

Why should you STOP
Destroying Storage Devices & Worry about
Secure Data Destruction?



Global Datasphere Expansion is Never Ending

- ☐ As per IDC Report, World Data will grow from **33 ZB** in 2018 **to 175 ZB** by 2025. **CAGR of 61%** over the **seven-year** period is observed.
- ☐ According to a report by IBM, it is estimated that **90% of the World's data** was generated in just the **last 2 years.**

Isn't this Humongous!





Reasons For Surge in Data Growth

- ☐ **Spurred Growth** in Internet Usage (15-fold rise between 2010-2020)
- ☐ **Technological Advancements in hardware** like never before
- ☐ **Growth in IoT Devices** like smartwatches, smart phones, smart appliances, smart gadgets and other electronic devices that record data
- ☐ Increase dependency on **Cloud computing** for backups and storage of information
- ☐ Predominant use of **AI**, **machine learning**, block chain technology across industries
- ☐ Post Covid Rapid Digital Transformation





Data Handling Challenges for ITAMs

- Maintaining Data Security and Privacy
- ☐ Handling **Data Disposal**
- ☐ Staying Compliant with **Multiple Data Protection Laws**
- ☐ Verifying Data Destruction For EOL IT Asset
- ☐ Comply with **Environmental Regulations and Standards**
- ☐ Track Chain of Custody to prevent Data Theft, and Leakage





Conventional Belief: Destruct IT Assets

☐ Shredding is Secure as per National Security Agency guidelines

What about Environmental Concerns?

What About E-waste Generated due to Shredding and Degaussing?

Physical Destruction Should Be Seen As The Last Resort!





Did You Know?

How Much E-waste Is Generated by Physical Destruction?

- According to Mission Critical Magazine, If a company has a 200-rack decommissioning project, that equals to 55,000 hard drives, which, if shredded, result in around four dump trucks of metal resulting in 33 Metric Tonnes of e-waste that ends up in a landfill.
- In the U.S. around **151 million phones end up in landfills or incinerators every year,** which amounts to 416,000 a day. By 2030, annual e-waste production is set to hit 82 million tons globally.



Source: According to World Economic Forum



E-waste Health Issues Owing To Physical Destruction

The piling e-waste is a cause of concern!

- According to EPA "An undetermined amount of used electronics is shipped from the United States and other developed countries to developing countries"
- Piling E-Waste is not only harmful for environment but to Human health. A study
 in 2018 found that in Guiyu China, E-waste was dumped in soil, water. The report found that
 traces of lead, cadmium and other heavy metals were found in human blood.





Why is Physical Data Destruction Unreliable?

- □ Data Leakage & High Security Risks
- ☐ Violation of Sustainability Goals
- Legal Complications and Hefty Penalties for Unsecure Disposal





Physical Data Destruction May Lead to Data Breach

2021 | Health Reach Community Health Centers' Data exposed in Maine

- Personal data of over 100,000 patients of HealthReach Community Health Centers' exposed in Maine.
- Incident happened due to improper disposal of hard-drives
- This led to HIPAA Non-Compliance and could attract a penalty up to US\$1.5 million.





Secure Alternative to Physical Data Destruction

Software Based Data Erasure aka Overwriting

The **Overwriting** technique is based on replacing the target data stored on all user addressable memory locations with non-sensitive data or binary patterns. Commercially, overwriting is also known as data erasure, which is implemented using specialized software tools.





Media Sanitization: Non-Destructive Technique NIST Special Publication 800-53 Revision 5 Cyber Security Framework

INFORMATION FLOW ENFORCEMENT | DATA SANITIZATION

When transferring information between different security domains, sanitize data to minimize [Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with [Assignment: organization-defined policy]].

<u>Discussion</u>: Data sanitization is the process of irreversibly removing or destroying data stored on a memory device (e.g., hard drives, flash memory/solid state drives, mobile_devices, CDs, and DVDs) or in hard copy form.

Related Controls: MP-6.





Advantage of Software Based Data Erasure

- Overwriting Ensures Complete Wiping
- ☐ Trusted Proof of Data Destruction
- Verifies Data Erasure
- Most Effective as is Prescribed by NIST, ISO 27001, and the likes
- Promotes Sustainability Goals and Boosts Circular Economy
- Helps Achieve CSR objective; Donate for Community well-being
- □ Cost Effective





Debunking Myths of Software Based Data Erasure

Myth 1: Formatting Permanently Sanitizes the Media

Myth 2: Deleting Helps Get Rid of Data

Myth 3: SSD Can Be Degaussed

Myth 4: Cryptographic Erasure is Full-Proof Data Destruction





Secure Data Destruction : Key Takeaway

✓ Promote Data Destruction over Device Destruction

- Helps Meet Regulatory Compliance
- Maintain Data privacy
- Promote Reusability
- Ensure Reputation management





Thank You



