Data Destruction Requirements in Today's Hyper-Risk Environment

The news is pervasive and affects companies worldwide, from small businesses to Fortune 500 enterprises. At any moment your security can be breached, your data stolen. Equifax lost nearly $2 billion in market capitalization in 2017 and its top executives were forced to resign.

End of use IT equipment

The accelerating pace of new technology introductions, shortened product lifecycles, and recent security breaches has re-ignited the IT Asset Disposal (ITAD) industry. As OEMs upgrade equipment to remain competitive, ITAD organizations are tasked with the safe and assured recycling or disposal of redundant or obsolete hardware to eliminate any possible risks to their clients' brand reputations.

The ITAD market projects a value of US$18 billion by 2024. The market grew from US$9.89 billion in 2015 and is estimated to expand at a CAGR of 7.1% during the forecast period from 2016 to 2024.

Fueling growth is the increased pace of hardware obsolescence as business requirements evolve to accommodate and run new apps. Though still in working order, processing speed and storage constraints pressure IT to regularly upgrade hardware to keep pace. The cost of maintenance and increased failure rates of older equipment increases downtime to unacceptable levels. Concurrently, hardware disposal has become a significant environmental issue. Laws and regulations that govern hardware disposal are evolving and vary by locale, adding complication.

What remains constant is the responsibility for data security in this hyper-risk environment rests squarely on the shoulders of IT.

"Washington State University hard drive theft potentially affects 1 million people."

-Healthcare IT News, June 19, 2017

End of IT Equipment Life Doesn't Mean the End of Data Risk

Re-purposing or physical disposal of hardware has never been more complex. In addition to computers and servers, "loose media" such as flash drives, disk drives and mobile devices are also sources of data exposure risk. IT managers must assume that any data resident on all hardware presents a security risk.

Asset management to track inventory and lifecycle costs of hardware requires a systematic foundation that informs IT managers of what, how, and when equipment should be re-purposed or disposed of when it comes to the end of its lifecycle. These decisions drive the cost efficiency of the entire IT supply chain and its final disposal process.

New Concern for IT: Company Image and Brand Reputation Risk

Safe and secure hardware disposal and data destruction is now a critical IT concern; secure end-of-life management of IT assets is a clear and present risk to company brand reputation. No longer buried in trade publications, data breaches are now widely headlined in the mainstream media, creating both business and brand image liabilities for IT executives and their organizations. Company data destruction is receiving increased scrutiny as part of an overall information retention management policy governing how information is securely maintained and how it is destroyed when IT assets reach their end-of-life.

Destroying proprietary and confidential corporate, personal, and customer data is an essential security step prior to hardware disposal or recycling. Criminal mining of data from improperly erased hardware can lead to serious breaches of privacy policies, disclosure of protected information, compliance problems, financial loss and added cost.

What is Trending Today: Rigorous Data Destruction Standards

> ***"Malware lets a drone steal data by watching a computer's blinking LED."***
>
> ***-Wired, February 22, 2017***

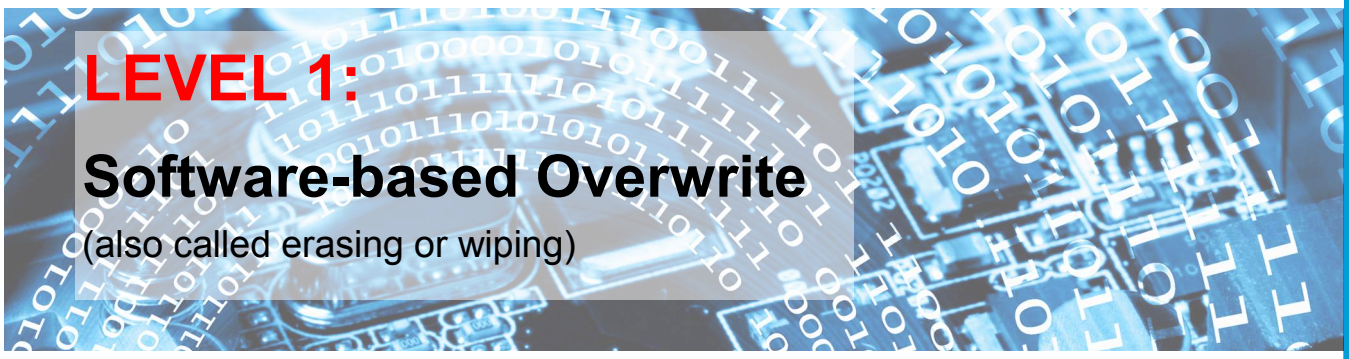
Data destruction standards and requirements vary by industry, but the trend is clearly toward higher levels of data protection utilizing increasingly secure destruction methods especially in financial services (PCI-DSS), healthcare (HIPAA) and defense sectors, where data exposure represents a great risk to the enterprise's brand reputation. Moreover, destruction of both data and hardware increasingly require compliance with certified proof.

Data Destruction: Four Proven Methods

Many companies now employ more than one method of data destruction when disposing of or recycling old hardware. Decisions to deploy one or more methods are typically determined by a company's risk tolerance and by the form of data residing on media.

While the four proven methods have not changed significantly, their level of precision and reliability has. Principally, regulations that govern treatment of data, which in turn affects each method's appropriateness, have become more exacting. Efficacy, cost, time spent, and documented proof of environmental and regulatory compliance are the new decision drivers. Financial services, defense, and healthcare industries are especially driven by increased public scrutiny resulting in stringent data destruction requirements.

Four Data Destruction Methods for Rotational Hard Disk Drives



LEVEL 1:

Software-based Overwrite

(also called erasing or wiping)

DESCRIPTION	PROS	CONS
Adds new data to the drive that replaces any encoded information with only zeroes or ones. <u>Four Common Variations</u> DOD 3 Pass (overwrites data 3 times) DOD 7 Pass (overwrites data 7 times) NIST Single Pass (comparable to DOD 3 Pass and acceptable in some industries) Gutman Algorithm (overwrites data 35 times)	Overwriting allows drives to be reused and/or resold. Semi-technical staff can operate the overwriting software. Clean. No debris as with physical destruction. No large capital investment needed. Can be performed prior to shipping drives off-site. Software overwriting tools are readily available in the open market.	Not possible on defective, non-operable drives. Cannot be performed on bad sectors. Secondary process (Level II, III below) needed for drives failing overwrite or containing bad sectors. Requires a robust process to confirm complete success of wipe on every drive. Unsuccessfully wiped drives are not visually identifiable from successfully wiped drives. As such, drives containing data can be mistakenly sold if not managed properly. Time consuming. A single pass may take several hours to perform. Larger and larger drive capacities are rapidly increasing the time requirements for overwriting. Storage arrays and related equipment can be more complicated than desktop and laptop devices, requiring skilled technical labor to perform overwriting. Requires periodic and random third party forensic data analysis to confirm overwrite software is working properly.

"Former Equifax CEO testifies before Congress."

-CNN, October 3, 2017

Four Data Destruction Methods for Rotational Hard Disk Drives

DESCRIPTION	PROS	CONS
Degaussing devices use a strong magnetic field that scrambles embedded data to point of unreadability.	If device is calibrated and working properly all data can be destroyed. Very fast. No mess. Non-technical staff can operate. Can be performed prior to hard disk drives leaving facility. Device can be used for multiple media types.	Complete data erasure verification is not possible. Hardware becomes inoperable. No proof data has *all* been wiped. Degaussed and non-degaussed hard disk drives are not identifiable without tagging and tracking. Requires investment in degaussing device(s), continued maintenance and calibration. Ineffective on newer high density drives. Ineffective on HAMR/MAMR drives.

Four Data Destruction Methods for Rotational Hard Disk Drives

LEVEL III:

Physical Destruction

DESCRIPTION	PROS	CONS
		Noise and debris can disrupt work-place or office.
		Data remains on pieces of destroyed hardware.
	Faster than overwriting.	Additional handling and destruction is needed.
<u>Two Methods</u>		Hard disk drives cannot be resold or reused.
	Cleaner than shredding. Limited particulate.	
Crushing/Punching Mechanical devices (hydraulic, electrical or manual) crush or deform the hard disk drive rendering it inoperable.		Noise, debris and dust can be diffi-cult to manage in an office environ-ment.
	Devices can be operated by non-technical staff.	
		Permitting can be time-consuming and cumbersome in some jurisdic-tions.
	Crushed hardware is easily identified by eye.	
		Shredders can be large, requiring additional square feet offices do not have.
Shredding	Faster than overwriting.	
Industrial sized paper shred-ders physically destroy hard disk drives.		Data remains on pieces of destroyed hardware.
	Shredder can be operated by non-technical staff with limited training.	
		Additional handling and destruction needed.
	Extremely difficult to retrieve data from shredded material.	Hard disk drives cannot be resold or reused.
		Possible environmental/ air quality issues.

Four Data Destruction Methods for Rotational Hard Disk Drives

DESCRIPTION	PROS	CONS
Hard disk drives are melted in furnaces and smelted back to elemental state (to metal form).	Complete and absolute destruction of data and hardware.	Media must be shipped to a refiner with proper equipment. Few refiners possess processing capacity at scale.

Which Method is Right for You?

Secure data destruction is a complex process. Deciding which method of data destruction to use requires a careful calculation of your company's IT asset mix, budget, time constraints, logistic requirements and environmental obligations. Collection and on-site packing, transportation logistics, including secure chain-of -custody, certification, remarketing, recycling, trade-in management, regulatory management, imaging, returns management and parts harvesting should play a part in your decision making.

Especially in the fields of healthcare, financial services, technology and value-added reselling, Sipi Asset Recovery offers the specialized know-how and deep technical knowledge to help clients master their unique business and compliance challenges related to digital asset management and secure electronic waste disposal.

Why Sipi Asset Recovery?

We understand the challenges you face for secure end-of-life data destruction and equipment disposition and have the deep technical know-how to advise you on the best strategies that maximize security, safety and value recovery. We are responsive, agile and innovative and believe that doing the right thing is just good business.

Contact Sipi's experts to learn more. Phone: (847) 750-9350 or visit www.sipiar.com

Sipi®
Asset Recovery
Earning Trust | Delivering Value®

Sipi Asset Recovery is a USA based, Woman Owned business focusing on helping organizations overcome the business, regulatory and environmental challenges of surplus technology. We carry certifications including R2, e-Stewards, HIPAA, ISO 9001, ISO14001, ISO18001 and PCI-DDS. We are a Certified Customer Service Organization who has earned the trust of large to small companies to provide IT asset disposition services ranging from onsite destruction, remarketing, donation and recycling. We're dedicated to earning your trust and helping tackle the unique challenges you face.

1300 W.N. Thorndale Ave., Elk Grove Village, IL 60007 | Follow us: