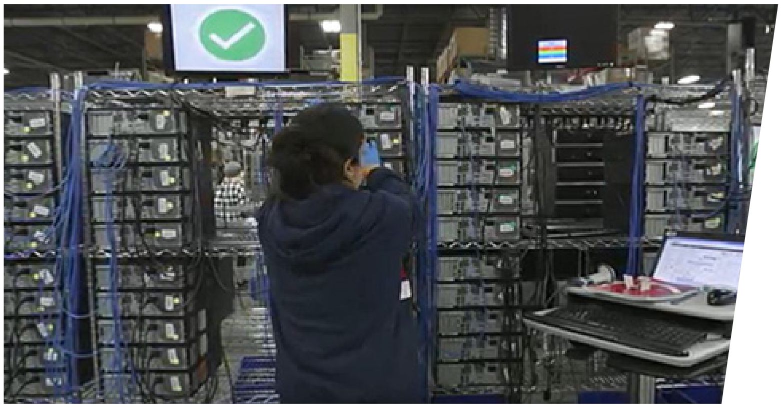
BEST PRACTICES FOR DATA DESTRUCTION

IRON
MOUNTAIN®

THE PROS AND CONS OF DIFFERENT DATA DESTRUCTION METHODS

A recent IDG research survey among 200 U.S.-based IT leaders found they are keenly aware of the risks associated with inappropriate disposal of end-of-life IT equipment. Their top concerns include: loss or theft of customer or patron information; damage to organization's reputation; loss or theft of intellectual property; punitive fines; and criminal charges. Despite these concerns, there is a great deal of confusion over how to erase properly the data on end of life IT assets. 56% of IT professionals who were recently surveyed by Blancco, a leader in data erasure software, erroneously believed that a quick or full reformat of a drive would permanently erase all data.

Failure to properly destroy the data on end-of-life IT assets can lead to serious breaches of data-protection and privacy policies, compliance problems and added costs. There are three main options for data destruction: 1) Overwriting, 2) Degaussing, and 3) Physical Destruction.



OVERWRITING

Overwriting involves writing new data on top of old. The process is analogous to recording over an old VHS tape. Because this process erases the old material and renders anything left completely unreadable, this form of data destruction is also called data wiping.

When data is overwritten, a pattern of 1's and 0's is written over the original information. Sometimes a random pattern is used but a set pattern can also be used which allows for later verification that the drive was wiped by detecting the set pattern. Overwriting data once is enough for most situations. However, for high-security applications multiple wipes may be required. This provides an extra level of assurance that the old data is destroyed.

On the downside, it takes a long time to overwrite an entire high-capacity drive. This process might not be able to sanitize data from inaccessible regions such as host-protected areas. Overwriting might require a separate license for every hard drive, and the process is ineffective without good quality assurance processes. Another factor to consider is that overwriting works only when the storage media is not damaged and is still writable.

DEGAUSSING

Degaussing uses a high-powered magnet to disrupt the magnetic field of the storage medium and destroy the data in the process. When applied to magnetic storage media such as hard disks, magnetic tape, or floppy disks, degaussing can quickly and effectively purge an entire storage medium.

While degaussing can be an effective method of data destruction, it has two major disadvantages. First, degaussing renders the hard drive inoperable by physically disrupting the delicate interconnected mechanisms of the drive - thus destroying any potential end-of-life value. Second, there is no way to ensure all data is destroyed. Because degaussing renders a drive inoperable, there's no way to run the drive to verify the data is gone. The effectiveness of degaussing can also depend on the density of drives. Finally, it should be noted that degaussing does not eradicate data from non-magnetic media such as Solid State Devices and CD's.

PHYSICAL DESTRUCTION

If you don't need to reuse hard drives, physical destruction is a possible data destruction option. Organizations can physically destroy data in a number of ways – including shredding, drilling, melting, or any other method that renders physical storage media unusable and unreadable.

There can be problems with physical destruction. First, it is prone to human error and manipulation. There is no reliable way to audit the physical destruction process. Second, most methods of physical destruction leave large portions of the drive platter intact, even if the drive is inoperable.

Data could still be recovered using forensic methods in such cases. Only pulverizing the disk to particles ensures the data is irrecoverable. Lastly, since physical destruction renders media unreadable, it also prevents them from being wiped and remarketed. This means that there is no longer the opportunity to recover any end-of-life value that these assets may potentially hold.

CONCLUSION

The best method of data destruction depends upon the type of media, the sensitivity of the data, and the end-of-life value of the assets. Many firms attempt to perform data destruction in house. That's not typically a good use of internal time and resources. Most IT asset disposition firms have the expertise and scale to perform data destruction on a much more cost-effective basis.

Iron Mountain's Secure IT Asset Disposition solution helps companies ensure that their IT assets are properly destroyed, recycled, or repurposed for maximum value — using secure logistics and chain-of-custody methods to ensure compliance, security, and sustainability.

FIND OUT MORE:

WWW.IRONMOUNTAIN.CA/SITAD

IRON MOUNTAIN®

WE PROTECT WHAT YOU VALUE MOST®

800.899.4766 | IRONMOUNTAIN.CA

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.ca for more information.