

Getting Rid of Backup Media: What's Your Destruction Plan?



September 2008

Table of Contents



Executive Summary **page 3**

Understanding Media Destruction **page 3**

How Do I Get Started? **page 5**

Can't I Do This In-House? **page 9**

Conclusions **page 10**

Getting Rid of Backup Media: What's Your Destruction Plan?

Data security concerns have been making headlines more than ever before. Physical security breaches, database hackers, backup tapes falling off of trucks, outdated hard drives and other backup media finding its way from forgotten storage units into more and more courtrooms... there is no shortage of electronic records in the spotlight in the wake of an increasingly technological age. More organizations now understand the benefits of implementing proactive strategies for storing electronic data through the use of archiving solutions, retention plans, and routine good-faith operation of electronic systems to combat the apparent difficulties associated with managing electronic data. However, there remains a wide gap between what most organizations have implemented and what still needs to be done before their house is in order.

Executive Summary

Of course, while most firms do not intend to keep all backup media forever, many end up in this situation because of a general lack of knowledge about the data on the media and fears of data spoliation claims. If your organization is like most, you will find that backup media – typically in the form of tapes – has been the method of choice for storing the bulk of older records. Not surprisingly, gaining a full understanding of what these mountains of backup tapes contain can be a daunting task and creates a conundrum: Getting rid of too much media without taking into account operational, legal, and regulatory requirements can pose significant legal and financial risks, while storing old tapes and hard drives indefinitely opens the door to substantial room for increased legal exposure.

Fortunately, there are practical ways of managing inventories of backup media that meet specific business- or regulation-driven guidelines for deletion. Specifically, comprehensive media destruction plans are a cost-effective and practical method of eliminating electronic data that an organization has no legal responsibility to keep. This paper discusses the prevailing motivation behind media destruction efforts, how to effectively plan the destruction process, best practices for media

elimination, and why you should trust electronic data experts to carry out your plan once you have identified media that can be safely destroyed.

Understanding Media Destruction

Since the amendments to the Federal Rules of Civil Procedure (FRCP) were put into place in December 2006, enterprises in the US have become more aware of the legal risks associated with mis-handling electronically stored information (ESI) found in lost or forgotten inventories of storage media. “Storage media” includes a wide variety of backup tapes, hard drives, and other types of removable storage devices used to house electronic data. Mitigating the risks associated with storing large volumes of backup media and reducing the accompanying storage costs are the primary reasons organizations seek out media destruction solutions.

“Media destruction” entails the physical eradication of backup media used to store electronic information. Destruction of media is accomplished through disintegration, incineration, pulverization, shredding, and melting. The National Institute of Standards and Technology (NIST) has published a set of guidelines for “media sanitization” and the various methods of

Getting Rid of Backup Media: What's Your Destruction Plan?

destruction.¹ A formal “Media Destruction Order” (MDO) can be issued by the Court as requirement for a particular case after litigation has ended, but in general, media destruction takes place in a proactive manner before litigation is a driving factor.

Primary Driving Forces

As indicated, there are several reasons businesses and other organizations take on media elimination practices. Primarily, enterprises are seeking to address the risk of legal exposure hiding in old backup media in storage, comply with regulatory requirements, and manage the storage costs associated with large inventories of electronic media.

For most organizations, backup media is typically created and managed within the IT department. As these inventories grow, so do the costs of managing them. Because IT budgets are relatively fixed, this group must redirect funds to effectively manage these inventories of tapes that provide no direct benefit to them. Formal media destruction practices help IT departments directly reduce the amount of money they spend on backup media, while allowing them to better manage the hardware and other resources surrounding older inventories of data.

For organizations in heavily regulated industries, such as the financial and health care sectors, regulatory requirements dictate a host of confidentiality and privacy issues. These guidelines carry substantial financial, criminal, and civil consequences for non-compliance. Listed below are some of the most recognized regulations for which non-compliance can carry weighty consequences, alongside the types of organizations most susceptible to them.

What You Don't Know Could Hurt You

Uncertainty about media content and fear of sanctions if data is wrongly deleted have resulted in “keep everything” retention policies. To address this uncertainty of what records can be safely deleted, in conjunction with the related dormant liability associated with doing so, General Counsels, IT departments, and internal legal teams have a vested interest in media destruction practices. “Dormant liability” refers to the unknown, potential legal liability -- measured in dollars -- which the data on the storage media may unnecessarily cost the corporation during litigation.² Eliminating media an organization has no legal responsibility to maintain instantly and dramatically reduces dormant liability by getting rid of data that is not subject to any legal hold or retention requirements.

Sarbanes-Oxley Act (SOX)

Health Insurance Portability & Accountability Act (HIPAA)

Fair & Accurate Credit Transaction Act (FACTA)

Gramm-Leach-Bliley Act (GLBA)

California Senate Bill 1386

All public companies

Healthcare-related enterprises

Financial institutions

Financial institutions

Organizations conducting business in California

Getting Rid of Backup Media: What’s Your Destruction Plan?

Consider the following situation: Depending on your organization’s designated backup strategies that are in place and whether the data resides only on storage media, you could end up in a situation where multiple, overlapping legal holds ³ eventually bring your backup tape rotation plan to a standstill – resulting in a mounting inventory of electronic data on piles and piles of backup media. The problem is compounded when a particular legal hold may only relate to a few documents on a given piece of media, yet your organization must preserve the entire tape... which can be millions of documents. Those millions of documents are now considered “evidence” that is potentially discoverable as part of a completely unrelated matter.

How Do I Get Started?

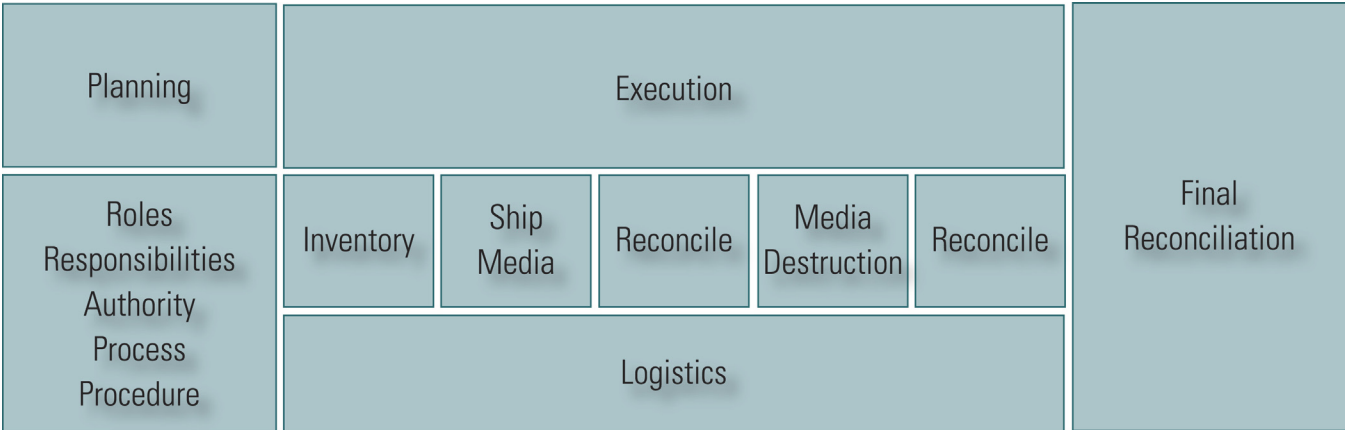
Once your organization has completed due diligence to determine what risks are most at play for your inventories of backup media, you need to act quickly and methodically to develop a plan of action to combat those risks. A meticulous media destruction plan can provide the details you need to take on this complex challenge.

Any well-managed project begins with a thorough plan. This means a clear understanding of deliverables, universal agreement of the desired end result, and contingency scenarios for a deviation from the original plan. It is absolutely critical that all members of the team – as well as all applicable stakeholders – understand and agree to every section of the plan. If the deliverables or end result is not clearly understood, expect the media destruction project to stall or potentially fail.

Step 1: Create a Work Flow

The first step toward a safe, efficient, and thorough media destruction effort must include the development of a complete work flow. A solid work flow should include planning, step-by-step execution, and detailed reconciliation of the final deliverables.

The work flow diagram below details the order of steps that should be carried out during the implementation of a sound media destruction plan, with each ensuing step discussed in greater detail later in this section.



Example Work Flow for a Solid Media Destruction Plan

Getting Rid of Backup Media: What's Your Destruction Plan?

Step 2: Determine Your Budget

Once the initial work flow has been developed, you will need to discuss budget allocation to identify who is paying for what. How organizations manage media destruction expenditures can vary widely, so your organization will need to determine – as early as possible – the amount and types of resources needed to carry out your media destruction efforts.

Reminder: *The number one cause for media destruction projects to run over budget is poor planning and failure to meet expectations that were set at the beginning of the project.*

Step 3: Set Up the Core Project Team

For a project of this importance, you should designate core team members immediately. These are the major stakeholders and the decision makers. Many departments will have a stake in media destruction activities, and it is a good idea to have a representative from each of the major departments to serve as members of the core team.

Some of the usual members of core departments typically include:

- Office of General Counsel
- Office of CEO
- Office of CIO
- Office of CFO
- Document Management Department
- Compliance Department

Reminder: *While you are forming your core project team, develop well-defined rules for each party to govern the media destruction activities as they move forward and become more complicated.*

Step 4: Develop a Plan

Before moving forward at this point, examine your media destruction plan to make sure it answers one fundamental question:

What media is going to be destroyed and how is it flagged for destruction?

A strict set of criteria must be developed to label a piece of media for destruction. At a minimum, the criteria for media elimination should include:

- Type of media
- Type of data
- Age of media
- Age of data
- Media location

Reminder: *Selection of media destruction must be exact. Before media can be flagged for destruction, it must meet all of the designated criteria without compromise. Questionable media, by default, must not be flagged for destruction.*

Consider the following factors as you develop your organization's media destruction plan:

- What types of media am I going to include in this destruction order?
- Who is authorized to issue a destruction order?
- How will exceptions be handled?
- For unknown situations, what is the process to resolve issues?
- Who within the organization is going to serve as the project manager?
- What reports are required?
- How exactly is the media going to be destroyed?
- What verification will I receive stating the media was destroyed?

Getting Rid of Backup Media: What's Your Destruction Plan?

Reminder: *It is important to be realistic when requesting reports. Many times, over-reporting causes more problems with a project than the reverse. At the beginning of a project, take a look at the reports available to you and then decide which information is truly critical, who needs to receive reports, and when they really need them.*

Step 5: Media Inventory

When conducting an inventory, it is best to have a standard form for collecting information. Basic information that should be collected during the inventory process should contain:

- Media make
- Media model
- Manufacturer's serial number (from manufacturer)
- Corporation-assigned serial number (if available)
- Any writings or markings on media (and/or on the external case, if available)
- Location of media
(i.e. XYZ Corp, building 101, room 15)
- Notation of any and all physical damage
- Time and date the inventory was taken
- Name and title of person conducting the inventory

Step 6: Packing and Shipping

Shipping arrangements should be made following your inventory. Generally, it is not recommended that companies pack and ship their own media, as backup media is fragile and susceptible to damage that can occur during shipping.

There are several shipping methods available, and you must decide which method meets your organization's needs.

Reminder: *Many vendors will provide shipping and shipping management services. This can be very helpful with large shipments or multiple locations, because it takes the pressure off of your organization's project manager. Each time a shipment is received by your vendor, an inventory should be conducted and verified off the master inventory. Any inventory discrepancies should be addressed immediately, and that part of the project should not continue until all issues are resolved.*

US Postal Service	Reliable service, low cost, limited security, slow delivery
FedEx or UPS Overnight	Reliable service, medium cost, slightly higher security than above, tracking mechanisms available, fast delivery
FedEx Custom Critical	Point-to-point shipping, only your media, very secure, detailed tracking mechanisms available, relatively expensive
Cargo Shipping	Medium cost, must be registered with airline, low security, specific security issues with non-direct flights
Do-it-Yourself Shipping	Medium cost, low security, time consuming

Getting Rid of Backup Media: What's Your Destruction Plan?

Step 7: Media Destruction

The method of destruction best suited for your organization will be based primarily on your security needs. There are essentially two types of media destruction:

- **Logical destruction** – Data is removed from media in such a way that the media is not destroyed while the data on it is forensically removed. Examples of this method include deleting files from media, re-formatting media, or over-writing media
- **Physical destruction** – Media is shredded and destroyed, allowing for no discrepancies or ability to re-use the media in the future. Destruction of media is accomplished through disintegration, incineration, pulverization, shredding, and melting.

It is recommended that a media destruction plan have at least three controlled steps before the media is actually destroyed.

1. The first step involves flagging a piece of media for destruction. The media must meet all of the criteria set forth by your organization's defined media destruction guidelines, leaving absolutely no room for error or interpretation. There cannot be any confusion on this point. If there are four criteria needed for destruction, then all four criteria must be present.
2. Once the first step is agreed upon by all necessary parties, the second step is to designate a destruction date and time, and create a Media Destruction Order for each piece of media. A cover page can list all of the pieces to be destroyed, but each piece should have its own

certificate. All documentation surrounding the initial identification of a piece of media for destruction should be numbered, logged, and controlled.

3. Once the second step is completed, the third step is the actual destruction. It is a good idea for a verbal "go" for media elimination to happen a few hours before the destruction. All communication should be logged and submitted with the completed destruction paperwork.

Following the destruction process, you should receive a master list of all pieces that were destroyed, as well as individual destruction certificates. Make sure each certificate is signed by the technician performing the destruction and by an Executive of the organization.

Many vendors can record the destruction of media and make it part of the official record. While the certification process can add cost to your media destruction project, it should be considered depending on the nature of the media being eliminated. For particularly outdated or sensitive media, it may be a good idea to have a mock destruction review prior to the start of the project.

Step 8: Reconciliation

Once the physical media destruction is complete, all documentation created during the process should be reconciled with your vendor and should be done in person whenever possible. The goal is to ensure each party has matching paperwork and that any and all discrepancies during the project were properly corrected.

Getting Rid of Backup Media: What's Your Destruction Plan?

Can't I Do This In-House?

Media destruction is a complex and time-consuming activity. No matter which option for eradication is chosen, meticulous care must be taken to ensure the operation is executed in a manner that leaves no doubt about the results. Because this is not a standard operation for most organizations, selection of a professional services organization that is capable of performing these sensitive procedures is highly advisable. Engaging trusted experts to carry out the destruction process can make media and data elimination a background task that is transparent to the daily operation of your enterprise, rather than attempting to develop the skills and tools to manage the process internally.

Who Can Best Help?

The best approach to safely and securely destroying media is to outsource to a trusted third party. When selecting such a service provider, pay careful attention to a firm's capabilities, background, and expertise. Taking proper time for due diligence will allow you to enjoy a more efficient and cost-effective media elimination process, while ensuring the defensibility of your methods as well as your data.

In general, you want to engage a service provider who is established in the market and has a solid history of handling electronic data and the many types of media on which it is stored. Additionally, always ask for references who echo the magnitude and complexity of your particular media destruction project. Generally, submitting a Request For Proposal (RFP) to evaluate a potential vendor's capabilities is one of the most thorough methods for determining whether or not a particular vendor will provide a good fit for your needs.

When seeking out vendors, look for one with a solid project management team that understands your problem and communicates effectively. Proactive communication through daily or weekly status reports is a bare minimum.

Choose a Vendor Who Can:

- Provide recommendations on the best options to employ
- Perform various media destruction/data elimination processes that are best suited for your specific needs and requirements
- Offers the highest of physical security at their facilities
- Manage the entire process with detailed chain-of-custody (CoC) logs that accounts for each piece of media at every step
- Offer custom-critical, secure transportation when necessary
- Maintain legal defensibility through a regimented CoC processes throughout
- Provide expert witness testimony
- Offer dedicated Project Managers
- Provide references earned from previous, relevant experience

Conclusions

As has been demonstrated many times over, inventories of backup media remain the unwitting provider of data security concerns. To address the myriad risks and escalating costs associated with storing electronic data on removable media, consider the recommendations offered in this paper. By becoming aware of the inventories of information at risk, you will be able to identify portions of those inventories that can and should be targeted for media destruction.

Most importantly, your approach to data elimination from backup media must be strictly regimented, documented, and reconciled. Creating a solid workflow and planning each step in painstaking detail can dramatically save your organization from heightened legal exposure and potentially save you from becoming another statistic in the legal community. Start planning now and seek out experts who can offer you peace of mind for your corporation's most critical data.

References

- ¹ The full report on media sanitation guidelines from NIST can be found at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
- ² To learn how much risk your organization is assuming by storing old backup media, insert your own quantities into the Media Storage Calculator that can be found at <http://www.renewdata.com/risk-calc.php>
- ³ For more information on legal holds as a function of the eDiscovery process, see The Sedona Conference's Commentary on Legal Holds, found at http://www.thesedonaconference.org/content/miscFiles/Legal_holds.pdf

About RenewData

RenewData is a leading provider of eDiscovery and ESI Risk Management (ESIRM™) services to assist corporations and law firms responding to lawsuits, investigations, and audits. Superior legal expertise, scalable technology, and a state-of-the-art facility featuring government-level physical security enable RenewData to provide clients with secure, accessible, and manageable data in a cost-effective and timely manner.

To help organizations understand and address the risks associated with storing large volumes of backup tapes, RenewData has developed Backup Tape Liability Management (BTLM™) services within the ESIRM product suite. BTLM services enable enterprises to know what type of data exists and where it resides, allowing for the potential elimination of large amounts of data while increasing an organization's ability to mitigate the legal exposure hiding within large inventories of backup media.

RenewData's BTLM services encompass several steps corporations can take toward better management of backup tape inventories, including:

- Comprehensive physical media audit
- Secure shipping services
- Legally defensible Chain-of-Custody (CoC) services
- Detailed container classification
- Data separation and de-duplication
- Certifiable media destruction services

RenewData helps organizations proactively plan for and manage electronic data in advance of the inevitable eDiscovery order, while helping reduce the costs and time demands associated with legal productions. Proactive ESIRM services provide a cost-effective solution for the management of risks associated with electronic data before, during, and after litigation.

RenewData has been ranked a "Top Provider" in the Socha-Gelbmann Electronic Discovery Survey Report for four consecutive years and was also ranked in the 2006, 2007, and 2008 Inc. Magazine lists of fastest-growing privately-held companies in the U.S. For more information, visit www.renewdata.com or call 888.811.3789.



512.276.5500
888.811.3789

www.renewdata.com

Copyright © 2008 Renew Data Corp. All rights reserved. RenewData and ActiveVault are registered trademarks and ESIRM and "Single-Pass Processing" are trademarks of Renew Data Corp. RenewData disclaims any proprietary interest in the marks and names of others.