



Recycling?

Managing Data Security Risks – A Practical Guide

Recycling your IT equipment? Sure. The vast majority of organizations understand that recycling IT equipment is essential to minimize corporate environmental risk. But what about the data on that equipment?

The facts and headlines regarding secure data breaches are all too commonplace:

- In the first 10 months of 2005, personal information of over 50 million Americans is exposed.
- About ½ of these are due to company employees either accidentally or maliciously exposing confidential data.
- An intruder obtains names, account numbers and verification codes (yes, those “highly secure verification” codes everyone asks for now) for 40 million credit card holders prompting a class action lawsuit and sale of the company.
- An internet company pays \$1.8 million in plaintiff’s cost in a class action suit and \$450,000 in fines for consumer privacy breaches.
- Healthcare company fined \$200,000 for patient data breach

Sarbanes Oxley, Health Information Portability and Accountability Act, Gramm-Leach Bliley Act

Who would have thought that the blessing of electronic technology in business would bring with it so much risk? After IT asset managers spent a decade focusing on minimizing risk by implementing environmentally responsible disposition programs, in 2005, the focus changed. Not slowly and surely over many years but suddenly, with a seismic shift. Thanks to privacy laws including SOX, HIPAA, GLBA and almost daily news stories exposing corporations failing to protect personal data, 2005 became the year when data security jumped to the top of the priority list for IT and Risk managers.

So how can IT asset and risk managers contain all this exposure? One of the answers is: by conducting due diligence for data security on all electronic asset disposition practices.

Recycling options and risks

Electronic asset disposition programs commonly include equipment resale, recycling and donations. All of these options can be viable if data security measures are audited and verified. Every risk manager must evaluate the level of potential exposure associated with different data security practices vs. the risk tolerance of the organization.

Data “erasure” or drive overwriting

This is the most commonly used method of securing data on drives intended for reuse or resale since the process imparts no damage to the drive.

- *How it works:* A series of zeros or random patterns are written on top of data in the drive, making it unreadable. Most electronics recyclers subscribe to the Department of Defense’s 5220.22-M overwrite standard that calls for overwriting the drive sectors three times with specific, different characters. Depending upon the sensitivity of data, the process is conducted more than once to assure data security, but time becomes a major factor in the cost/benefit of overwriting so that equipment can be reused.
- *Limitations:* Depending upon drive size, the process can take several hours to multiple days. Most recyclers have equipment enabling them to overwrite 100 or more drives at a time. But, time is money. With decreasing resale values, too much time in preparing equipment for resale becomes cost prohibitive.
- *When it doesn’t work:* Many drives contain faults in the drive platter that prevent overwriting. With the right technology and forensics tools, data and segments of the data residing in these areas can potentially be recovered.
- *How to assure you are protected:* When auditing your recycler, have them clearly demonstrate the drive overwrite process. Randomly request return of erased drives for evaluation of overwrite effectiveness. You may be unpleasantly surprised to find how often drives are either missed entirely or the overwrite is ineffective. Make sure you are getting the protection you are paying for!

Drive degaussing

Degaussing is much more secure than overwriting because data is actually eliminated rather than covered up. Degaussing destroys the functionality of the drive so it can no longer be used.

- *How it works:* Data on a hard drive is actually stored in a magnetic field that resides between the drive platter and a cobalt chromium plating on the platter. Degaussing reduces the magnetic field to a zero state which eliminates all the data stored in the field. The drive must be removed from the PC and placed in a degaussing unit one at a time. The process generally takes about one minute per drive.
- *Limitations:* Degaussers cost anywhere between \$15K and \$50K and only one drive can be degaussed at a time. Be ready to pay significantly more for this level of security.
- *When it doesn't work:* The amount of magnetic force applied by a degausser must be strong enough to negate the magnetic field in a given drive. The National Security Agency maintains a Degausser Products List that indicates the types of drives individual degaussers are capable of erasing. If you ship your recycler drives that their degausser is not rated for, data could remain on the disk. Additionally, improper placement of the disk in the degausser can render the process ineffective.
- *How to assure you are protected:* Get the model number for your recycler's degausser and check with the NSA's Degausser Products List at https://www.nsa.gov/ia/government/MDG/NSA_CSS-EPL-9-12A-B.pdf to be sure that the drives you will be sending can effectively be degaussed by that unit. Again, random checking of degaussed drives will assure you that your recycler is using the equipment properly.

Drive destruction

Common drive destruction techniques run the gamut of punching a hole in the drive with an awl or drill press, to mechanical shredding, to delamination.

- *How it works:* Punching, drilling or shredding a drive renders the drive unusable. A new process, referred to as delamination, goes beyond shredding by delaminating the cobalt chromium plating from the drive platter, effectively eliminating the magnetic field where the data resides.
- *Limitations:* These techniques certainly damage or destroy the drive to the degree that it can no longer be used but unless the process includes delamination, the data remains on the drive platter, or on pieces of the platter. With the right technology, data can be retrieved from drive particles as small as 19 microns.
- *When it doesn't work:* Highly motivated individuals with the right equipment can retrieve data from destroyed or shredded drives that have not been delaminated.
- *How to assure you are protected:* Find out just what your recycler means by "drive destruction". If delamination is not a part of the process, make sure that the destroyed drives are secure when they leave the recycler's facility, headed to their final destination for metals recovery. Or, require that your recycler send your drives for delamination and material recovery.





It's *not* just about the hard drives

Data forensics, or the science of recovering electronic data, no longer starts and ends with computer hard drives. Consider the following:

- Older **fax machines** have ink cartridges that leave an imprint of every document faxed
- **Printers** have memory devices that can be imaged
- **PDA's** and **cell phones** have memory devices that can be imaged and analyzed
- Portable media such as **zip disks, floppies, CDs, DVDs and flash cards** are obvious sources of data that can be easily analyzed and are many times haphazardly guarded.

What about protecting my data during transport?

If securing your data prior to transit is not practical or economical, there are a couple of options available. Some companies that traditionally provide on-site document shredding services have equipped their vehicles with drive shredders as well. Just remember that knowing where the shredded drives are destined and how they will ultimately be destroyed is part of your due diligence process.

Alternatively, drives housed in PCs can be locked out with encryption software prior to transit. This will entail loading the software onto every computer and providing your reseller/recycler with the pass code to bypass the lockout.

Either of these options involves technician time to either remove the drives for on-site shredding or load the software.

Trucks used for transportation to the recycler can also be sealed to prevent loss during transit. A metal or plastic tag that cannot be opened and reattached is applied to the rear access door and, upon arrival at the recycler, is cut off and mailed back to the shipper as evidence of safe arrival. The only economical drawback here is that companies with smaller quantities can not take advantage of less-than-truckload freight rates since, once sealed, the trailer cannot be opened to share freight.

The bottom line:

Most IT asset and risk managers have learned that the only way to assure their recycler is providing environmentally responsible recycling is to conduct a comprehensive audit including downstream vendors. Now, auditing the recycler's data security processes is equally important toward protecting the organization from liability. To help determine which data destruction techniques are right for your company, answer the following questions:

1. **How sensitive is my data?**
2. **What is the residual value of my equipment?**
3. **What will it cost to make data on the equipment secure?**
4. **After I pay to secure the data, is there enough residual value left to justify some level of risk associated with reuse?**
5. **If the rewards of resale or reuse are marginal, is destruction more economical and more secure?**
6. **Should I be destroying printers, faxes, cell phones and other units that also store data?**
7. **Have I properly audited my recycler's data security practices to assure they are effective?**
8. **Have I randomly tested the effectiveness of my recycler's process?**
9. **Who in my organization is minding the data?**

Lauren Roman is Executive Vice President at MaSer Corporation, Michael Magliaro is Executive Vice President of LifeCycle Partners and Judy Gosselin is CEO of JAG and Company Investigations

