as hard drives, PDAs, cell phones by serial number from the original user to final destruction is a best practice to be strived for. The more detailed your records, the more credibility during audits and litigation.

So now that you have a policy in place that covers the ATA principles, the issue is - do we want to perform this activity internally or outsource? Let's revisit our original questions about choosing a third party paper shredder. You will want to apply similar processes to your data storage devices.

You want to save time, you want an efficient and environmentally appropriate disposal process and you want a procedure that has tight controls with auditability.

You've decided to consider a third party. How do you select one?

VENDOR SELECTION. The vendor selection criteria below are from the National Association for Information Destruction (NAID) certification program (www.naidonline.org). A NAID AAA certified secure destruction facility must meet these audit criteria. If the vendor is not certified, a vendor due diligence visit should include:

1. Vendor employee screening criteria:
 - a. Employment history verification
 - b. Criminal record search (at least 7 years)
 - c. Drug screening with annual random screens
 - d. Signed confidentiality agreements
 - e. I-9s

2. Operational Security:
 - a. A written procedures manual should include
 - o Step by step description of control of media
 - o Access controls
 - o Description of exact destruction process
 - o Time frame for destruction
 - b. Visitor logs and visitor badges.
 - c. Walled or fenced secure areas with lockable doors and gates and video surveillance on all entrances and exits and work areas. The video records should be maintained for at least 90 days
 - d. A secure storage area for holding of to be destroyed material. The area should be large enough to accommodate all materials to be destroyed.

- e. A secure area devoted only to the destruction of the material. No non-secure activity can occur in this area.
 - f. A monitored security alarm system to secure building when unoccupied.
 - g. A security system checklist with monthly records of checking for operational integrity of the system.
3. Destruction process
- a. Inspection of equipment used for destruction. Is it adequate for the job?
 - b. Inspection of destroyed material and control of material after destruction.
 - c. Inspection of destruction area. Is it clean and orderly? Are the jobs batched or handled separately?
 - d. What quality control processes do they use to assure destruction?
4. Endorsements:
- a. Certificate of destruction includes destruction method, date of destruction and materials destroyed by serial number if appropriate or weight or count.
 - b. Certificate of proper disposal includes environmental compliance and/or certification of responsible disposal methods. (A number of states require that electronics i.e. hard drives, PDAs, cell phones be processed by a state licensed facility and mobile shredding of electronics may not be a permitted activity. Be sure to know your state's environmental regulations for the processing of electronics and that your vendor has the required certifications)
 - c. Does the vendor retain project records and for how long? Are they readily accessible?
5. Vendor Assurances:
- a. The vendor has a valid business license.
 - b. The vendor can provide certificates of insurance showing general liability insurance of at least \$2,000,000, the State required workmen's compensation insurance and professional liability insurance.

Transportation issues.

The physical control of a record or media containing records during the destruction process is a major security consideration. A third party service provider may provide you with the options of onsite destruction or plant-based destruction. In some cases onsite destruction may not be physically or financially reasonable. You will need to transport your media to a remote facility.

All media should be segregated, inventoried and isolated in a manner that reasonably minimizes the chance of unauthorized access and diversion of the media from the destruction process both at your facility and during transportation. The use of secure lockable containers is a recommended control practice. When possible, serial number

inventory records of accumulated data storage devices should be maintained for audit trail purposes.

When considering offsite transportation options, keep in mind the following:

The vast majority of security breaches are internal breaches where individuals know what the information is they are looking for and where it can be found. Outside transportation breaches are typically accidental losses and the major risk is that someone will find the media and try to reuse it. If the media or device is cleared, purged or physically damaged in such a manner as to make the device or media unusable, the principal risk is eliminated. The likelihood of someone accidentally finding a storage device and applying sophisticated (and very expensive) forensic data recovery techniques is extremely remote. Therefore, utilizing a technique to disable a device prior to offsite shipment is a recommended practice.

Transportation Options

- UPS/FEDEX with online tracking
- Bonded Courier
- Vendor provided bonded transportation
- Armored Courier
- Internal employee delivery and witness

Utilizing a secure container and maintaining tight audit trails while shipping UPS or Fedex would be adequate to show reasonable efforts to protect sensitive information required under government regulations. The higher security levels of transportation provide evidence of extraordinary precautions

Summary and Conclusion:

Records management has historically been focused on the management of paper records. We have developed good physical controls for the destruction of paper records and a large paper shredding industry has evolved providing an efficient and inexpensive service. But despite astonishing advancements in data storage technology and equally important changes in privacy regulations and the rules of litigation discovery, many organizations continue to use fragmented and outdated electronic destruction procedures - developed years ago. Electronic records systems demand the same attention to efficient records destruction procedures as you have developed for paper records. We hope that the information provided you today might help you in formulating an updated electronic data destruction policy for your firm. (END)

NIST GUIDELINES FOR MEDIA SANITIZATION

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
Purge	<p>Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging.</p> <p>Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36]</p>
Destroy	<p>There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.</p> <ul style="list-style-type: none"> • <i>Disintegration, Pulverization, Melting, and Incineration.</i> These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • <i>Shredding.</i> Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. <p>Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²).</p>

Media Type	Clear	Purge	Physical Destruction
ATA Hard Drives	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	<ol style="list-style-type: none"> 1. Purge using Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** 3. Purge media by using agency-approved and validated purge technologies/tools. <p>**Degaussing any current generation hard disk will render the drive permanently unusable.</p>	<ul style="list-style-type: none"> • Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	<ol style="list-style-type: none"> 1. Purge using Secure Erase The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** 3. Purge media by using agency-approved and validated purge technologies/tools. <p>**Degaussing any current generation hard disk will render the drive permanently unusable.</p>	<ul style="list-style-type: none"> • Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
Zip Disks	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	<p>Degauss using a NSA/CSS-approved degausser.</p> <p>**Degaussing any current generation zip disks will render the disk permanently unusable.</p>	<ul style="list-style-type: none"> • Incinerate disks and diskettes by burning the zip disks in a licensed incinerator. • Shred.

Media Type	Clear	Purge	Physical Destruction
SCSI Drives	<p>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</p>	<p>Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand. ***Degaussing any current generation hard disk will render the drive permanently unusable.</p>	<ul style="list-style-type: none"> • Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
Magnetic Tapes			
Reel and Cassette Format Magnetic Tapes	<p>Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.</p> <p>Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.</p>	<p>Degauss using an NSA/CSS-approved degausser.</p> <p>Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape.</p>	<ul style="list-style-type: none"> • Incinerate by burning the tapes in a licensed incinerator. • Shred. • Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a destruction facility or for recycling measures.
Cell Phones	<p>Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings.</p> <p>** Please contact the manufacturer for proper sanitization procedure.</p>	<p>Same as Clear.</p>	<ul style="list-style-type: none"> • Shred. • Disintegrate. • Pulverize. • Incinerate by burning cell phones in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
Personal Digital Assistant (PDA) (Palm, PocketPC, other)	Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	<ul style="list-style-type: none"> • Incinerate PDAs by burning the PDAs in a licensed incinerator. • Shred. • Pulverize.
Networking Devices			
Routers (home, home office, enterprise)	Perform a full manufacturer's reset to reset the router back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	<ul style="list-style-type: none"> • Shred. • Disintegrate. • Pulverize. • Incinerate. Incinerate routers by burning the routers in a licensed incinerator.
Equipment			
Copy Machines	Perform a full manufacturer's reset to reset the copy machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	<ul style="list-style-type: none"> • Shred. • Disintegrate. • Pulverize. • Incinerate. Incinerate copy machines by burning the copy machines in a licensed incinerator.
Fax Machines	Perform a full manufacturer's reset to reset the fax machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedures.	Same as Clear.	<ul style="list-style-type: none"> • Shred. • Disintegrate. • Pulverize. • Incinerate. Incinerate fax machines by burning the fax machines in a licensed incinerator.
Magnetic Disks			
Floppies	Overwrite media by using agency-approved software and validate the overwritten data.	Degauss in a NSA/CSS-approved degausser.	<ul style="list-style-type: none"> • Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator. • Shred.
Optical Disks			

Media Type	Clear	Purge	Physical Destruction
CDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations:</p> <ul style="list-style-type: none"> • Removing the Information bearing layers of CD media using a commercial optical disk grinding device. • Incinerate optical disk media (reduce to ash) using a licensed facility. • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). ** <p>** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm².</p>
DVDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations:</p> <ul style="list-style-type: none"> • Removing the Information bearing layers of DVD media using a commercial optical disk grinding device. • Incinerate optical disk media (reduce to ash) using a licensed facility. • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). ** <p>** This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm².</p>