Phiston TECHNOLOGIES® INC.
Innovation, Ingenuity, Integrity

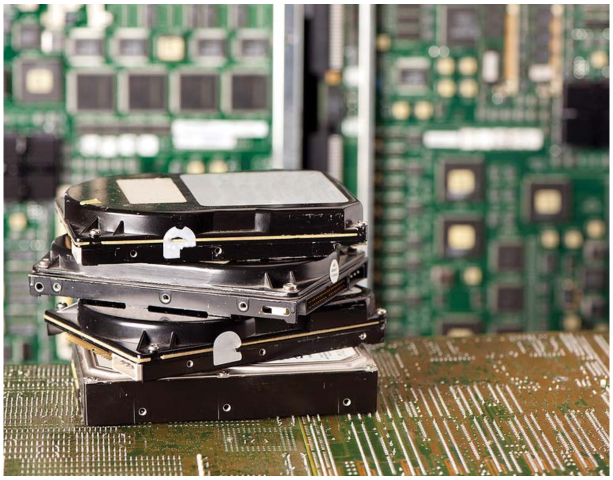
The Importance of In-House Data Destruction

Complete and permanent data deletion doesn't just happen when you empty your recycle bin. Learn more about the importance of in-house data destruction for your organization here.

ABSTRACT

Say you're looking to delete unwanted files on your hard disk to free up storage capacity for its redeployment. Or you want to discard it as it carries redundant or outdated data.

Whatever the case, it should be clear that you can't achieve permanent deletion of confidential files using simple commands like emptying the recycle bin. Well, at least not in this era where insider threats and corporate cyberattacks are increasing, and there is a growing risk of loss of sensitive information, costly fines, and damaged corporate reputation.



In other words, it's vital to consider data security throughout your entire company's data lifecycle, including its end-of-life. Especially given the need to comply with data security laws and regulations.

DATA SECURITY LAWS AND REGULATIONS

Regulations and legislation regarding data destruction are getting more strict each day. This is especially the case for organizations handling:

- Classified information and controlled unclassified information (CUI)
- Personally identifiable information (PII)
- Sensitive but unclassified information (SBU), or
- Information for official use only (FOUO)

The General Data Protection Regulation, for example, classifies data sanitization as a data processing technique. It also requires organizations that process personal data for EU residents to follow specific steps before destroying the data or the associated hardware.

For instance, data owners have the ultimate control over what should happen to their data – and data destruction is no different.

At the same time, companies must completely erase data on end-of-life devices instead of just deleting it. And destroy end-of-life hardware in a way that renders it completely useless! Think of the hardware stripped off its magnetic strips (degaussers, for instance, use powerful magnetic fields to destroy the information stored in certain media and also make the devices unusable) but also physically destroyed or broken apart using drive shredders.

Besides the European GDPR: most US states have data destruction laws, too. These typically require government or private entities to dispose of, destroy, or make personal information indecipherable.
Added to that is the Federal Trade Commission, which requires individuals or businesses that use consumer reports for business sake to dispose of the resulting data under strict guidelines. Electronic media and files, for instance, must be destroyed or erased in a way that makes consumer data unreadable. On their end, paper records must be burned, shredded, or pulverized.

Industry compliance regulations boast their own sets of data destruction instructions, too, which include rules on data sanitization, data shredding services, and more. As does HIPAA for organizations disposing of health-related information.

Now, these laws and regulations have varying restrictions. Some, like HIPAA, limit how long you can store sensitive data on certain operating systems. That means you may need to destroy data regularly.
Any non-compliance can attract hefty fines. For instance, not adhering to GDPR requirements can risk your organization a fine of £18m or 4% of the organization's global turnover, whichever amount is higher.

Non-compliance can also increase the risk of a data breach, further escalating the financial consequences of compensations and lawsuits. All while putting data owners at risk of fraud and identity theft.

When you combine compliance with the need to understand your data: where it lives, how widespread it is, the pieces that are the most sensitive, etc. And the need to safeguard the data under destruction from theft or compromise makes data sanitization a challenging task.

THE CHALLENGE OF DESTROYING DATA SECURELY

Data destruction is an increasingly vital task. And in a bid to mitigate in-house workload, companies are increasingly outsourcing data sanitization to third parties.

Unfortunately, relying on third-party solutions can expose the organization to data insecurity risks at multiple touchpoints within the data destruction process. In particular when transferring the data to the vendor's drive destruction facility.

There are many risks in retaining off-site sources for data and hardware disposition, too. In fact, some vendors don't destroy the IT assets as promised but sell them – sometimes to malicious players.

In one instance, journalism students from the University of Vancouver bought seven hard drives at $35 per drive from Agbogbloshie e-waste dealers. Agbogbloshie is a digital graveyard in Ghana, home to discarded electronic devices from the United States and other developed nations.

In just seven drives, these students found bank statements, social security numbers, credit card numbers, and other personal information. They also retrieved a highly-sensitive $22m US defense contract in a drive, which also had contracts with Homeland Security, NASA, and TSA.

In 2003, two MIT graduates bought 158 hard drives from eBay, small salvage companies, etc. Upon investigation, they found that 49 of those drives contained sensitive information, including medical data, corporate financials, PII, and more than 5,000 credit card numbers.

In 2006, Idaho Power Company discovered that 84 of the 230 drives they had contracted Grant Korth, a salvage vendor, to sanitize had been sold to parties on eBay. Yet, those drivers contained sensitive information, such as confidential correspondence, proprietary company information, and employees' data.

In 2009, Kessler International bought 100 hard drives from eBay for six months. Upon investigation: they found 40% of the drives to contain sensitive information.

The list is long.

And goes to show that many companies trust third-party solutions to do as they promised. Unbeknownst to them: the number of reputable data destruction companies is declining. As more vendors are driven by greed. Some even offer to recycle personal computers for free, only to sell them to cybercriminals.

Then there's the human error. For instance, Morgan Stanley was 2020 alleged to have breached their clients' financial information. That's after their data sanitization vendor misplaced several computer equipment storing customers' PII.

It's therefore not a wonder that a recent ZDNet study found that 59% of second-hand or refurbished hard drives on online marketplaces have identifiable data of the previous owner or data center.

Add that to the growing cyberattacks on third-party vendors. As criminals target companies that deliver data destruction services to multiple entities, to increase the amount of information they can harvest from one source.

All the while, organizations remain fully liable for the data they process, and no amount of third-party mishaps can deflect liability.

THE SOLUTION: IN-HOUSE DATA DESTRUCTION

All data, including CUI, PII, FOUO, and SBU, should be destroyed at end-life on-site, with adequately rated equipment. this link is broken

Here are additional reasons to destroy data and associated IT devices in-house:

Control over the destruction process

Sensitive data controlled by the government or private organizations should be accounted for at all times. That means going beyond keeping it safe to document what your organization has done to safeguard data erasure.

Such measures can quickly become cumbersome when your organization manually tracks decommissioned hard disks. For example, by monitoring their processing before shipment, tracking them during shipment to the vendor's destruction facility, and confirming they have been wholly obliterated.

In-house data destruction processes can ease the documentation by removing:

- Third-party stakeholders.
- Invisibility issues associated with relying on an outside partner to destroy a hard drive or delete data.

From a regulatory compliance perspective, gaining control over the data being destroyed is helpful. But it also makes it easier to safeguard against insider threats.

Sure, persons in your organization can still access decommissioned IT assets, but you limit that possibility. Instead of being in the dark, not knowing who handled your decommissioned hard disks at what point in time increases the risk of insider threat.

Plus, it's easy to monitor and safeguard disposable IT assets when dealing with a few of them. Unlike a disposition vendor who is handling 1000s of such daily.

Certificate of destruction

You have multiple options when it comes to destroying data. However, they all function differently.

For instance, physical destruction is ineffective if the IT asset is not shredded completely. (As any access to substantial parts of the decommissioned hardware can allow malicious players to recover data.) It gets worse in data destruction software data wipes, as those are more vulnerable to leaving recoverable data.

Yet, inferior destruction methodologies, human error, and other problems can slip in: if your organization fails to vet the data disposition company they partner with properly.

That makes it upon you to ensure they have the right sanitization tools and expertise to destroy all the decommissioned IT assets – it could be hard disks, USB sticks, or smartphones. You should also check that they have a solid reputation in your niche and provide genuine certifications from government agencies, such as NAID AAA or GSA Schedule 70.

Then again, keeping the destruction process in-house helps eliminate these shortcomings because you can verify proper deletion every step of the way.

Keeping end-of-life budget under control

Subscribing to services, as opposed to spending money on hardware, has revolutionized the IT world. However, the long-term costs of such hard drive data destruction service subscription services can add up to more than the cost of buying a hardware solution.

Take degassers, for example; such a durable machine can help you recoup the purchase price in no time: by saving on data disposition service subscriptions.

FIND A REPUTABLE DATA DESTRUCTION COMPANY EQUIPPED TO HANDLE YOUR DATA DESTRUCTION NEEDS

Protecting your organization from corporate data breaches and insider threats is relatively easy with the right policy and tools in your arsenal.

At Phiston Technologies, we believe in proactive product development, agile innovation, and secure site data destruction – as evidenced in our no-hassle yet effective hardware crushing machines.

We take pride in being one of the best data security and data destruction companies firms in the US: Serving Facebook, LinkedIn, IBM, Amazon, Verizon, and more. Contact us today to learn how we can help you destroy data in-house: to prevent all the pitfalls of using third-party disposition companies.

THE PHISTON ADVANTAGE

At Phiston Technologies, we believe in innovation, proactive product development, and secure destruction of data.

Our goal is simple: destroying your media to preserve and promote data security. We build products to ensure complete media destruction.

As data storage continues to evolve, so will the need to advance current data destruction products. Phiston will always be ready to provide security solutions to keep your organization safe and in compliance.

Phiston as a company is a leader in end-of-cycle media destruction and has various products that can handle all. Our clients include some of the largest tech companies in the world, and our devices are deployed across all 50 states and in 49 different countries.