



## The Data Destruction Dilemma

How to Destroy Hard Drive Data Without Destroying System Value

### EXECUTIVE SUMMARY

At the same time that the number of computer systems being retired is growing into the hundreds of millions, the need to protect the sensitive data in those systems is also growing dramatically. Gartner estimates that from 2006 through 2010, consumers and businesses will replace more than 925 million PCs worldwide (Gartner IT & Software Asset Management Summit 2006). And the Identity Theft Resource Center is reporting about 10 million cases of identity theft per year (idtheftcenter.org). Given that computers are repositories for financial records, medical records, personal correspondence, legal documents, digital images, Internet usage history, and other confidential information, the importance of destroying hard-drive data when systems are retired cannot be overstated.

These statistics about computer asset retirement and identity may be new to you, but they are likely not surprising. Anyone in business today understands firsthand the importance of keeping technology current in order to operate efficiently and effectively. And anyone who reads a newspaper or watches the news understands how easily sensitive data can be compromised and how disastrous the consequences can be. A recent article in *Information Security News* (05/04/2006) quoted another Gartner study as indicating that nearly 80 percent of companies surveyed indicated that “managing data security and privacy risks were very important or most important when disposing of obsolete hardware.” More tellingly, perhaps, the story went on to point out that the same study also found that nearly one-third admitted to having no policy in place at all for the security of used equipment.

There's little doubt that people know *why* they need to protect the data in their old computer systems. The problem is that they may not know *how*. Worse yet, they may *think* they do—and pay a high price for being wrong.

This paper will examine:

- the factors driving the need to retire computer assets without compromising the security and privacy of the data on them
- the options available for disposal of computer equipment and the relative risk they pose to data security
- the need to make sound strategic decisions about systems retirement and data destruction, and the criteria for making such decisions

You absolutely can control the data security risk associated with retiring computer assets. But it requires a clear understanding of all the available options and how to assess them. Only then can you make sound security *and* business decisions about them.

# Identity Theft and Regulatory Risks: Driving Data Destruction

Two recent phenomena in particular are making organizations acutely aware of the need to destroy sensitive data on computer assets that are being retired. The first is the risk that sensitive data on computer systems could fall into the wrong hands, and the second is the increasing likelihood that taking steps to guard against such a disaster is mandated by law.

## DATA AT RISK:

### Coping with Hardware Vulnerabilities

The last several years have been rife with hair-raising examples of sensitive computer data being put at risk. Here are just a few.

- Early in 2006, dozens of backup tapes containing medical information on thousands of people, including their HIV status, were sold at a government auction in British Columbia (*Globe and Mail*, 01/19/2007).
- A major U.S.-based transportation-equipment manufacturer has had laptops with sensitive employee information on them stolen three times since 2005 (SearchSecurity.com, 12/13/2006).
- Every federal government department or agency in the U.S. has reported at least one loss of personally identifiable information since 2003 (idtheftcenter.org).

Like many data losses, these were not the result of someone hacking into a computer system. They happened because organizations failed to protect their hardware from data security breaches. This underscores the importance of securing the physical assets where data resides, and not just focusing on the firewalls and anti-virus programs that secure the networks through which data travels.

## GLB, HIPAA, SOX:

### Complying to the Letter

Today, protecting sensitive data from security breaches isn't just a good business practice; in many cases, it's the law. Today, there are dozens of local, federal, and international laws aimed at keeping private data private. And violating them can cost a company plenty.

- NORPDA, or the Notification of Risk to Personal Data Act, requires U.S. businesses and government organizations to notify customers of

network security breaches that could cause personal data to be disclosed. *Penalty for noncompliance: \$5,000 per violation or up to \$25,000 per day.*

- HIPAA, or the Health Insurance Portability and Accountability Act, protects personal healthcare information such as medical records. *Penalty for noncompliance: Fines of up to \$250,000 and jail sentences of up to ten years.*
- GLB, or the Gramm-Leach-Bliley Act, requires companies in the financial industry to protect personal financial data such as social security numbers and account numbers. *Penalty for noncompliance: Regulatory fines and the prospect of personal liability for CEOs and board members.*
- California Senate Bill 1386 protects residents of California from having any confidential information about them disclosed by any organization doing business with them – even if the organization is not physically located in California. *Penalty for noncompliance: Fines determined on a case-by-case basis.*
- PIPEDA, which is Canada's Personal Information Protection and Electronic Documents Act, protects personal information collected about Canadian residents. *Penalty for noncompliance: \$10,000 to \$100,000 for failing to respond or for destroying records.*
- Data Protection Act is a British law governing the protection of data about individuals in the UK. *Penalty for noncompliance: A fine of up to £50,000.*

The most well-publicized examples of failures to protect data under laws such as these seem to involve computers that have been lost or stolen, or firewalls that have been breached. But they apply equally to computers that have been retired from service. If you fail to remove all the relevant data from a system that is being retired, you are in violation of laws like these.

# Recovering Value, Minimizing Risk: Striking a Balance

The data destruction dilemma goes beyond the challenge of ensuring that sensitive data is no longer accessible to anyone. If it were that simple, organizations could just routinely take a hammer to their old systems and smash them—and the data in them—to bits. After all, according to some, “the only way to truly erase a hard drive is to grind it up into tiny pieces or riddle it with bullets,” as writer Charlie Russo has reported (“Disposing of IT assets the right way,” SearchCIO.com, 06/22/2005).

But the need to ensure that data is destroyed almost always coexists with a desire to recover the value that remains in systems that are being retired. New computers tend to be retired after about four or five years, according to methodologies used by the *Computer Industry Almanac* to calculate PC replacement rates ([www.c-i-a.com](http://www.c-i-a.com)). Computers of that age are far from worthless. They may no longer be right for the organization that has been using them—their processing speeds or memory capacities may no longer be sufficient, for example—but they still have value.

## THE RISK / VALUE CONTINUUM

The challenge in retiring computer assets is to reduce the data security risk as much as possible while still retaining as much asset value as possible. Risk and value exist on a relative continuum. The accompanying chart describes the various methods of dealing with retired hard drives in terms of their relative effects on data security and recovery value. The chart illustrates how the various methods may be appropriate for a range of types of systems based on the type of information they contain, such as:

- **Typical Home System:** tax returns, digital photographs, correspondence, Internet history. Typically, the risk of inadvertent disclosure of this type of information is limited to the individual owner of the PC.
- **Typical Business System:** client lists and information, financial records, social security numbers, business plans. The risk of inadvertent disclosure of this type of information is significantly greater than for a home PC, and may extend to the entire organization, as well as beyond the organization to people like clients or patients.
- **Critically Sensitive Systems:** national security information and other classified documents. Inadvertent disclosure of this information can lead to catastrophic consequences.

Keep in mind, too, that servers, desktops, and notebook computers are not the only assets that present data security risks. The same awareness about risk should be present when retiring other assets such as external storage systems, various forms of media, and mobile devices such as PDAs and cell phones.

## DATA DESTRUCTION METHODOLOGY

**File Deletion:** Deleting files (using Windows Explorer, for example) does not reliably make a file unrecoverable. Deletion simply removes the file markers that allow an end user to overwrite that part of the drive; it does nothing to destroy the data. A person with basic computer knowledge, using readily available software utilities, can easily recover files that have been deleted.

**User-Conducted Disk Wipe:** Specialized software tools for wiping disk drives are commonly available. Such tools can be effective for simple configurations, but not every tool is effective with every hard drive technology. Additionally, wiping tools are not able to wipe bad sectors on drives, so any data on those sectors remains undestroyed. Without expertise in selecting the appropriate wiping tool for a given hard drive configuration, and without manual verification of a successful wipe, user-conducted wipes may not be fully effective.

**Three-Pass Professional Disk Wipe:** Experienced electronics asset recovery companies perform professional disk wiping. These companies process hundreds or thousands of drives per day, and have a suite of wiping tools to address practically any hard drive technology or condition. Redundant erasure is highly recommended to help ensure total erasure. Most recovery companies will utilize a three-pass wipe, which complies with the 5220.22M Department of Defense standard. The three-pass process requires first writing 0s over the entire drive, then writing 1s over the entire drive, and then writing a random sequence of 0s and 1s over the entire drive.

➤ **(Greater Than) Three-Pass Professional Disk Wipe:** Some electronics asset recovery companies will, at customer request, overwrite a drive in excess of the three times mandated by the DOD standard. This provides an extra measure of security for organizations operating in highly regulated industries, such as financial organizations or those working with classified customer information.

**Three-Pass Professional Disk Wipe with Manual Verification:**

Erasure tools all report when erasure is complete, but how do you know if it was successful? Very rarely, despite best efforts by an electronics asset recovery company, a process escape or an issue with a wiping tool will result in some data remaining on a processed hard drive. The best electronics asset recovery companies use a variety of diagnostic tools to visually inspect every single hard drive processed and manually verify that data wiping tools have successfully eradicated all data.

**Degaussing:** This process exposes a hard drive to extremely high levels of magnetic fields, completely eradicating the data. This process is gaining popularity in the marketplace for highly confidential information, but it renders the drive unusable and therefore completely valueless.

**Shredding:** Shredding is the act of physically destroying the hard drive by smashing and cutting it into pieces. Typically, shredding is performed after the magnetic bits on the disk have been eradicated by one of the other means suggested above.

**THE ELUSIVE (But Not Impossible) RISK/VALUE BALANCE**

Shredding a hard drive may indeed be the appropriate means of disposing of computer assets that contain information that could have truly devastating consequences if revealed. No asset worth \$100 or so is worth even a small risk of a multi-million-dollar lawsuit, for example. And no asset of any value is worth risking lives, as could be the case with a computer that contains highly classified government information.

Elsewhere along the risk / value continuum, however, is the potential for striking that very desirable balance between posing the least possible risk to the data and recovering the most possible value from the asset. This can be achieved by making informed decisions about how to dispose of assets—decisions based on the value of the data in them and the potential recovery value of the assets themselves.

Methodology	Effectiveness of data destruction	Percentage of resale value preserved	Typical unit cost	Applicability		
				Typical Home PC	Typical Business PC	Critically Sensitive PC
Nothing	0%	100%	\$0	Light Green	Light Yellow	Light Orange
File deletion	10%	100%	\$0	Light Green	Light Yellow	Light Orange
User-conducted disk wipe	50%	100%	\$2-4	Light Green	Light Yellow	Light Orange
Three-pass professional disk wipe	90%	100%	\$10-15	Light Green	Light Yellow	Light Orange
>Three-pass professional disk wipe	95%	100%	\$12-20	Light Green	Light Yellow	Light Orange
Professional disk wipe with manual verification	99+%	100%	\$15-20	Light Green	Light Yellow	Light Orange
Degaussing	100%	0%	\$2-6	Light Green	Light Yellow	Red
Shredding	100%	0%	\$1-2	Light Green	Light Yellow	Red

**DATA DESTRUCTION METHODOLOGY**

# The Pitfalls of a Do-It-Yourself Approach

The reformatting and user-conducted wiping methods described in the previous chapter can present a number of potential pitfalls.

- Formatting gives a false sense of security, in that it only moves the pointers to the data — but leaves the data itself on the drive.
- Selecting the right tool is not a trivial consideration, since certain types of disk drives require specialized wiping tools.
- Any bad sectors on the drive may still contain data, but these sectors may not be accessible to conventional wiping tools.
- Even professional tools are not 100% reliable. Having the tools and expertise to manually verify a successful wipe and record the results in a database (creating an audit trail) is the only way to confirm a successful wipe.
- There is no liability indemnification when you wipe a hard drive yourself. By contrast, electronics asset recovery companies assume liability for the data on the drives.

## PROOF THAT OLD PCS ARE PUTTING DATA AT RISK

Consider just a few real-world examples of the risks of reselling or donating computer assets without taking the proper precautions.

- Testing by a German technology firm of hard drives bought on eBay revealed that seven of every ten tested still bore readable information (CNET News.com, 04/24/2005).
- An investigation into computer equipment disposal in the UK discovered that only two of more than 100 hard drives from computers bought online, at computer fairs, or from traders contained no recoverable data — and one of those was brand-new. (*The Register*, 02/17/2005).
- In 2005, the city of San Antonio, Texas learned that one of its discarded computers had ended up in a garbage dump in Nigeria. At the time, the city typically sold its old computers on an Internet auction site (*San Antonio Express-News*, 02/12/07).

Chances are that the original owners of these systems never set out to put their data at risk. They probably never dreamed their systems would end up on the open market — much less end up on the market with data still remaining on the hard drives. But that's exactly what can happen.

## SIMPLE STEPS TOWARD PREVENTING DISASTER

The problem isn't that computer assets are being resold or donated; the problem is that they're being resold or donated without first being demonstrably stripped of their data. For that, it's best to rely on the expertise and resources of professionals with a demonstrated core competency in data security.

- No matter how you intend on disposing of computer assets, it's generally wise not to attempt to erase the hard drives yourself. There are many, many software programs available to wipe drives clean, and none of them can be expected to address all drives and file types. It takes special expertise in hard drive structures, file types, and wiping technologies to reliably wipe a drive.
- Don't always assume that just because you've wiped a drive, all the data has been erased from it. In some cases, the identifiers of or pointers to the data may be erased, while the data itself remains on the drive. Manual verification by a skilled technician is really the only way to be sure data has been completely erased.
- Instead of reselling or donating systems yourself, consider accepting an offer for them from a company specializing in data destruction — and let them resell or donate them on your behalf, or return them to you for donation. You'll find criteria for evaluating such companies in the remainder of this paper.
- Look for another way to recover value from your assets — by, for example, signing up for a trade-in program when you buy new computers. Virtually every major computer manufacturer today offers such a program.
- Be sure you have a serialized report of each asset you replace with a verifiable audit trail that proves erasure.

# Beyond the Hard Drive: The Hallmarks of Sound Data Destruction

Erasing data from the hard drive is an important aspect of asset disposal—but it's not the only one. The end-to-end process of successful data destruction involves everything from protecting the drive from physical tampering before the data is erased, to verifying that the process has been successful after the data has been erased, to creating a detailed report documenting the successful erasure. You must consider these and other issues in order to make sound strategic decisions about how best to erase the data on hard drives and to whom the job should be entrusted.

**Physical security.** Even if you are going to erase or destroy a hard drive, it's critical to take precautions against theft or other breaches of the data on it *before* the data is destroyed. Ask yourself these questions:

- Where are computer assets stored while awaiting disk erasure? Who has access to them?
- If computers are being taken to a remote location for processing, is there a chain-of-custody policy in place to protect their integrity on the way there and after their arrival?
- If a third party is handling the data destruction, is there video surveillance at its facility? Are background checks performed on the employees? Are incoming assets tracked by bar code so that their whereabouts are known at all times? Is the data destruction process transparent to you, the asset owner?

**Software expertise.** Because there are myriad choices of software programs for erasing data on hard drives, it takes deep expertise to evaluate their effectiveness and appropriateness for the task at hand. This is one of the main reasons that outsourcing data destruction to a specialized company is a good option. Keep the following points in mind:

- Experts in data destruction should be familiar with virtually every disk wiping program available, including knowing which ones work on the different types of assets in the product mix (servers, desktops, notebooks), which ones work best for systems from specific manufacturers, and which ones don't work well at all.
- Because good companies that specialize in data destruction recognize that some programs work better on some systems than others, they can make informed decisions to standardize on software that will work optimally in their product mix.
- A data destruction company that can make informed choices about software tools is more likely to be able to effectively erase data

on hard drives than a company that does not have the expertise to select the right software for the job.

**Adherence to the DoD standard.** The 5220.22M Department of Defense standard is the accepted standard for overwriting hard drives, as described on page 3. A data destruction company should provide redundant erasure that meets or exceeds this standard.

**Verification and follow-through.** Some companies that provide data destruction services believe that following the DoD standard of three passes on the hard drive is sufficient. But it's better to be able to confirm erasure and to be prepared to take additional steps as required. To that end, a company should offer the following services:

- Additional examination, either visual or mechanical, should be undertaken after wiping a drive to verify that no data remains on any sector of the drive—or, in rare cases, reveal that it actually does.
- Once it is verified that no data remains on a drive, the company should provide a certificate of destruction attesting to that fact, supported by a complete audit trail of the data erasure process.
- In the unlikely event that data does remain on any sector of a hard drive after it's been wiped, a provider of data destruction services should have the capability to effectively destroy the drive. The company should be specifically equipped to physically shred the drive or to perform degaussing, as described on page 4.

**Modularity and flexibility of services.** Not every company has the same data destruction needs. The company that you contract with to provide these services should offer a range of approaches to match your circumstances. One size does not fit all in the data destruction business.

- Overwriting should go beyond the accepted DoD three-pass standard when appropriate.
- Organizations whose data is of a particularly critical nature should be able to request a seven-pass approach if desired.
- Conversely, companies whose data is not particularly sensitive should be able to opt for fewer than three passes—even just one pass, if that is what is appropriate for them.
- A data destruction company should be able to handle not just computer components with internal hard drives, but also less commonly occurring assets such as SCSI drives, disk arrays, optical drives, and PDAs and other mobile devices.

**Integrity of operations.** Given the nature of the work, a company that offers data destruction as part of its services should offer the following specific services to assure you that their work is done with the highest integrity.

- The company's operations should be ISO 9000-certified to meet accepted standards for quality management of processes.
- The company should provide a detailed accounting of the entire process from receipt of assets through final disposition.
- The company should offer documented indemnification of your company in the event of a data breach that occurs on its watch.

Given the gravity of the consequences that can result if data is mishandled, it's extremely important to make the best possible decisions with regard to rendering data on the hard drive inaccessible once the asset is retired. This isn't easy, but the more information you have to work with, the more confident you can be of making the right choice.

## ABOUT TECHTURN

TechTurn is the trusted industry leader for technology recovery, refurbishing and remarketing. Through its world-class facilities and processes, TechTurn provides the foundation for sustainable technology, providing companies with an economically smart, environmentally friendly and risk-free method for the recycling and reselling of used technology. Since 1999, TechTurn has been the preferred take-back partner for 300 of the Fortune 500 and the top four computer manufacturers. These leading organizations provide TechTurn with a non-stop supply of high-quality, high-value technology systems and components that, after testing and certification, are remarketed to customers worldwide. By extending the life of these products, TechTurn is able to enrich the lives of millions of people worldwide while also helping to significantly reduce the amount of e-waste that is filling landfills and polluting the environment. For more information, visit [www.techturn.com](http://www.techturn.com).

# TechTurn™

©2007 TechTurn, Inc. All rights reserved. All other trademarks are property of their respective owners.