Blank is change

Take a look at the top two contenders for end-of-life data security—and be more fully informed about your options.

"Blancco defines data sanitization as the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable—a definition in line with Gartner's Hype Cycles."

Let's look at the risks and considerations when choosing how to best secure data on your no-longer-wanted IT storage assets.

In its landmark 2022 article, "Why Big Tech shreds millions of storage devices it could reuse," the Financial Times investigated global data center growth, organizational policies—and the routine destruction of related data storage assets.

Their findings?

Largely motivated by the fear of data leakage and data privacy violations, IT leaders worldwide—including cloud providers—contribute to an immense amount of drive destruction in the name of data security.

And it's no wonder.

IBM recently reported that the average cost of a data breach exceeded $4M in 2023. Yet that's dwarfed by a device disposal breach that resulted in more than $90M in fines alone, not including millions more in a hefty legal settlement.

Yet today's businesses regularly put their data at risk at this stage. Often, data protection processes are outpaced by the technologies they're designed to protect.

In an era of escalating data consumption, **blank is change**. More importantly, it's effective.

Here's how it holds up against traditional practices—and how you should use it to protect your data.

Drive Destruction vs. Data Erasure: Which Data Disposal Method is Most Secure?

Drives that have been used in a highly protected and confidential information system will need to be retired eventually, even if the data on those drives gets transferred to another storage device.

In this situation, making stored data permanently inaccessible will be critical during the decommissioning process.

How do you make sure your highly sensitive data is completely destroyed at end-of life? We take a look at physical destruction methods such as shredding and degaussing, as well as secure data erasure.

Decommissioning drives with confidential data? Select the right data disposal method for your business.

Properly sanitizing the data from your used desktops, laptops, servers, loose drives, mobile devices, flash drives, or any other storage device is absolutely critical when it comes to decommissioning, no matter what the end destination (Redeploy? Sell? Donate? Recycle?) is for those devices.

That's because even if the once-valuable data is completely obsolete or trivial to your organization now, it can still offer a goldmine for hackers and **black market data brokers**.

Whatever the catalyst for drive disposal, an organization risks data leakage if data can be found or reconstructed from **discarded storage devices** or their components.

That could lead to heavy fines from regulators. It can breed lawsuits by those affected. There's also the risk of financial loss and reputational damage.

Three types of sanitization: which data destruction method is right for you?

Blancco defines data sanitization as the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable—**a definition in line with Gartner's Hype Cycles**. A device that has been sanitized has no usable residual data. Even with the assistance of advanced forensic tools, the data will not ever be recovered.

According to Gartner, there are three methods to achieve data sanitization:

- **physical destruction,**
- **cryptographic erasure**, and
- **data erasure**.

We address the pros and cons of cryptographic erasure in our white paper, "**The Crypto Erase Conundrum: What's Your Organization's Risk Tolerance?**" But in an era where shredding drives and degaussing are often the "go to" methods of final drive destruction, how do you know the best sanitization method for your organization—and whether to choose between physical destruction or data erasure for your most sensitive information?

Determining how much data protection you need

If you've already determined that your data storage devices require the utmost in protection at end-of-life, feel free to jump to the **end of this article** for our recommendation on how to treat your storage devices at that time.

Otherwise, to determine how secure your data disposal processes need to be and whether to choose data erasure vs. physical destruction, consider the following:

- Data confidentiality and impact
- Persistence of data sensitivity
- Drive or device final destination
- Determination and capabilities of your adversary

Data confidentiality and impact

Data security rests on three fundamental objectives: Confidentiality, Integrity, and Availability.

Among other places, these are outlined in the U.S. document, Federal Information Processing Standards (FIPS) Publication 199, "**Standards for Security Categorization of Federal Information and Information Systems (PDF)**."

Created in response to the Federal Information Security Management Act (FISMA) of 2002, this publication from the National Institute of Standards and Technology (NIST) weighs each of these three attributes according to risk of impact (low, moderate, high) when determining the amount of data protection needed.

For instance:

- If sensitive data is accessed inappropriately, does this breach of *Confidentiality* have a low, moderate or high level of impact to the organization or its stakeholders?
- If the data is falsified, used to misdirect users to imposter websites, somehow destroyed or the *Integrity* of the data is otherwise compromised, what is the level of harm that could result?
- In the cases of websites going down or denial of service attacks, what is the level of impact when data *Availability* no longer exists?

When it comes to end-of-life data protection, *Confidentiality* is the chief concern. This is particularly true when unauthorized data exposure could cause great financial loss, brand damage, or other harm if made available to the wrong people.

Persistence of data sensitivity

Will the sensitivity of your data quickly age out?

The NIST SP 800-88, Rev 1, "Media Sanitization Guidelines" recommend that, for disposition decision making, "it is important to understand what types of data may be stored on the device in order to apply the techniques that best balance efficiency and efficacy to maintain the confidentiality of the data." Also, "the length of time the data will remain sensitive should also be considered."

Just because the data is sensitive now, will its value diminish quickly enough that it will soon be worthless to nearly everyone?

Or will the information you need to protect still be considered high-risk or highly confidential for months or years to come?

This can be important to consider as data recovery techniques advance. More sophisticated data recovery tools and skills will also become more commonplace. These factors may also influence whether you want to meet or exceed bare minimum regulation requirements.

For data that will remain sensitive or valuable for some time, you'll want to know that you've successfully removed all data from devices and device fragments for both now and in the future.

Drive or device final destination

When it comes to high-risk data storage, moving devices from a more securely protected data environment to a lesser one is risky.

Typically, even if the data on an old drive has been previously declared confidential, if the drive is to be reused within the same organization, the risk of data exposure to external parties is lower than if the drive was reused externally. Even so, if the drive is to be redeployed in-house, it still must be thoroughly sanitized in a way that protects the data while preserving the life of the drive.

This allows a drive previously used by say, the finance department, to be redistributed to a different department without fear of employee salaries and bank account information being exposed internally.

However, once drives leave the organization, the organization is no longer in control of any potential data access. Any residual data may be exposed long after the organization has relinquished it to other owners.

Determination and capabilities of your adversary

The truth is, any of the three data sanitization procedures—data erasure, cryptographic erasure, physical destruction—will protect your data if executed properly from the beginning to the end of the process.

Costs, environmental impact, and the ability to reuse your devices will differ, of course. But for any enterprise especially concerned about protecting data at end-of-life, trouble occurs when any of these data disposal methods are performed incorrectly.

At that point, data sanitization remains incomplete, and data is still recoverable by someone with adequate know how and the right tools.

The value of your data, how much of a target your organization's data may be, and the capabilities of those who would benefit from your data must also be considered as you weigh your risk and choose your data disposal methods.

Subversive data access methods can be divided into two primary categories:

1. A more basic approach ("ordinary means" according to NIST) that allows keyboard access via a standard hardware interface or

2. A more advanced approach ("extraordinary means") that uses forensic or laboratory techniques.

With the most notorious data access crimes committed by well-funded teams of malicious actors (rogue nation states, crime syndicates, etc.), advanced data recovery using extraordinary means can be a very real possibility if your data is valuable.

A look at physical destruction

So how do you ensure that your highly sensitive data is undoubtedly, permanently, and completely protected from the moment of device decommissioning?

The answer: Use a combination of physical destruction and secure data erasure for end-of-life drives that have stored your most confidential, high-risk data—but only if sustainable reuse truly isn't an option.

Over a third (35 percent) of organizations physically destroy end-of-life IT equipment because they believe it is "better for the environment." But is it? **Read: Technology Recycling Vs. Reuse**

With e-waste continuing to be an issue worldwide, and global data consumption accelerating, reuse is the most sustainable option when it comes time to retire data storage devices.

With the right methods and levels of software-based sanitization (data erasure), data is permanently rendered inaccessible while leaving the device intact. This prevents usable devices from prematurely heading to landfill, something physical destruction cannot do.

But there are other drawbacks to physical destruction that can also make it a less secure option.

Effective and ineffective physical destruction

Done correctly, physical destruction is a valid data disposal option. It can sometimes be the only option for damaged drives and devices.

But it's unnervingly easy to take missteps or leave gaps that can put your data at risk. And, with data being stored at ever greater densities, commonly accepted, so-called "military grade" physical destruction techniques are rapidly falling out of favor.

Degaussing

Intended to demagnetize hard disk drives (HDDs), degaussing doesn't apply to solid-state drives (SSDs)—at all.

So, if you send a batch of drives for degaussing assuming they're all HDDs, you may unwittingly send several SSDs (or hybrid drives with SSD components) laden with sensitive information along with them. The result? When finally disposed of or recycled, the SSDs will still have all their original data.

What's more, not all degaussing machines are adequate to the task of demagnetizing all HDDs. If using this method at all, we recommend checking for degaussers approved by your region's security authorities (e.g., the NSA publishes NSA/CSS Evaluated Products List for Magnetic Degaussers)—and being diligent about separating drive types. You'll also want to make sure your degaussers are new enough and capable enough of addressing the drives you have.

Degaussing will render the drives unusable. However, note that even with approved degaussers, the NSA recommends additional destructive methods in combination with degaussing to achieve true sanitization.

Shredding, pulverizing

While HDD destruction can be accomplished with larger shred sizes, the ever-increasing data density of SSD chips means that larger pieces can harbor readable, accessible data, especially if chips are left intact.

Keeping up with such data storage evolution is one reason the globally renown IEEE Standards Association developed a new data storage sanitization standard.

As of the August 2022 release of **IEEE 2883, "IEEE Standard for Sanitizing Storage**," shredding and pulverizing are considered obsolete methods of sanitizing high-density drives.

So, while the requirements below may still be in effect in policy documents, shredding and pulverizing on their own may not provide adequate protection for your top-of-the-line, data-dense data storage drives, particularly as technologies continue to advance.

For those organization that require shredding or pulverizing, there are some important measurements and tactics to keep in mind:

- For shredding, the U.K.'s National Cyber Security Centre advocates a particle size of 6mm, while the U.S.'s National Security Agency advocates an even smaller shred size of no larger than 2mm—the size of the edge of a U.S. nickel.
- Even with hard disk drives, the NSA maintains the 2mm maximum shred size before disks can be considered sanitized.

For all drive types, the idea is to shred small enough so that recreating the data from fragments would be infeasible. Additional security comes from mixing the particles with those of other drives.

IEEE 2883 does include melting or incinerating as legitimate, fully effective forms of drive sanitization and data protection.

"IEEE 2883…obsoletes the shred and pulverize methods of the Destruct sanitization method. Strong warnings are added for using degaussing method of Destruct." — SNIA Storage Security Summit 2022: IEEE™ 2883 – Sanitization of Storage

Other physical destruction risks

Whatever physical destruction method chosen, there are still other operational vulnerabilities, even if the correct data disposal processes are followed precisely for each drive type.

For instance, in any physical destruction scenario, unless you have rock-solid chain of custody measures in place, **you introduce risk of loss or theft** by leaving devices in storage until they're finally handled, or by giving a third-party data destruction service access to your devices.

Whether destruction is conducted at your facility with mobile shredders or degaussers or transported to an IT asset disposal (ITAD) facility for ultimate physical destruction, there's risk in relying on this method alone since there are many points of vulnerability, including people and process vulnerabilities and the risk of loss or theft.

One way to do this is to carefully vet the vendors providing drive destruction services, from

- ensuring secure transit of drives,
- checking for adequate staff clearance,
- providing a clear audit trail of each device from receipt through sanitization and to disposal,
- ensuring that all equipment is in good working order, and
- ensuring all staff is well trained in the correct drive destruction and verification processes.

Applying these practices when looking for a data destruction vendor will help ensure that you've minimized the chances of data being susceptible to breach and provided you with the assurance that you are working with a reputable vendor that is highly expert in protecting your data.

Combining physical destruction with secure data erasure

Physically destroying hard drives, computers, mobile devices, and other storage devices is viscerally satisfying.

While **data erasure has been proven both secure and effective**, fully able to completely eliminate data without destroying the device itself, there's something reassuring about seeing drives mangled beyond recognition.

However, because subpar physical destruction processes can leave data vulnerable, it's still wise to first perform secure and complete data erasure on any device used for confidential data—even if you intend to shred, pulverize, or recycle the drive or device rather than reuse it.

Because subpar physical destruction processes can leave data vulnerable, it's still wise to first perform secure and complete data erasure on any device used for confidential data.

However, this "belt and suspenders" approach incurs several needless costs: time, money (both processing and replacement costs), and waste.

Using data erasure alone

With automated data erasure, especially if performed at the point of decommissioning, you can safely retire storage assets, no matter the final destination, without fearing human error, unintentional loss, or deliberate hacking.

But after devices have been certified and verifiably erased, secure device reuse is a real option.

The effectiveness of software-based data sanitization

Whether redeployed internally or externally, verified software-based sanitization renders data inaccessible, extends the life of IT assets, keeps functional devices out of landfill, and extracts more value from your IT investment.

After 25 years of sanitizing drives and devices with Blancco software, millions of erasures, rigorous and regular testing by third-party organizations, and a record of zero breaches, the effectiveness of data erasure in protecting against illicit data access is proven.

Also, because software-based data sanitization can be launched immediately across thousands of devices at a time and even **remotely**, you can use it to protect your data right at decommissioning for even large-scale projects.

This reinforces your chain of custody and shields your sensitive information throughout any transit or storage time. The data is simply no longer accessible by anyone.

Removing confidential data through software-based data erasure can happen in live environments or be applied to hundreds or even thousands of drives onsite:
Top Technology Company Erases 4,000 Servers Simultaneously Case Study - Blancco

Ineffective alternatives

One caution:

There are also faulty implementations of "**wiping**" data from hard drives: Overwriting may not reach all sectors (they may be hidden or damaged) or manufacturers' built-in sanitization processes may not be implemented correctly.

Lesser attempts at removing data, such as **reformatting** or simply deleting files, are completely inappropriate for even slightly sensitive data. With these methods data can be recovered fairly easily.

Just as care should be taken when selecting a drive destruction provider, it's important to choose your erasure software-based data destruction solution carefully, and insist on both erasure verification and an audit-ready, tamper-proof report. The report will identify each drive and the method and level of erasure used, among other details critical to chain of custody and compliance reporting.

So, what is the most effective method of data disposal?

Blancco data erasure software has been tested, certified, approved, and recommended by **14+ governing bodies** around the world. Our data erasure software **erases to 25+ standards** and provides certificates of erasure to meet security and regulatory compliance requirements. And, **our patented SSD solution** handles functionality differences across a myriad of SSD vendors.

We are confident that **Blancco data erasure solutions** provide all you need for permanent, secure data sanitization, rendering your data completely unrecoverable.

And, because the drive or device remains physically intact, Blancco data erasure gives you the ability to redeploy your data storage assets—and **operate more sustainably**—without fear of data leakage at any time.

However, if your organization mandates or prefers physically destroying your old data storage devices, weigh your destruction methods and vendor options carefully. Then, use the points in this article to advocate adding data erasure as an extra layer of protection against future data access.

Experience Proven Security at Device End of Life

At Blancco, we have enterprise-scale solutions that permanently and completely eradicate your data, getting your devices and environments completely blank—with or without physical destruction.

Start your journey to blank now.

Visit our content hub