WHY DATA ERASURE in the DATA CENTER

A recent Ponemon Institute research paper indicated that 70% of data breaches originate from off-network devices. Modern Enterprises realize the necessity of securing data located in off-network data bearing devices. These devices include hard drives, USB memory sticks, and Flash Media. Hard drives in the data center are located primarily in storage arrays and servers of various sorts.

When an Enterprise is finished using a hard drive, either because of a warranty (RMA action) or end of life, there are essentially four options:

	Cost	Risk	Impact on Environment
Erase	Low — $0 per drive + cost of erasure appliance & software	Low — statistically impossible to recover useful data. Common Criteria EAL4+ Augmented erasure software now available	Low — Drive reused
Shred	High $1250 per + cost of shredding	Low — if a high quality shredder that shreds to less than 1/250th of an inch is used.	High - landfill
Degauss	High $1250 per + cost of degaussing	Medium — a very strong degausser is necessary otherwise data may be left intact.	High - landfill
Storage	High $1250 per + cost of storage	Medium — each time the drive is handled risk of loss increases.	Neutral — but eventually drive must be destroyed

Disk Shredding

Obsolete government document DoD 5220-22M required physical destruction for data classified higher than Secret. The University of California at San Diego's Center for Magnetic Recording Research (CMRR) published the "Tutorial on Disk Drive Sanitization" (Gordon Hughs, Tom Coughlin) which states that unless a disk is shredded to particles of less than 1/125th of an inch, meaningful data may (and has been) be recovered. This paper was written in 2008 and explicitly states that the as drive density increases (yearly) the acceptable size of a shredded disk particle will need to be smaller than 1/125th of an inch.

Disk Degaussing

Drive designers continually increase the linear density of magnetic recording to create higher data storage capacity per disk. This raises the disk magnetic coercivity, the field required to write bits on the magnetic media. As the magnetic coercivity increases, the fields required to erase the data on recorded disks increases. Thus an older degausser may not fully erase data on a newer hard disk drive. New perpendicular recording drives may not be erasable by present degaussers designed for past longitudinal recording drives.

Greg Stickel
Virtual I/O Solutions
gstickel@virtual-io..com

Future generations of magnetic recording media may use very high magnetic coercivity disks to achieve areal densities greater than 500 gigabits per square inch. These drives may have technology using laser light in the magnetic write element of the disk drive, to raise the temperature of a spot on the magnetic medium in order to lower the magnetic coercivity to the point where the write element can record a bit on the very high coercivity magnetic media. For disk drives using this Heat or Thermally Assisted Magnetic Recording (HAMR/TAMR) technology the degausser field required to erase the disk drive at room temperatures may be impossible or impractical to achieve. In this case the drive may have to be physically destroyed.

"Hybrid drives" are now being introduced for notebook or laptop computers that have flash memory write cache on hard disk drive circuit boards. Magnetic degaussing would not affect any resident data on such semiconductor memory chips. Data on these non-volatile semiconductors would have to be sanitized using some other technique. For all these reasons degaussing of all the data on hard disk drives will become increasingly impractical.

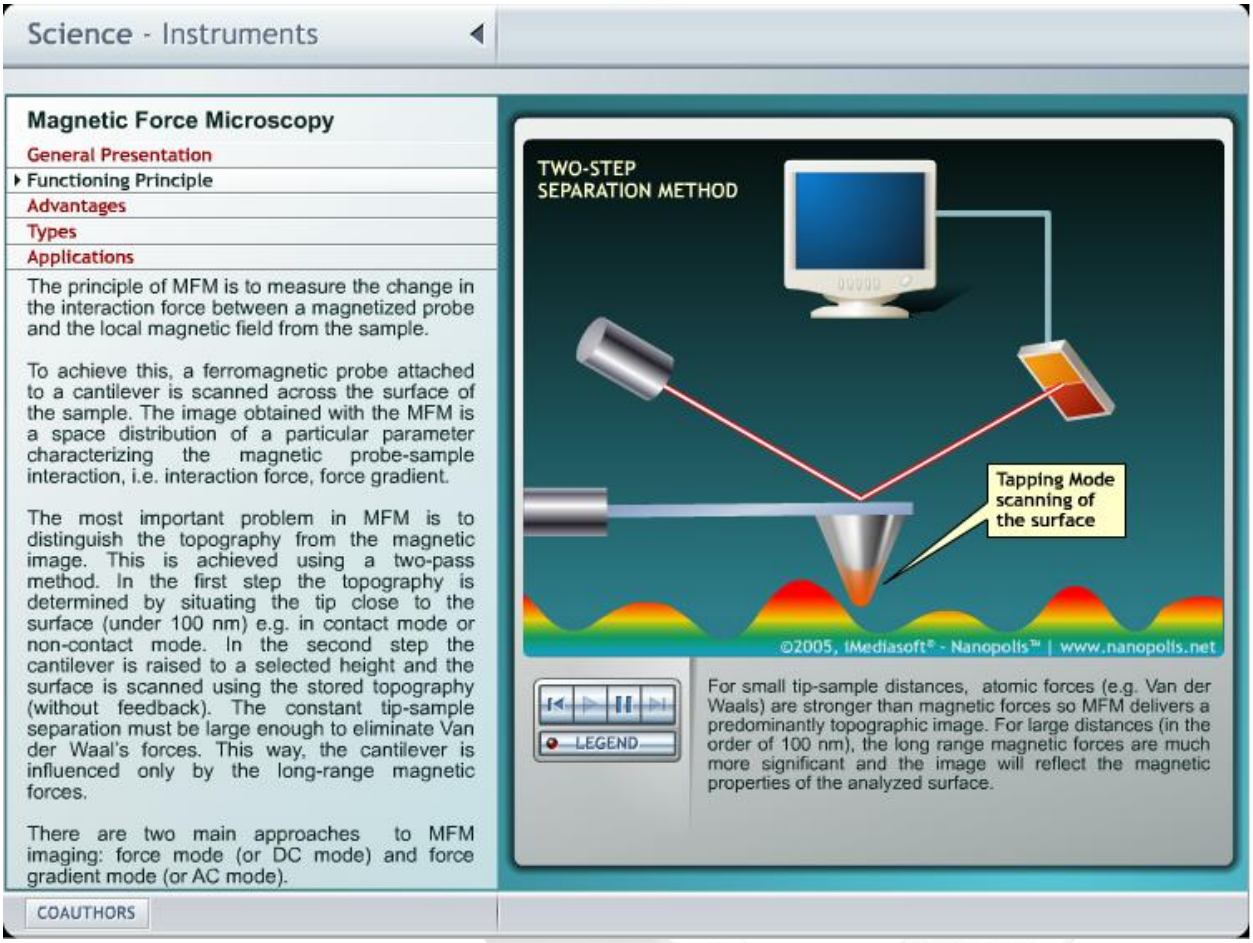
Data Erasure (Overwriting)

When a hard drive is erased with the correct combination of hardware and software, recovery of any meaningful data is virtually impossible, according to forensics research conducted in 2008 by Craig Wright (Overwriting the Hard Drive, The Great Wiping Controversy). The odds of recovering a single bit of data correctly are 50% for any given bit. This implies the odds of reconstructing data on an erased hard drive using Magnetic Force Microscopy (MFM) are no higher than if a person simply guessed whether any given bit on a drive were a 1 or a 0.

Data Overwriting Process

There are as many as eighteen international erasure processes. The most commonly used in the United States is the Department of Defense (DoD) 5220-22M. This standard is typically associated with either a 3 pass or 7 pass overwrite, although the standard as updated in 2006 no longer specifies a recommended number of overwrites. The National Institute of Standards and Technology (NIST) is the most up-to-date "authority" regarding data security in the U.S., and they specify that for drives manufactured since 2001, a single pass overwrite is adequate to protect from both a keyboard and laboratory attack.

Greg Stickel
Virtual I/O Solutions
gstickel@virtual-io..com



RMA Drives

Working drives are constantly pulled from active storage arrays and servers because modern storage arrays and servers utilize "Predictive Failure Analysis (PFA)". A drive in a RAID group is pulled, a replacement drive inserted,, the data is rebuiltto the new drive. Manufacturers now require this pulled drive to be returned via Return Merchandise Authorization (RMA) to their facility. Most often, this "failed" drive still spins and holds vital customer information, the release of which would be in violation of PCI and HIPPA requirements:

1) PCI 3.1.1. — Data owners must "implement a data retention and disposal policy that includes…processes for secure deletion of data when no longer needed.
2) HITECH Act — Protected Health Information (PHI) is rendered unusable, unreadable or indecipherable…if one or more of the following applies: Electronic media have been cleared, purged, or destroyed consistent with NIST Publication 800-88, Guidelines for Media Sanitization, such that PHI cannot be retrieved.

Erasure of RMA or standalone drives requires the use of specialized hardware and software. The best software erases all areas on a disk, including the DCO & HPA, yet it should not erase the "service area" (leaving the drive serial number intact). The best erasure software should not need to reformat the drive block size prior to erasure, because doing so would render the drive unrecognizable to the manufacturer. The best erasure software should be able to erasure any block size (512, 520, 522, now 524K) and return the drive in recognizable condition. Every

Greg Stickel
Virtual I/O Solutions
gstickel@virtual-io..com

attempt should be made by the software to erase any bad sectors on the disk, if bad sectors are found which cannot be erased sector by sector, the software should be able to step down and attempt to erase block by block. Can the erasure product erase Fibre Channel, SAS/SATA, SCSI, and IDE drives? If not, multiple products may be required. As drive capacities increase the ability of the software/appliance to pick up and continue to erase after an aborted erase attempt(power loss, appliance reboot, etc), becomes increasingly important. Drive erasure times can range from a few minutes to a couple of days depending on the drive capacity/speed and erasure methodology chosen (1x,3x, 7x overwrite).

Data Center Storage Arrays

Disk arrays house the vital data of any enterprise, most of which is subject to regulatory compliance. Disks in these arrays are subject to the same data security requirements as RMA drives. If there is no longer a requirement to house sensitive customer data (per PCI-DSS 3.1.1 requirement), said data must be securely erased. There are two common situations which require the eraser of all or some of the disks in a storage array:

1. End of Life (EOL) — An array has been fully depreciated, or its lease has expired, the data has been copied to a replacement array. Now it is necessary to erase the data from the disks within the array prior to its transfer to a third party.
2. Repurpose — An array may have been use for a specific customer or application and now will be reconfigured for other use. Sensitive customer data must be erased prior to new use of the array (per PCI-DSS 3.1.1)
3. Transfers — An array may need to be transported from one facility to another (within the same enterprise) and data must be erased prior to transfer as protection against theft or inadvertent loss.

Specialized hardware and software is required the erase storage arrays at EOL. The preferred method of erasure is via direct attachment to Disk Array Enclosures (DAE), or disk drawer. Specialized HBA's and software are required to address the disks directly and perform a secure erasure of the drives. When performed correctly, all data may be securely erased from each drive.

Disk array erasure is best accomplished using a dedicated erasure appliance. Erasure can be accomplished with various data erasure software packages and the right combination of servers/HBA/Cables/Connectors, but there is a reasonably high degree of skill required to accomplish erasure using this approach. Most corporations will choose to either use a dedicated appliance or outsource array erasure to a service provider with the necessary skills and equipment.

Summary

Disk erasing in the data center is best accomplished via a specialized appliance which bundles necessary hardware and erasure software. RMA drive erasure will almost always require the use of specialized appliances. The most complex data erasure in the data center is for full disk arrays. The difficulty to erase an array ranges greatly depending on the manufacturer/model of array to be erased — with true enterprise class arrays (HDS USP, EMC DMX, IBM DS8000) among the most challenging the erase .Modular arrays are generally easier to erase with the drives remaining in their enclosures.

Hard disk erasure in the data center is becoming the alternative of choice because of both superior economics and security vs. shredding or degaussing.

Greg Stickel
Virtual I/O Solutions
gstickel@virtual-io..com