



Technology Paper

## Drive Disposal Best Practices

### Guidelines for Removing Sensitive Data Prior to Drive Disposal

Sooner or later all hard drives are retired. Since the vast majority of jettisoned drives contain sensitive data, the drive owner should either remove the data or completely destroy the drive. But many organizations either fail to understand the risks of leaving data on drives and take no action to remove it, or mistakenly believe the data has been safely deleted when in fact it can still be recovered. This paper provides a set of guidelines and best practices to assist organizations in properly removing the data on hard drives prior to their disposal or reuse.

#### **Most Drives Contain Sensitive Data**

Industry analysts estimate that 80 percent of corporate laptop and desktop PCs contain sensitive data. The percentage of enterprise servers with sensitive data is even higher. Data commonly stored on a hard drive at retirement time includes sensitive personal information, such as personal names, physical and email address, as well as home, work and cell phone numbers. Personal financial information, such as social security numbers, credit card numbers, account numbers, IDs and passwords, are also commonly found. Most hard drives at retirement time are also storing varying amounts of intellectual property, such as company trade secrets, confidential memos and emails, product designs, sales forecasts, financial data, customer lists and contact information, and sensitive human resource information. User IDs, passwords and decryption keys that can access other systems or decrypt untold volumes of data in existing or stored databases, applications or archives can be particularly damaging.

# Drive Disposal Best Practices

## Guidelines for Removing Sensitive Data Prior to Drive Disposal



### Data Thought to Be Safely Deleted Often Isn't

Before recycling or selling a computer or drive to another entity, most organizations will *delete* the data. However what they may not realize is that deleting the data or even formatting the hard disk does not make the data unrecoverable. MIT conducted a study to see what type of information would be recoverable from used hard drives. They purchased 158 hard drives from eBay and other merchants. The devices originally belonged to a number of organizations ranging from banks to law firms. Researchers attached the drives to a workstation running a program called FreeBSD and copied data images from the drives. Of the 158 drives, only 12 had their data destroyed in such a way that it could not be recovered. Sensitive files including thousands of credit card numbers, individual's names and contact information, emails, social security numbers, medical records and other sensitive files were recovered from the remaining 146 drives. In many cases this data was recovered from drives that had actually been reformatted<sup>1</sup>.

To add to the challenge of data deletion, not even formatting a hard drive will completely remove the data. Unfortunately most users, organizations, and merchants reusing or reselling used equipment believe otherwise. This false understanding is derived from the somewhat misleading warning given before format operations: "Warning: Formatting the disk will permanently remove all data." However, formatting a disk does not delete the actual data. Only a small percentage of data on the drive is actually overwritten. As an example, on a 10-GB drive with 20,044,160 sectors, formatting rewrites only 21,541 sectors—less than 1 percent. Formatting *complicates* the recovery of fragmented files, but does not prevent it.

### The Sensitivity of Some Data Never Goes Away

Some may justify not taking strong action to destroy stored information on old drives because they believe the data on them is no longer sensitive or the drive can no longer be read. These beliefs are likely to be incorrect.

It's true that some amount of intellectual property and company trade secrets will eventually become obsolete or public information. However, the sensitivity of some data never goes away. Addresses, phone numbers and social security numbers can last a lifetime, and it's rare for a hard drive to not contain at least some of these. It is never safe to assume that the sensitive data stored on a disk will become un-sensitive. Another often-misunderstood area is just how easy it is to read data from old drives. That pile of discarded drives in the storage room may seem so old and so obsolete that there is little risk of sensitive data being read from them, but that is not the case. Today's computers have no difficulty reading 15-year-old drives.

### Legislation and Good Business Practices Require Hard-Drive Sanitizing

Not only is it good business practice to remove all sensitive data from hard drives before they are repurposed or retired, numerous laws impose stiff penalties when private information is compromised. For example, in the United States, the state of California passed SB-1386. This *Security Breach Information Act* requires that all potential victims be notified when there is reason to believe that their data could have been compromised. At the time of this writing, most states within the U.S. have passed similar laws and all are expected to do so soon. Comparable legislation exists in Europe and Asia. In order to comply with these and other similar laws, anytime a drive leaves a data center or organization, whether for repair, reuse or retirement, all sensitive data must be removed or encrypted.

### Hard Drive Sanitization Approaches

There are four basic approaches to sanitizing hard drive data to ensure it is unrecoverable. Three approaches are patterned after standards created by the Department of Defense (DOD). They include *destruction*, *degaussing* (exposing the drive to a powerful magnet) and *overwriting*, and are described in the National Industrial Security Program Operational Manual DOD 5220.22-M. The fourth method is *cryptographic sanitization*,

<sup>1</sup> Remembrance of Data Passed: A Study of Disk Sanitization Practices. Simson L. Garfinkel and Abhi Shelat. Massachusetts Institute of Technology.

# Drive Disposal Best Practices

## Guidelines for Removing Sensitive Data Prior to Drive Disposal



applicable when data on the drive has been encrypted. Sanitization occurs by destroying the digital key required to decrypt the data.

Each of these methods has various advantages and disadvantages. Some require lots of time to execute. Some require very expensive and sophisticated equipment and are suitable only for large operations. In some cases, the particular circumstances make one method the only viable selection. The following sections detail the pros and cons of each approach.

### Physical Destruction

Whenever a drive is non-operational, or when the data cannot be fully sanitized, the hard drive must be removed from the workstation or server and destroyed, either electronically (see degaussing) or physically. Physical destruction is typically done by shredding the entire drive or the drive's platters. At a minimum, the platters must be badly warped or distorted, rendering the drive or any of its components inoperable. This can generally be achieved by drilling the drive in several locations perpendicular to the platters and penetrating completely through from top to bottom. Hammering or crushing is equally effective but more labor intensive. Simply destroying the logic section of the drive without damaging the platters is insufficient and not recommended.

While awaiting destruction, the equipment must be gathered and stored in a secure facility. This can be a significant expense for organizations with widely-dispersed locations. Following the actual destruction, hauling and dumping costs can also be significant.

Physically destroying a hard drive is a time-consuming process and requires powerful and expensive machinery; therefore, many find that outsourcing the task to a reputable service is more attractive than doing it in-house.

Although physical destruction is expensive and not particularly environmentally friendly, if executed correctly, it is effective for any drive, even non-operational ones. It is also an attractive option if the drives are to be discarded anyway and not reused. Since the drives are going to be picked up and hauled off, a service that shreds the drives and then hauls them away is a step-saving alternative.

### Degaussing

Degaussing to erase the magnetic media on the drive requires specialized equipment designed and approved for the type of media being purged. Degaussing modern hard disks requires magnets capable of generating fields several orders of magnitude stronger than those required to degauss floppy disks or tapes.

Industrial degaussers rated for hard disks are very expensive. Further, their duty cycle is relatively short, making them questionable for sanitizing large numbers of drives in a short time. As degaussing destroys hidden portions of the drive used for bad block recovery, drive head positioning and other functions, drives sanitized in this manner will generally be nonfunctional. Thus degaussing is not feasible if reuse of the drive is desired.

While degaussing of hard drives has a number of disadvantages when compared to other hard disk sanitization methods, degaussing is a suitable practice for other magnetic media, such as floppy disks and backup tapes.

### Overwriting

Sanitizing a hard disk by overwriting is a process whereby a software program writes a combination of 0s and 1s over each location on the hard drive multiple times. This process obscures the previous information under multiple layers of magnetic flux, rendering the data unreadable.

According to DoD 5220.22, functional drives should be overwritten three times prior to disposal or reuse. Three overwrites is generally sufficient to make the data unrecoverable, although it is possible for very sophisticated laboratories utilizing magnetic electron microscopy to determine previous data patterns and recover the data. That being said, we are unaware of any cases where data has been stolen after three overwrites.

Software programs in compliance with DoD wiping or overwriting standards are available to sanitize hard drives. These programs, typically priced somewhere between US\$50 for individual licenses and about US\$500 to US\$2000 for professional versions, are capable of providing

# Drive Disposal Best Practices

## Guidelines for Removing Sensitive Data Prior to Drive Disposal



reasonable assurance that data will be unrecoverable under most conditions.

Unlike either physical destruction or degaussing, overwriting does not destroy the hard drive, so the device may be reused. Another advantage of overwriting is that it is less expensive than either physical destruction or degaussing when sanitizing a small number of drives.

However, overwriting is very time-intensive. It can take far too much time to be cost effective for many organizations, especially organizations that need to sanitize lots of devices. Because overwriting tools repeatedly write data to every track, sanitizing a disk in this manner can take minutes to hours depending on the number of passes performed, the size of the drive and the speed of the system.

### Cryptographic Sanitization

A fourth approach to sanitizing hard drive data uses cryptography. This method is very effective, instant and simple to administer. Sanitization by cryptography works by first encrypting all data as it is written to disk. The only way to read or obtain data protected in this manner is to use a valid decryption key. Instant and thorough sanitization occurs when the decryption key is destroyed.

Cryptographic sanitization is limited to environments where the disk encrypts the data, but in those settings, it has a number of significant advantages over other alternatives. First, cryptographic sanitization is instantaneous. A command issued by an administrator instantly destroys the decryption key, making all data immediately unrecoverable. When compared to other methods of sanitization, cryptographic sanitization saves minutes if not hours of handling for every device. Second, cryptographic sanitization can be done remotely. It's not necessary to gather retired equipment and drives into a physically secure storage facility while they await sanitization. Third, the hard drive is not destroyed, as it is in physical destruction or

degaussing. Drives cryptographically sanitized can safely be reissued within the organization, or sold or donated for reuse.

When cryptographic sanitization can be employed and the drives reused, the cost savings can be substantial. Gartner Inc. reported that the per-PC cost of sanitizing by destruction or overwriting ranges from US\$84 to US\$135<sup>2</sup>. Cryptographic sanitization and reissuing mitigate these costs.

The only disadvantage of cryptographic sanitization is that it is limited to those instances where hard disk encryption has been deployed. Since more and more disks are being encrypted, this disadvantage is expected to be minimized over time.

### Best Practice Recommendations

The following guidelines should aid organizations as they implement disk drive disposal or retirement procedures.

	Encrypted Drives	Unencrypted Drives
Operational	For drives where all sensitive data has been encrypted using standard and accepted encryption practices, such as AES, Triple-DES, Blowfish, etc., and where a secure erase feature is present to destroy the drive's decryption key, sanitizing is best done cryptographically. This method of sanitization allows the drive to be redeployed or disposed of.	Operational drives with unencrypted data should be overwritten with sanitization software that meets DoD 5220.22 specifications. This requires the data to be overwritten at least three times prior to disposal or reuse. Destroying the drive by either physical destruction or degaussing is also an option if it is not feasible to reuse the drive.
Non-operational	If an encrypted drive is permanently non-operational, meaning that the decryption key can never be recovered or used to access the drive's data, then the drive's data has already been sanitized. However, if there is even the slightest risk that the drive could be made operational, the key must be destroyed wherever it is stored.	Unencrypted drives that are defective, dead or unable to complete an overwriting process complying with DoD 5220.22 or NIST 800-88 standards should be degaussed or physically destroyed using the methods described above.

<sup>2</sup> TCO's Last Surprise, Gartner Inc. September 2003

# Drive Disposal Best Practices

## Guidelines for Removing Sensitive Data Prior to Drive Disposal



### Additional Recommendations:

- Develop and disseminate a clear set of policies that govern retiring and disposing of hard disk drives.
- Educate users about the organization's privacy policies, including the policies and proper techniques for sanitizing disk drives.
- Generate and maintain adequate documentation regarding all disk drives that are retired. This documentation should show how and when the disk was sanitized as an audit trail showing that best practices were adhered to.
- As organizations replace existing computers, servers and hard drives, IT and security staffs should encourage the deployment and use of encrypting hard drives to minimize data sanitization burden and costs. Not only will sensitive data be better protected during the drive's useful life, the costs to retire the drive will be significantly less.

There are a number of techniques to sanitize hard drives and meet legislative requirements. Unfortunately most disk drives in existence today are not capable of encryption and contain sensitive data in the clear. Such drives must be sanitized using degaussing, overwriting or physical destruction. However, sanitization by encryption is much simpler and more cost effective than any other method. Therefore, organizations should begin now to look for ways to transition to encrypting disk drives over the next few years.

### Summary

A staggering amount of sensitive data is stored on disk drives around the world. Since sensitive data can have a very long life span, it is critical to destroy that data on disk drives as they go out for repair, reuse or disposal.

Numerous laws and regulations require that sensitive data be safeguarded against disclosure, and there is no time limit placed on the requirement to protect the data. If a 10-year-old disk drive containing sensitive data goes outside of the organization without being sanitized, serious consequences may ensue.

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550  
ASIA/PACIFIC Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888  
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 130-136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00