



Avoiding Self-Inflicted Security Breaches Through Effective Hard Drive Decommissioning

Inadequate Data Destruction Can Result in Lost Business, Reputation, Civil and Criminal Liability

Executive Summary

Every business has data that must be destroyed. According to a NAID report of a Conference Board survey, data security has become a primary concern for top executives. While hackers and viruses present a constant threat, a study by Gartner indicates that 90% of all security breaches were “self-inflicted.” In other words, these problems were avoidable if the company took the right steps.

One area that is often misunderstood, or completely overlooked, is hard drive decommissioning—the process of removing data from a drive prior to disposal or recycling. While there are several methodologies for eliminating data from hard drives, there are problems with each method. High costs, slow process times, uncertainty of the effectiveness of the method and questionable chain of custody must be considered before implementing a decommissioning strategy.

Failure to protect and destroy sensitive and confidential records and files will have catastrophic consequences to a business on numerous levels. Financial loss, irreparable damage to a company’s reputation, as well as civil and criminal liability for Directors and Officers can result from data that is accessed from hard drives that were not thoroughly sanitized.

It is critical that data on drives is destroyed beyond forensic recovery before disposal or redeployment of the drives. This paper will compare the current methodologies based on effectiveness, cost, time and other practical considerations. It will also review Ensconce Data Technology’s new Digital Shredder product that provides in-house sanitizing that successfully addresses all decommissioning concerns.

Table of Contents

Executive Summary	1
Data Destruction Reality Check - The Failures	3
When is Data Destruction Necessary?	3
Methods of Data Destruction	4
<i>Deleting</i>	4
<i>Software Overwriting</i>	4
<i>Degaussing</i>	5
<i>Mechanical Shredding</i>	6
<i>Secure Erase</i>	6
Ensconce Data Technology’s Digital Shredder	7
Consequences and Penalties for Non-Compliance	9
A Worst-Case Scenario	10
Conclusion	10
Contact Information	11
Appendix - Technical Discussion of Erasure Techniques	12
<i>Weak Erase</i>	12
<i>Block Erase</i>	12
<i>Secure Erase</i>	13
<i>Fast Erase</i>	13

Data Destruction Reality Check - The Failures

Simson Garfinkel conducted a study for part of his Ph.D. thesis on Computer Security at MIT's Computer Science and Artificial Intelligence Laboratory. He purchased 230 used hard drives from various sellers and discovered a remarkable amount of sensitive data that could have seriously harmed the original owners if it had fallen into the wrong hands. Garfinkel was able to access corporate trade secrets, financial records, personal medical records and credit card numbers by the thousands.

In the July 2006 issue of Smart Computing, it was reported that Symantec also examined used computers and found social security numbers, banking statements with account numbers and balances, confidential employee records, numerous corporate documents and emails.

Be advised that you don't have to be an IT professional to extract data from recycled hard drives. In 1997, The New York Times had two articles regarding a woman in Nevada who purchased a computer that had been used in a pharmacy. She found that the computer still contained the complete records of its customers, including both personal and medical information.

The message is clear from large corporations to small businesses. Potentially damaging data is not being properly eradicated from hard drives. It is essential that every business reevaluate their decommissioning strategy now to avoid failures and resulting penalties.

When is Data Destruction Necessary?

There are some obvious circumstances when the need for data decommissioning is required. Unfortunately, there are other cases that are often overlooked. An effective decommissioning strategy must be prepared for each of the following circumstances:

- When a user's computer is upgraded and the old machine is to be sold, donated, discarded or recycled.
- Whenever a drive is re-configured for existing or new users.
- Whenever equipment containing storage is returned to a manufacturer or VAR for warranty repair.
- As a method for ensuring that the offending code of an extreme virus attack or hacking attempt is completely removed from the infected storage device.
- When a hot spare was automatically placed into service, and then removed when the faulty RAID drive was replaced. In this case the hot spare should be erased, as well as the original failed RAID drive if the drive is still operational (replaced due to imminent failure).

Care, Custody and Control

Special attention must be given to this aspect when evaluating any decommissioning process. Any process that requires you to forfeit custody of your data should be considered circumspect from an auditing standpoint. It is important to remember the difference that digital data represents over other forms of data such as paper.

Paper data that is relinquished to a third party for shredding is rarely organized in a fashion that is useful to the third party, nor does the paper, itself, have any intrinsic value. However, handing someone a hard drive is equivalent to giving that person an organized data structure that is instantly usable. Although the monetary value of a single hard drive may be negligible, a person who is in a position to collect several drives per day, may be able to supplement their personal income by an amount that is substantial enough to tempt a sale to a third party.

Methods of Data Destruction

There are several hard drive decommissioning methods. It is important to understand the advantages and potential disadvantages of each. The primary concerns are effectiveness, time, ease of deployment and cost. More importantly, care, custody and control are considerations that cannot be taken lightly when selecting a methodology for decommissioning hard drives.

Deleting

This is the most common method used to try to delete data from hard drives. The primary problem is that deleting is not destroying. Executing the basic delete function on your computer only removes the file system's pointer to that file, not the file itself. All of the data remains on the hard drive and can be easily recovered with simple software tools.

Software Overwriting

The U.S. Department of Defense defines overwriting as "a software procedure that replaces the data previously stored on magnetic storage media with a predefined set of meaningless data." Currently, the DoD requires three levels of overwriting. It warns that there can be problems with "ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), or inability to overwrite bad sectors or tracks of information in inter-record gaps." (U.S. Dept. of Defense Standard 5220.22-M)

Many software overwriting programs are available. The procedure can be done in-house and it assures that the hard drive is not being exposed to an unsecured environment. Furthermore, overwritten hard drives are reusable. This can have material financial benefits.

As for the shortcomings, the overwriting process itself is time consuming. It can take many hours or even days to complete depending on the size of the hard drive. This creates a substantial loss in productivity in a large enterprise that may have hundreds of computers to decommission and redeploy.

Overwriting requires the user to install and run the software, create a boot floppy, then engage in the lengthy procedure that must circumvent the higher-level operating system. According to Robert Varmosi, Senior Editor of CNET Review, “the process is mind-numbing and subject to human error.” He also points out, “there is no way to easily visually check that the erasure has successfully occurred.” In addition, these software overwriting programs leave “evidence that erasure has occurred, which may possibly cause a legal discovery problem.” (CNET Review, June 10, 2005)

Expense is also a concern. The software requires a separate licensing fee for each hard drive to be overwritten.

Software overwriting can be a complementary methodology in a comprehensive decommissioning strategy. However, it is not foolproof and is prone to mistakes by the user. As noted earlier, the DoD cautions users about incomplete erasures that make the achievement of the decommissioning objective uncertain. There is also the matter of the inability to certify the procedure.

In lieu of these concerns, in 2005 Bob Johnson, Executive Director of the National Association for Information Destruction, stated that the NAID could not endorse overwriting alone for erasing data from hard drives.

Degaussing

Degaussing is a process that utilizes a machine to produce a strong electromagnetic field that destroys magnetically recorded data on a hard drive.

Originally, degaussing was used to erase bulk quantities of unshielded tape and cartridge media, which require a lower electromagnetic field. It had the benefit of allowing the media to be reused. Today’s shielded hard drives require stronger electromagnetic fields for complete degaussing. There is no way to guarantee that a particular degaussing machine is powerful enough to destroy all of the data on every hard drive. Furthermore, degaussing destroys other components of hard drives. As a result, they are rendered inoperable and cannot be reused or tested to ensure that the data is gone.

Degaussing machines cannot be used in random locations. Caution must be taken so that the strong electromagnetic fields do not produce collateral damage to other susceptible equipment nearby. Companies often utilize the degaussing services of outside vendors. This is due in part to the cost of these powerful machines. Outsourcing can create problems with the chain of custody as care and control are compromised.

If degaussing is outsourced, the hard drives are collected and stored prior to shipment. This makes them vulnerable if they are not stored in a secure location. Once shipped, they are exposed to other people. One final concern is that the degaussed hard drives become inoperable. In other words, there is no way to verify that the procedure has been effective. This makes it impossible to guarantee that the data cannot be retrieved from the drives.

Mechanical Shredding

Mechanical shredding physically tears the hard drive into tiny pieces. Much like degaussing machines, mechanical shredders are large and expensive. Typically, companies employ outside shredding services. The problems associated with internal storage prior to shipment and forfeiture of care, custody and control after shipment are problematic as well.

Secure Erase

Two common disk drive interface standards, ATA (also known as IDE) and SATA, contain a feature known as secure erase. Secure erase is an easy-to-use, data destroy command, amounting to “electronic data shredding.” It completely erases all possible user data areas by overwriting, including the so-called G-lists that contain data in reallocated disk sectors (sectors that the drive stops using for data because they have bit hard errors).

Although secure erase exists within the command set of most IDE and SATA drives over 15GB in size, it is not an easy command to implement on a standard PC running Windows and with a modern BIOS. In most cases, references to this command set are blocked by either the operating system, antivirus software or the system BIOS itself. To date, usage of secure erase via software utility requires the user to create a boot floppy and reboot the machine under an alternate operating system. This approach has limitations, since it does not circumvent BIOS protections that may interfere.

Ensconce Data Technology's Digital Shredder

Given the state of the industry and the pressing need for organizations to improve their data decommissioning strategy, it is clear that a better approach is needed. To that end, EDT has created the Digital Shredder (DS).

The DS is the central component in an organization's overall decommissioning policy. By combining the best available erasure techniques into an integrated, portable environment, you can avoid the problems associated with unintentional loss of data.

Based on an industrial-grade, single-board computer, the DS has been custom built to overcome the limitations of today's product set. Its unique design circumvents the limitations imposed by PC Bios and high-level operating systems...no need to install software on every PC; no need to create boot disks.

Secure Erase - The DS will use the strongest and fastest erasure method known – secure erase—on all ATA and SATA drives. In the event the target drive is too old to have the internal commands, or is an SCSI drive, the DS will automatically detect this and recommend an alternative erasure method.

Multiple Drive Support - The DS supports ATA/IDE, SATA and SCSI drives, and it can do so simultaneously. Multiple drives can be processed at once, making IT resources more efficient. There is also no need to wait for all the drives to complete the routine. Hot swappable bays allow drives to be inserted at any time.

Cable-Free and Tamper-Proof Drive Bays - Due to extensive customer feedback about ribbon cables and power connectors, EDT has engineered an easy-to-use drive interface called a "Personality Block." Different personality blocks fit different drive formats and manufacturers. Once inserted, the bays are electronically locked during the erasure to insure that no one can interrupt the process, even if you step away.

Portable Design - Completely integrated design eliminates the need for a keyboard or mouse. The DS weighs less than 10 lbs. (carrying case optional), so it can be used in the field versus locked in a rack.

Certification Labels - The Digital Shredder includes a laminated label printer that produces certification labels that can be applied directly to processed drives. Labels can only be printed at the end of a successful erase procedure (or can be reprinted by the system administrator). This insures that the process was completed. The label includes all pertinent information pertaining to procedure used, user's name, date/time, method used, elapsed time, hard drive serial number, make, model and manufacturer. This provides a comprehensive diary of the decommissioning process.

Built-In Security - Required username/password login insures that no malicious destruction of drives is possible.

User Programmable Scripts - Allows users to not only erase drives, but also prepare them for reuse. Erased drives can be partitioned, formatted (various file systems supported) and even receive a binary image copy from a drive in another bay.

No License Fees - No per-disk fees, port dongles or boot disks. Simply insert and erase. Software updates can be downloaded from the Ensconce Data Technologies website (<http://www.ensconcedata.com/>) and loaded via USB port on the back of the device.

The chart below lists measurements for ensuring the proper decommissioning of hard drives.

Comparison of Data Destruction Methods					
Critical Requirements	EDT Digital Shredder	Commercial Software	Degaussing Machines	Mechanical Shredders	Third-Party Providers
Destroys data beyond forensic recovery	Yes	No	Maybe ¹	Maybe ⁴	Maybe ⁵
Ensures absolute Care, Custody, & Control of the process	Yes	Yes	Maybe ²	No	No ⁶
Provides certification with a defensible audit trail	Yes	No	No ³	No	Yes
Easy routine to install & implement	Yes	No	No	No	No ⁷
Reformat the drive for potential re-use	Yes	Yes	No	No	No

1. Degaussing machines may not produce a strong enough magnetic field to destroy all of the data.
2. In many cases, degaussing is a third party process.
3. Since the degaussing process disables the hard drive, there is no way to test the process to ensure that the data is gone.
4. Depends on the extent to which the disks have been shredded.
5. Depends on the method used by Third Party Provider.
6. Handing off drives to a Third Party does not absolve legal responsibility.
7. Third Party Providers usually establish set pick-up schedules. The interim periods create an internal storage and security challenge.

Consequences and Penalties for Non-Compliance

Certifiable data destruction is no longer an option—it is a financial and legal necessity. Data loss and data theft can cripple a company financially, ruin its reputation and result in prison sentences for Directors and Officers. Congress has passed several laws mandating penalties for non-compliance, and restrictions and consequences only promise to become increasingly severe.

	Gramm Leach Bliley	Sarbanes Oxley	FACTA	HIPAA
	Financial Service Modernization Act	Public Company Accounting Reform & Investor Protection Act	Fair and Accurate Credit Transaction Act	Health Insurance Portability & Accountability Act
Directors and Officers Penalty Per Violation	\$10,000	\$1,000,000		
Institution Penalty Per Violation	\$100,000	\$5,000,000	\$11,000	\$50,000 to \$250,000
Years in Prison	5 to 12 years	20 years		1 to 10 years
FDIC Insurance	Terminated			
Impact on Operations	Cease and Desist			
Individual Civil Fines	\$1,000,000		Civil Action	\$25,000
Institution Civil Fines	1% of Assets			

A Worst-Case Scenario

If a company believes its hard drive decommissioning method is foolproof, it can become complacent about its data security. Improperly sanitized hard drives can fall into the hands of competitors and unscrupulous employees who can retrieve valuable intellectual property, financial records, personal employee records and other sensitive and confidential material.

When this security breach is made public, the resulting firestorm becomes a public relations nightmare. The company's reputation may never recover, as the perception will always be that this is a company that can't be trusted. Investors will retrieve their investment and seek other opportunities.

The company will be held liable for any resulting damages, such as credit card information that is then used for fraudulent charges and civil lawsuits incurred for the release of private records.

The responsible directors and officers will face embarrassing public trials that can carry fines of up to \$1 million per violation (how many potential violations does each drive contain?) and 20 years in prison per offense.

If the security breach and resulting data loss is severe enough, the company may cease to exist.

Conclusion

Every business must evaluate its decommissioning strategies now to be certain they are not just compliant, but airtight.

Inadequately decommissioned hard drives that result in data loss or data theft are self-inflicted security breaches that are easily preventable. A false sense of security can have catastrophic consequences for the company, its employees, customers and investors.

Previously accepted decommissioning methodologies such as overwriting, degaussing and mechanical shredding must be reevaluated in lieu of their potential failures and vulnerabilities. Given the financial and legal implications of non-compliance, an on-site, turnkey decommissioning procedure that can provide certification is essential to every business.

EDT's Digital Shredder provides the best decommissioning solution, as it offers care, custody and control through every step of the process, and successfully addresses all major decommissioning concerns.



Contact Information

100 Market Street, Suite 203

P.O. Box 6796

Portsmouth, NH 03802 USA

T: 877.338.6246

F: 877.338.6246

www.deadondemand.com

Appendix - Technical Discussion of Erasure Techniques

Although we have made a high-level comparison of disk erasure methods, it will be helpful to compare the various forms of data erasure that exist within the family of data overwriting. To date there has been a direct correlation between the security level of the erase and the time commitment required to perform the erase. This creates a tendency for users and IT personnel to adopt time-saving processes over security, believing the likelihood of information loss to be minimal.

Unfortunately, most users are not aware of the totality of information stored on their drive, nor do they necessarily know what the next use of the drive may be.

Weak Erase

These are erase actions taken by standard users, using typical interfaces such as DELETE commands, or high-level disk formatting. In reality, these commands do nothing more than indicate that the space occupied by the file is now available for eventual reuse. There are several easily obtainable programs for recovering such deletions, including high-level reformatting. (Low-level formatting does actually erase data, but is no longer an available command on ATA drives). From an uninformed user perspective these commands appear to delete data and are very quick to perform.

Block Erase

This method is known more commonly as “overwriting.” There are literally dozens of overwrite programs on the market, with a variety of features. Windows does not provide a means for performing a block erase, but it can be performed in Linux. Nearly all of these utilities claim to meet Federal Government requirements in DoD 5220 which requires three writes – 0’s, its binary complement 1’s, and a then random data pattern which is verified by a read. The shortcoming is that the majority, if not all, of these software utilities cannot erase reassigned user blocks, since these have no logical block address to write to and physical sector address drive commands no longer exist in ATA drives. Also, some of these programs fail to perform the final verification read stage. One final consideration is that there are viruses that can affect these programs and make the report a successful erase, even though no erase actually occurred. A user may have no knowledge that such a virus exists on their PC.

Finally, block erase can be a very slow process depending on the size of the drive. Several hours is certainly an average, and it is possible for large drives to take days to complete. On average, it is eight times slower than ATA secure erase (below).

Secure Erase

Secure erase is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. Secure drive erasure is excellent and quick, and is superior to DoD 5220. The Center for Magnetic Recording Research (CMRR) conducted verification testing that showed that the erasure security is equivalent to DoD 5220 overwrite, because drives having the command also randomize user bits before storing on magnetic media. They verify the block writes via their internal write fault detection hardware, avoiding a separate read verify pass. This speeds execution time, increasing user willingness to secure erase drives. An in-drive command has higher security from malicious software attack. All computer software is vulnerable to attack, but secure erase “hides” behind the standardized drive interface, rejecting any nonstandard commands. It is approximately eight times faster than the three block-writes plus verify of DoD 5220. CMRR testing shows that multiple pass block overwrite utilities, which attempt to meet DoD 5220 can take days to execute, in a drive that can internally secure erase itself in 30 minutes. There is currently no executable secure erase feature for SCSI drives. Though the command (Security Initialize) does exist as a standard, it has not yet been implemented.

Testing at CMRR on drives with secure erase demonstrates that a single verified write pass with a random data pattern makes all original data unrecoverable (see the resources on the CMRR website: <http://cmrr.ucsd.edu>). Drives randomize user data before magnetically recording, so the zeros data pattern in the ATA specification meets DoD 5220. This random write takes place on all drive user data sectors as well as re-allocated sectors (the G-list sectors), in order to ensure that no user data “echoes” remain on the disk (such as O/S page files, crash recovery files or free space from deleted or modified files).). Enhanced secure erase is a method that uses two passes with off track recording. It is currently not available in existing disk drives.

Fast Erase

Fast erase does not actually erase the data. Fast erase is accomplished by issuing a standard “set user password” to a ATA drive, with a randomly selected 256-bit user password and setting drive security to “maximum.” This command completes in milliseconds, leaving the drive locked with a secure password.

When another user acquires the drive it will be locked against any data access commands until a secure erase command is issued and completed. This fast erase only prevents access to data. By comparison, full secure erase has higher security as it ensures that the data is erased before loss of custody. It is theoretically possible to circumvent the fast erase password protection and gain access to the data that is still recorded.