

# Securing Storage



## COMPLETE DATA ERASURE ON STORAGE SYSTEMS

BY LEO COLBORNE

**O**UT OF SIGHT, OUT OF MIND. When storage systems are upgraded, retired due to proactive maintenance, reach the end of their lease, or are repurposed or resold, companies often delete the data from the disks and forget about it. However, there is a tremendous amount of critical, confidential, and competitive information on those disks that cannot be completely erased by just pressing a delete button.

This exposes competitive intelligence, increases vulnerability to industrial espionage and litigation, and jeopardizes an organization's compliance with corporate governance practices and state, federal, and industry regulations that protect proprietary and confidential corporate, customer, and patient information. For example, regulations such as DOD Pub. 5220-22.M, Sarbanes-Oxley, and HIPAA require proof of secure erasure.

- > Un-erased information is still accessible when storage systems are returned under lease, redeployed, swapped, or repurposed.
- > Corporate guidelines require data erasure and removal of proprietary information prior to returning leased systems or repurposing storage systems.
- > Some companies or industries require proof of data erasure and overwrite levels.
- > Companies have different data disposal standards for different types of information.
- > Some companies and industries require a three-pass or greater overwrite process (recommended in DOD 5220.22-M level).
- > Companies have strict security requirements, to retain all disks and you need to secure them.

- results, but the overwrite application must be sophisticated enough to locate and overwrite hidden and damaged sectors, as well as produce audit reports for compliance purposes.
- > **Degaussing:** Demagnetizing to remove all data. Degaussing can be effective, but it often leaves the disk drive unusable. This is not a good thing when a company intends to repurpose the drives. It is also not cost-effective to degauss large numbers of high capacity disks in storage systems.
- > **Destruction:** Physically crush and shred drives. This destruction is extremely effective in erasing data and can be therapeutic for a stressed-out IT professional. However, it is time consuming, costly, and impractical for retiring a large number of drives.
- > **Storing old drives:** Physically storing drives. Presumably drives are erased

## “Un-erased information is still accessible”

Consequently, it is vital that data be completely erased and the erasure recorded to ensure critical and confidential information is secure from accidental or malicious recovery. Done correctly, data removal meets important compliance regulations and guidelines for erasing data, such as sensitive patient records or financial procedures.

### Why Ensure Erasure?

There are several reasons for completely and provably erasing stored data, including:

- > Data disposal and erasure has to conform to industry and other regulatory requirements.
- > Potential litigation, loss of intellectual property, or financial loss can result from un-secure data disposal.

### Delete That Disk

Most companies know how to implement security measures to protect existing data. However, the options for safely and securely removing data from a drive so it cannot be retrieved are not nearly as advanced. These common measures include one-pass overwrites, degaussing, physical destruction, and physically storing old drives.

- > **One-pass overwrites:** Replacing data stored on hard disk drives with a variable bit pattern of 1's and 0's that effectively renders the data unrecoverable. A single pass will successfully overwrite some of the data, but not all disk sectors are visible to overwrite applications. This can leave highly critical information perfectly intact. Multiple passes can yield better

before being stored, but not necessarily. It has been estimated that 85% of business espionage crimes are inside jobs. So, this technique may make it easier for employees to access retired drives to commit these crimes. And physical storage does not meet most compliance regulations for erasure, nor does it protect a firm in the event of litigation.

### Best Practices

The most efficient, cost-effective, and compliant method of erasing data is to completely overwrite the drive to render the data virtually unrecoverable, and to have the capacity to report the procedure. This is harder than it looks, especially with large and complex storage systems. Companies can assign service levels according to the relative importance of

the data; with more overwrite passes for critical information. (Common overwrite levels go from three passes for noncritical data up to seven for the most sensitive information.) Once done, the professional service or erasure application should deliver an independent audit and written proof of service completion.

Observing best practices in data erasure has a number of benefits for security-conscious firms. Complete data erasure maximizes compliance measures by managing risk, ensures information in the life cycle disposal phase is really being disposed, enables that utilization and repurposing storage, and lets IT professionals sleep at night knowing they have secured important data on released storage assets.

### Data Erasure Services

A number of hardware and software vendors provide data erasure services for the PC market, but storage systems are relatively ignored. Due to the sheer size and complexity of storage systems, efficient and complete data erasure is beyond the capabilities of the simpler

methods. But managing the data life cycle from creation through deletion includes making sure that data has actually been disposed.

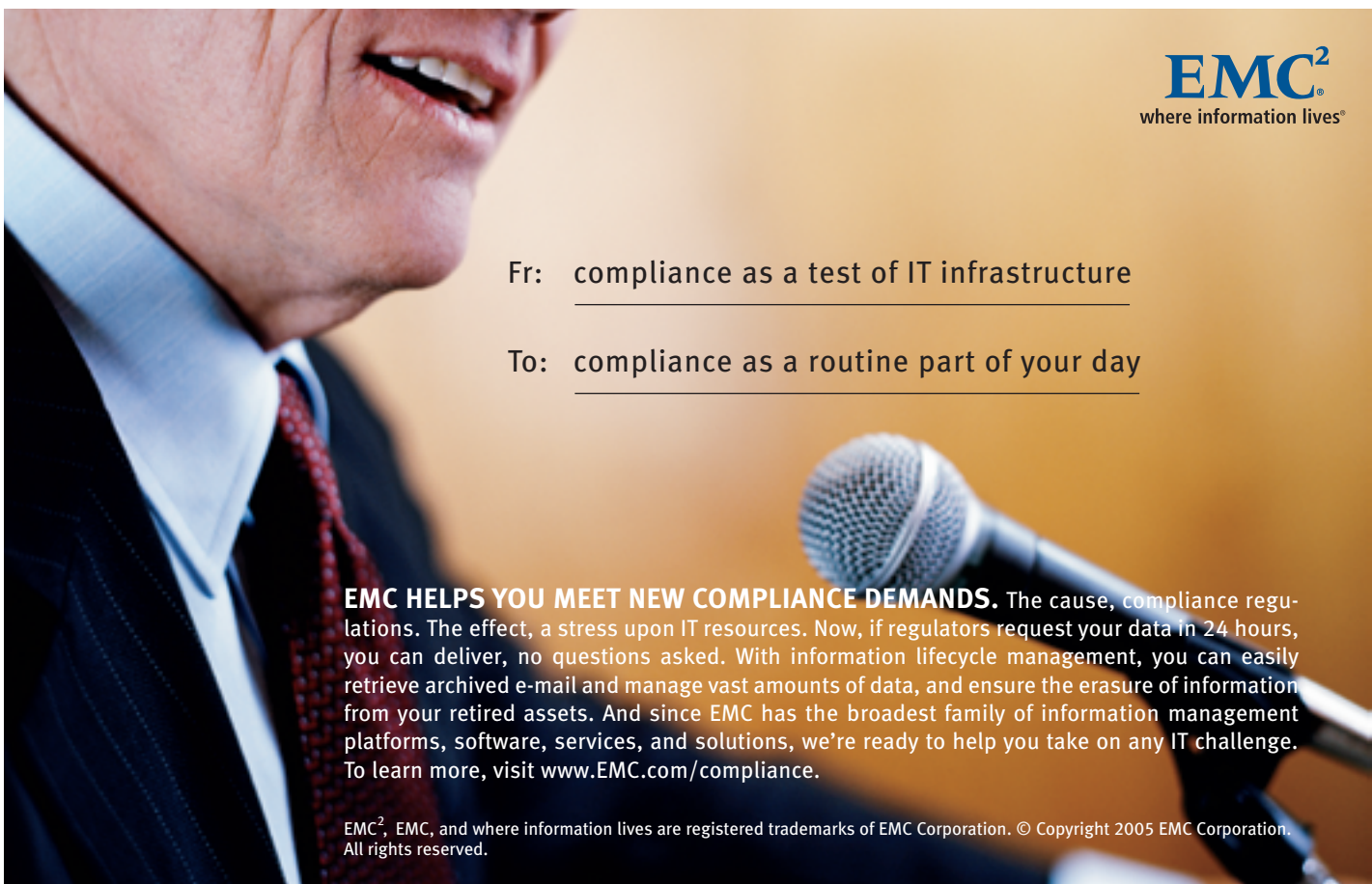
Storage system data erasure services can completely erase data on storage assets and prove they've done it. For example, EMC's non-host-based process completely overwrites proprietary and sensitive data, offers flexible overwrite passes and provides audit reports to meet compliance requirements. Any secure data erasure for storage systems should be able to handle the specific requirements of storage assets, be available from highly trusted professional services (for complete security and audit purposes), erase multiple disks and frames concurrently, have a flexible overwrite pattern for differing specifications, be delivered at the customer location to increase security and eliminate delays, and provide an independent audit and documentation of data erasure.

While firewalls and other security measures protect data on the front end of the storage life cycle, it is equally

important to protect data at the back end. When it comes to returning, reselling, repurposing, trading, or swapping out storage assets, companies need secure and complete data erasure to meet corporate governance, industry specifications, and governmental mandates. Reliable and proven data erasure services dramatically reduce potential legal litigation due to uncontrolled distribution or viewing, avoid the physical destruction of perfectly good equipment, and address any security concerns. As a result, companies can safely sell or reuse storage equipment and ensure they have the audit trail necessary to meet corporate and industry conformance requirements. Most importantly, this will protect an organization's most valuable asset – its information. ■

### About the Author

*Leo Colborne is EMC Corporation's senior vice president for Global Customer Service and is responsible for the overall management, operation, training, tools, infrastructure and resources for the company's industry-leading global support organization ([www.emc.com/global\\_services/init/data\\_erasure/index.jsp](http://www.emc.com/global_services/init/data_erasure/index.jsp)).*



**EMC<sup>2</sup>**  
where information lives®

**Fr:** compliance as a test of IT infrastructure

**To:** compliance as a routine part of your day

**EMC HELPS YOU MEET NEW COMPLIANCE DEMANDS.** The cause, compliance regulations. The effect, a stress upon IT resources. Now, if regulators request your data in 24 hours, you can deliver, no questions asked. With information lifecycle management, you can easily retrieve archived e-mail and manage vast amounts of data, and ensure the erasure of information from your retired assets. And since EMC has the broadest family of information management platforms, software, services, and solutions, we're ready to help you take on any IT challenge. To learn more, visit [www.EMC.com/compliance](http://www.EMC.com/compliance).

EMC<sup>2</sup>, EMC, and where information lives are registered trademarks of EMC Corporation. © Copyright 2005 EMC Corporation. All rights reserved.