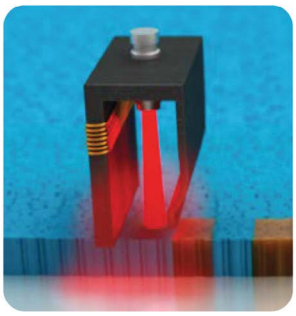
Phiston TECHNOLOGIES® INC.
Innovation, Ingenuity, Integrity

Why Degaussers are Becoming Outdated

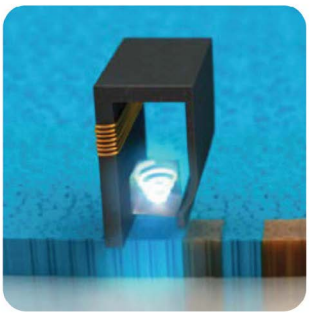
Degaussers provide an excellent way to erase confidential data from storage devices. But is this method becoming outdated? And what are the alternatives?

ABSTRACT

Degaussing is a commonly used method for overwriting data and erasing it. Unlike shredding, disintegration, or melting, degaussing a hard drive won't physically destroy it. Still, this secure data destruction technology assures sensitive data is erased in seconds and in an environmentally friendly way (as the devices are made easier to recycle).



HAMR



MAMR

However, degaussers do not work on all media devices, as they can only be used on magnetic storage media, and the NSA no longer accepts machines with magnetic fields less than 30,000 Gauss.

In this article, we will explain how a degaussing machine work and evaluate whether they are becoming outdated. We will also present a few suitable additional methods you can combine to ensure data security and compliance.

WHAT IS DEGAUSSING, AND HOW DOES IT WORK?

Degaussing demagnetizes or neutralizes the magnetic field that is used in data storage. This can be done to any magnetic media devices, such as video tapes, hard drives, or floppy discs.

Although there are various types of degaussers, they all work as follows: A degaussing coil passes through a controlled and powerful magnetic field. This process rearranges the magnetic particles (or changes the magnetic domains) within the hard drive or storage device, making the information unrecognizable and unrecoverable - thus erasing all previously saved sensitive data.

The degaussing process doesn't just wipe off the data that is stored in a device; it also damages the servo data that the hard drive needs to make the read/write function work (or the startup files). As a result, you cannot reuse a hard drive once it's been degaussed.

DEGAUSSING PROS AND CONS

Degaussing remains a popular method for wiping out data from electronic devices (particularly those holding sensitive data or top secret data). However, as with any method, there are pros and cons to it. Let's go through them in some more detail.

Advantages of Degaussing

Degaussers ensure that all sensitive information is erased permanently. When used correctly and on the correct drives (magnetic media), the degaussing process is 100% reliable. In fact, the NSA recommends degaussing and destruction as the two main methods you can use for data removal. The whole process can also typically be completed in just seconds.

Because magnetic media is considered challenging to dispose of, using a degausser is also more environmentally friendly than, for example, shredding. For one, because there are fewer toxins being emitted, but mainly because the recycling process is made easier by not physically destroying the device. A shredder will break up the HDD and mix up all its materials, such as PCB, metals, and plastics. Degaussing doesn't change the physical appearance of the HDD, making these materials easier to separate and reuse.

Downsides of Degaussing

The main downside of using a degausser is that the method is only effective for magnetic media. This means that you cannot use a degausser for solid-state drives (SSDs) and there's a question about its effectiveness for HAMR and MAMR drives. So, as a media sanitation technique, it will only be successful if you use it for the correct media type.

For degaussing to be 100% effective, you will also need to use two to three times the energy rating of the device you are trying to sanitize. In other words, the stronger the magnet used for degaussing, the better the data destruction. If your permanent magnet is not strong enough, fragments of data might remain.

ARE DEGAUSSERS BECOMING OUTDATED?

To understand whether or not degaussers should still be considered an effective way to deal with sensitive data stored in an electronic device, we should first see how storage methods have changed over time.

Nowadays, most tablets (and more PCs) do not use hard drives but flash memories. This involves very different requirements and considerations when it comes to decommissioning them, as you cannot degauss an SSD or newer drives, such as HAMR and MAMR. Even though the National Security Agency accepts some overwriting procedures for data sanitation, most compliance regulations will still state you need to destroy the media.

Now, there's another issue with SSDs, and that's that they are difficult to wipe out completely. This is due to the fact that SSDs have an area specifically dedicated to load-balance memory cells. This area can be large but also invisible to the operating system. So, the only way to guarantee it's not still storing confidential or proprietary data is to physically destroy the drive.

When it comes to making sure any information is made 100% irretrievable, no matter the storage device, it's best to have redundancy. So, rather than asking whether degaussers are becoming obsolete, it's better to evaluate how they can be combined with other methods to guarantee data destruction. This is also what the NSA supports. First, degauss the device. Then, make sure the storage device is physically destroyed.

PHYSICAL DESTRUCTION AND OTHER ALTERNATIVES TO DEGAUSSING

There are several methods businesses can use to destroy a storage device physically. Let's go through them in some more detail.

Hard Drive Shredders

Shredders (or heavy-duty electronic media shredding machines) are designed to physically destroy hard drives by completely griding up and destroying all of their parts. This process can deal with hard drives, cassettes, CDs, and other devices and makes the information previously stored in them irretrievable. Hard drive shredders are highly specialized machines. Some shredding machines also compact the resulting material so they are easier to dispose of.

Hard Drive Disintegrators

Heavy duty disintegrators are designed to destroy large amounts of material. They can break down hard drives, CDs, microfiches, magnetic tapes, and other devices into 3 mm particles - thus making them impossible to reconstruct or read. These machines, which have a conveyor system and a knife that slices the devices into small particles, are especially useful for destroying solid-state devices. However, it's important to make sure these particles are handled correctly, as they can be poisonous to both humans and the environment. Disintegrators should always be installed in well-ventilated rooms.

Hard Drive Incinerators or Melters

Incinerators can melt devices (this can be done by using steel smelters that can reach 2,500°F or dipping the hard drives in acid). Although this method can destroy SSDs, flashcards, and others, the substances used are highly toxic and dangerous to the environment and humans. Of all the physical destruction methods mentioned in this list, incinerators are the least advisable and most unsafe.

THE IMPORTANCE OF DESTROYING MEDIA FOR COMPLIANCE

Several organizations must abide by compliance regulations when it comes to erasing data. After all, cybercrime is a concern for anyone using technology - and this is even more important for government agencies and businesses that need to deal with sensitive information. In some cases, not abiding by this law can actually be considered a crime, so it's important to always ensure the data is completely erased. Do-it-yourself methods for hard drive destruction are both dangerous and expensive. The efforts to deal with large amounts of devices can be considered unreasonable for many companies, plus the shards from broken-down drives can cause serious injury.

Since there is a prevalent concern about data security (and how to deal with solid-state drives, in particular), it's best to consider using multiple methods to ensure the data is really destroyed.

CONCLUSION

Degaussing a hard drive is an excellent way to ensure data security. However, you should keep in mind that degaussing won't work with SSDs, HAMR and MAMR drives, laptops, and tablets because these devices use electronic charging to store information. So, using a hard drive degausser on them would have no effect.

To correctly sanitize an SSD, you're left with two options: Using software (which usually won't comply with data security regulations as it's not 100% foolproof) or physically destroying it using shredders or disintegrators. It's important to mention that none of these methods should be carried out without supervision because they are subject to regulation and can be highly hazardous.

To answer the question of whether degaussers are becoming outdated - we can say there's definitely a tendency towards using more SSDs and newer drives that cannot be degaussed. Thus, this method will only be effective if combined with other physical means of destruction.

When choosing whether to use a degausser or not, first look at the type of media that needs to be wiped. Then, make sure you use a degausser with enough power to erase a hard drive. Lastly, consider exploring other additional methods like shredding or disintegrating.

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.