Data Sanitization for Data Center Decommissioning

HORIZON
TECHNOLOGY

FROM DATA CENTER DECOMMISSIONING
TO STORAGE REMARKETING, WE'VE GOT YOU COVERED

HORIZON
TECHNOLOGY

Contents

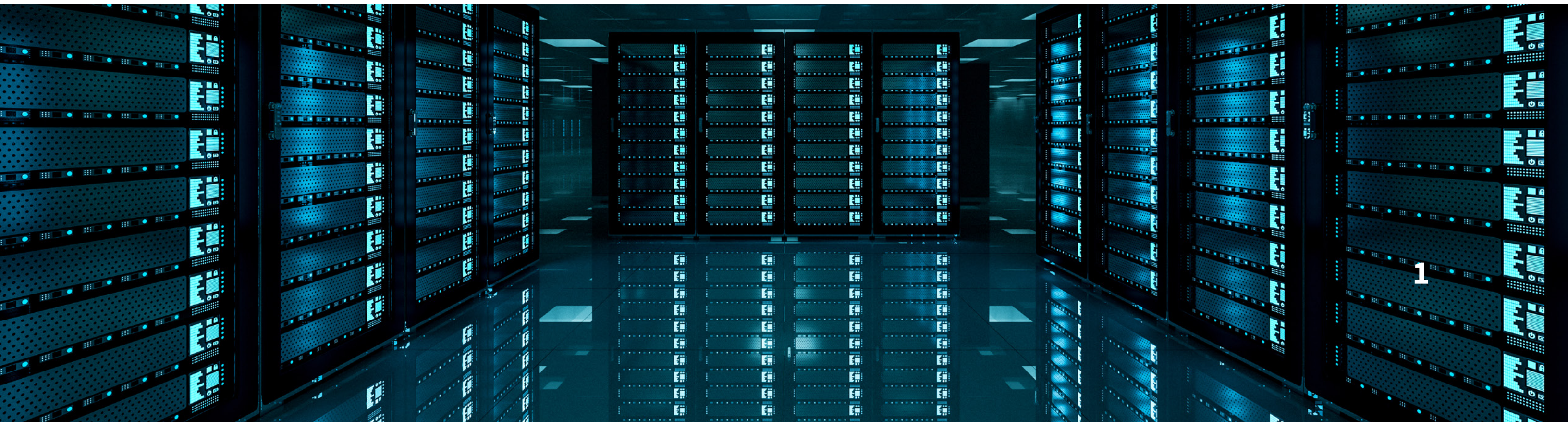
DATA EXPLOSION

We are in the early stages of an explosion of data the likes of which the world has not before seen. Experts herald the emergence of a new data-driven world similar in magnitude to the disruptive force of the industrial revolution. Today's corporations rise and fall around their management of data.

All of this data needs a place to live, and the hardware that houses it doesn't last forever. Hard disk and solid state drives have finite life spans. Once it is time to refresh, upgrade, or decommission, what to do with the obsolete hardware and the data on it?

In an era of heightened sensitivity to data breaches, it is easy to forget that your retiring hardware assets have recoverable value.

"According to research by IDC and Seagate, nearly 20% of the data produced by 2025 will be critical to the functioning of everyday life."



MANAGING YOUR ASSETS

Companies must also take into consideration the physical security of their data.

Whether data is in an offsite data center, on-premise, or anywhere in-between, it's contained on a variety of hardware, from flash storage to spinning hard drives through tape and optical media.

Meanwhile, organizations must account for their employees' devices, such as laptops, smartphones and other mobile devices. IT asset management is a head-spinning proposition at the best of times.

Major organizations such as Google—otherwise a large-scale seller of used HDD—have gone so far as to deploy robots to destroy redundant or retiring hard drives containing sensitive data. Where's the value recovery in that?

"Are you migrating storage to the cloud and working out what to do with your retiring drives?

Or are you approaching a refresh cycle and want to maximize value recovery from your retiring asset?

You need peace of mind that your drives will be comprehensively sanitized."

DATA BREACH CENTRAL

With great regularity, we hear about corporate data being compromised—hacked, stolen, or otherwise misused by nefarious actors. Those corporate entities are widely held responsible for the security of the data they store. Given the sensitivity of the data and the increasing value companies derive from it, securing data is an issue that's been moving up the corporate ladder, from the IT function all the way to the C-suite in many organizations.

Keeping data digitally secure is a huge challenge for the enterprise. As hackers' digital tools get more sophisticated, IT's digital countermeasures seek to rise to the task. And although consumers are generally not careful with data on their own disused devices, they are not forgiving of companies that do not take care of data stored outside of their control. The risk of legal suits inflicting damage on your corporate reputation is real.

At the same time, the proportion of enterprise data breaches directly attributed to the sloppy disposition of storage drives is low. The majority of data breaches stem from malicious attacks on active systems, not decommissioned assets.

"According to a 2018 study conducted by Ponemon Institute and sponsored by IBM Security, the average cost of a data breach globally is $3.86 million. U.S. companies experienced the highest average cost of a breach at $7.91 million. For those companies experiencing mega breaches of more than 1 million records, malicious activity was at play in more than 90 percent of cases in the past two years."

WEIGHING THE OPTIONS

So, with data security in mind, what to do with all the hard drives kicking about when it comes time for a refresh cycle or to decommission parts of a data center?

When responsible companies decide to upgrade and replace, or dispose of, outdated equipment, one of the considerations must be how to wipe the data from those devices, or otherwise sanitize the hard drives where the data resides.

It's a thorny issue. There are a number of approaches that can be used to delete data from hard drives, including deleting unwanted files; using software tools; encrypting the drives; or physically destroying the drive, by degaussing it (*such that the drive is demagnetized by use of a strong magnetic field*), drilling through it, or shredding it, to make it inoperable.

> "A significant loss of potential value is caused by a lack of understanding and knowledge of the full capabilities of modern data sanitization."
> — iNEMI

THE CASE FOR REUSE

Too often data center operators opt to destroy without fully exploring the feasibility of reusing the drive in some fashion. According to the International Electronics Manufacturing Initiative (iNEMI), many fully functioning HDDs are destroyed unnecessarily due to data security concerns. Amid fears that data might be left on the media after sanitization, hard drives are rendered inoperable instead of being reused or remarketed.

The reality is HDDs are going nowhere any time soon. In spite of the rise of flash storage driven by high performance and falling costs, the high capacity and lower costs of spinning disks resonate with hyperscalers managing huge clouds.

Much in the same way that tape is still in deployment, HDD will remain a permanent fixture. As such, we need to bring every effort to bear on prolonging the use of each hard disk drive in circulation for as long as possible.

> “The rise of cloud-based storage means that most (spinning) hard disks will be deployed primarily as part of large storage services housed in data centers.”
> — Google Cloud

HARD DRIVES FROM HARD DRIVES

When a drive has physically failed and dismantling is necessary, we must ensure the smartest possible disposition of the asset. Researchers are already working to develop innovative ways of reusing and recycling otherwise failed HDD components into new hard disk drives. Storage leader Seagate, a member of iNEMI's HDD working group, calls for the creation of "*hard drives from hard drives*."

Nonetheless, many retiring disks still have a functioning life ahead of them. Through rigorous and professionally managed data sanitization, organizations can recover value from storage hardware, both helping the environment and the bottom line.

That the form factor and design of hard disk drives haven't changed that much in the past few decades make HDDs the perfect candidate for refurbishment and redeployment. The best possible environmental outcome for a HDD is to reuse until it is no longer possible to reuse, industry professionals say.

"Clients in our space are recovering more than$1 million in annualized asset value for a resource— retiring HDDs— they previously only viewed as a disposition headache."

DECODING DOD

To shift industry behavior toward greater consideration of reuse before electing for dismantling or destruction, data center operators must feel confident in the thoroughness of the data sanitization process for hard drives.

For some time, the "*DOD standard*", officially known as DoD 5220.22-M, was widely touted as industry best practice. The problem is that the standard was never intended to be a standard, and—in its stipulation of three overwrite passes—represents too heavy-handed an approach for most data sanitization cases, requiring additional time and cost. If the initial overwrite is sufficiently rigorous and thoroughly tested, isn't that enough?

Despite this, the DOD standard, which originated in 1995, continues to get used in ITAD marketing statements today.

NIST SP 800-88

By contrast, the U.S. National Institute of Standards and Technology (NIST) guidelines for computer media sanitization, known as NIST SP 800-88, are widely considered to be the actual go-to standard.
NIST 800-88 provides rigorous and comprehensive guidance for companies and U.S. government entities to ensure they are following best practices for data destruction.

The NIST standard recommends that once organizations decide to embark on a sanitization project, clear steps are followed:

- Verification of personnel competencies—meaning that anyone doing the sanitizing is competent and trained on the equipment to be used.

- Verification of equipment—meaning that the equipment that's being used is properly calibrated and that proper maintenance procedures are used on the equipment.

- Verification of results—ensuring that the data to be sanitized has actually been sanitized.

> "Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. The level of effort applied when attempting to retrieve data may range widely"
> the NIST 800-88 guidance explains.

ADISA, R2, & e-Stewards

Another standard that actively supports organizations seeking to achieve best-in-class control around data sanitization is offered by the Asset Disposal & Information Security Alliance (ADISA). ADISA conducts audits of companies who wish to become a part of the alliance. Once it's determined that the company is capable of meeting the organization's criteria, the company is eligible to apply to be certified.

ADISA has a rigorous process for certification, and conducts regular audits of at least two per year for its certified members. These may include unannounced operational audits of each company, involving forensic tests of a sample size of 10 pieces of media. Full audits are carried out at least every three years.

R2 is an industry-leading certification for responsible recyclers of electronic equipment seeking for accreditation. It has a well-established presence in North America, and a growing profile internationally. e-Stewards also offers a rigorous certification program for e-waste recyclers, differentiating its accreditation by stipulating the prohibition of exports of e-waste to developing countries.

THE HORIZON DIFFERENCE

How rigorous is your approach to data sanitization? Are you clear on the process your ITAD vendor deploys to ensure data is comprehensively erased from the storage drive prior to remarketing?

Horizon has been focused on the hard drive industry for over 20 years, working with the most recognizable names in the industry.   As the world's largest distributor of factory recertified drives for Seagate, WDC, and Toshiba, we offer unparalleled technical expertise and the highest levels of security for your data sanitization workflows. Our process includes:

- System level uploads of test/wipe results by individual drive prior to movement to the next workflow juncture.
- Systematic second auditing of serialized wipe results at the outbound audit (OBA).
- Physical shredding of any device that cannot be successfully sanitized to ensure no data can be recovered.
- The generation of serialized certificates of data wipe and drive destruction for all processed drives.

All data sanitization is completed in strict accordance with the NIST SP 800-88 standard as well as DoD 5220.22-M, where deemed appropriate. Horizon wipe software and workflow is 3rd party certified by ADISA.

Do not overlook the potential to recover value from your retiring assets when approaching a refresh cycle or decommissioning a data center. It's not only good for the environment but good for your bottom line.

Contact us today and let's start a conversation.

info@horizontechnology.com
(949)-595-8244
www.horizontechnology.com

HORIZON
TECHNOLOGY