WHITE PAPER

proton™
DATA SECURITY

Degaussing 101

State of Cybersecurity

How did physical data breaches become such a threat to businesses? Consider this — on average, 1 out of every 4 hard disk drives will fail after the first four years of use, a Backblaze study reported.

With such a rapid rate of retirement, it can be difficult for large organizations to keep up with recycling these electronics. They're often relegated to bins in data centers, with all their data still on them, waiting to be picked up by a third party to be disposed of.

Unfortunately, employees don't always follow protocol and sometimes devices end up in the trash or in vendor's hands with data still on them. Third parties aren't that much more reliable, as many data breaches have resulted from service companies not properly erasing information from media once it's in their possession.

It's best to sanitize media "in-house" before releasing to a third party for disposal. Degaussing has been tried and tested by the National Security Agency as the only way to safely erase data from magnetic media, yet it doesn't always get the recognition it deserves.

Understanding Hard Disk Drives and Tapes

When it comes down to it, employees often fail to recognize the amount of information stored in just one hard disk drive – and how difficult it is to sanitize it. There are three common routes organizations take to delete data from retired electronic media:

- Software wipe/overwrite/reformat.
- Moving files to the recycling bin.
- Physical destruction.

Technologies are always rapidly changing and we don't yet know what trove of data future hacking methods will unveil.

These drives contain platters which have a special magnetized coating that allows users to read and write information, as well as retrieve it whenever needed with no fear of losing the data. Each device possesses a specific magnetic field strength, otherwise known as coercivity. Coercivity is measured in Oersteds (Oe) and identifies the magnetic field intensity required to "demagnetize" a hard drive and bring it back to a zero or blank state, thus erasing the data. This necessitates the need for a strong degausser, because anything below the required amount necessary will not effectively or totally erase the data.

Coercivity makes data on hard drives resilient and inhibits software or physical destruction from completely rendering data unreadable, because once magnetized, a hard disk or tape will always retain the information until it is demagnetized or degaussed. This is why these three options never truly work.

Basically, if skilled computer forensics lab were able to analyze a disk overwritten with software or were able to find any small piece of magnetic media they could retrieve millions of bytes of information stored on it. Since technologies are always rapidly changing and we don't yet know what trove of data future hacking methods will unveil, degaussing is the only way to ensure this information is forensically unrecoverable.

It's easy to see why these common methods of data erasure don't work—they fail to demagnetize the media. Software wipes and reformats simply move the data around or cover it up with code so it's more difficult to find, while physical destruction leaves the door open to the idea that residual data can be found and extracted from a small portion of the disk or tape.

What Does Degaussing Do?

In terms of permanently erasing data, none of the aforementioned options suffice, and much of the reason has to do with the composition of a hard disk drive which makes data extremely difficult to erase.

Data can only be truly erased by applying a reverse magnetizing force, known as degaussing. This is when a degausser, which can utilize either permanent magnets or electromagnetic pulses, exposes the magnetic media to a strong magnetic field, measured in Gauss or Tesla (10,000 Gauss = 1 Tesla). Each unit essentially chips away at the magnetic coating until the drive is left in an entirely blank state. According to the NSA, current hard disk drives have a coercivity of up to 5,000 Oersteds and tapes have up to 3,000 Oersteds. In order to ensure complete erasure they need to be exposed to a strong magnetic field. A general rule of thumb is a Gauss force of at least 3 times the media's coercivity. So a 5,000 Oersted hard drive would require 15,000 Gauss (1.5 Tesla) which a reputable degausser can produce. Of course, along with the data, prerecorded factory information like the servo tracks are also erased which will render the device unusable, which is the goal.

2 in every 3 IT teams believe employee negligence, such as insider threats, is the most common source of a data breach.

The degaussing process is also much shorter than that of a reformat or software wipe as well, as the most powerful degaussers on the market that apply up to 20,000 Gauss can render magnetic media completely unreadable in less than one minute. Former methods can take hours to complete, and in the end, leave organizations vulnerable to having their data stolen. It's also important to remember these insecure methods require the hard disk drive to be operational—since every 1 in 4 drives fails to live past four years, this is often impossible. This means if a company relies on software to erase data, they'd be out of luck in this scenario.

Many companies leave retired electronics in storage bins in a data center or locked room because they either don't know how to dispose of them correctly, or they're waiting for a third party to get rid of them. Both options make a company vulnerable to data theft, especially from an insider which poses the largest threat. According to one study by Experian, 2 in every 3 IT teams believe employee negligence, such as insider threats, is the most common source of a data breach. It just takes one misplaced drive that contains Terabytes of information to fall into the wrong hands before a whirlwind of legal consequences form.

With degaussers, businesses can quickly and efficiently demagnetize media as it's retired. This allows them to take control of their data protection methods, rather than leave it in someone else's hands.

Most Effective Data Erasure Method

Why is it so important to have a secure procedure for erasing data in place? The financial consequences that can be levied on organizations that fail to protect client data are staggering, and can have a detrimental impact on revenue.

Laws like the Gramm-Leach-Bliley Act can fine a financial institution 1 percent of its total assets. The Health Insurance Portability and Accountability Act can charge health care organizations $50,000 to $250,000 per violation, depending on the severity of negligence. Each lost record is considered a violation, meaning one lost hard drive could multiply a potential fine thousands of times. All in all, the following laws all require electronics that once stored consumer information be securely sanitized:

A combination of degaussing and crushing provides a potent one-two combo for data security.

- GLB Act.
- HIPAA.
- National Institute of Standards and Technology Guidelines for Media Sanitization.
- Payment Card Industry Data Security Standard.
- Fair and Accurate Credit Reporting Act.
- Federal Information Security Management Act.
- Personal Information Protection and Electronic Documents Act.
- Sarbanes-Oxley Act.
- Family Educational Rights and Privacy Act.

It's entirely evident that degaussing enables organizations to take control of data protection within their ranks and move away from third-party services, but what's the best way to act upon this? A combination of degaussing and crushing provides a potent one-two combo for data security.

By first demagnetizing the media, then physically destroying it, organizations can rest assured knowing their information cannot possibly be recovered. Smashing a tape or hard disk drive into tiny pieces doesn't necessarily make the device more secure, as degaussing is proven to be effective on its own, but it does create a visual deterrent and provides peace of mind.

Conclusion

In a digital world, data can be considered as valuable as gold, yet is too often treated as worthless as trash.

Roughly two data breaches occurred each day in 2015, according to the Identity Theft Resource Center, and the California Dental Association reported the most common type of data breach in the medical industry is a physical breach.

While many IT departments focus on active threats like viruses and malware, it's often passive instances that do the most damage. Leaving a functional hard disk drive out in the open, or failing to sanitize electronics before they're thrown away can create a nightmare scenario for any well-run business.

Organizations that take the time to explain the dangers of software wipes, reformats and physical destruction before degaussing to those involved with the sanitization and disposal of retired electronics will ultimately see a return on their invested time through a less likely risk for client information to be leaked or stolen.

When it comes down to it, does your business want to leave its livelihood and data protection in other people's hands? Degaussers allow organizations of any size to take control of their data sanitization procedures and immediately erase data from electronics, removing all likelihood of a data breach from the equation.

Interested in adding degaussing equipment to your IT team's tool bag? Contact Proton Data Security Inc. today to learn what type of degausser fits your company best.

proton DATA SECURITY

(888) 881-9000
info@protondata.com