Don't Give Away Privacy! A Degausser FAQ

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for May 2008 CSI Alert

Is Computer Disposal Too Unsexy To Think About?

The topic of my recently completed spring issue of "Protecting Information" was "Information Disposal." While doing the research for it, and talking with information security folks, one of them told me the topic of information disposal is not sexy enough to put many resources towards within most organizations. Another information security officer asked me, "What's new to think about? Nothing has changed with disposal issues over the past decade."

Granted, thinking about how to throw away old computers, storage media and papers does not ignite the fire of enthusiasm as much as thinking about new hacking threats and cybercrime ploys. Many organizations spend significant time and money on activities and tools to prevent and mitigate technology-based incidents, such as unauthorized network intrusions, malicious code, and so on. This is certainly necessary for modern business! However, it seems procedures are getting increasingly sloppy when it comes to controlling the disposal of old computer hardware and media that contain personal information.

The number of reports concerned with the disposal of personally identifiable information (PII) on computers and electronic storage media is increasing. Many information security and privacy incidents have occurred by simply and thoughtlessly putting computers, USB drives and cell phones out on the streets or into public trash cans. While it may not be a sexy topic to address, organizations need to put forth effort in ensuring proper disposal or they will likely experience ridiculously unsexy privacy breaches resulting from improper disposal practices, and then even more unsexy fines and bad publicity as an aftereffect.

Know the disposal laws

The U.S. has the Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule (at ftc.gov/os/2004/11/041118disposalfrn.pdf) and several other laws that include requirements for the proper and safe disposal of PII. A few other U.S. laws that include disposal requirements include, but are not limited, to:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Resource Conservation and Recovery Act (RCRA)
- International Traffic in Arms Regulations (ITAR)
- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)

Several states, such as Arkansas, California, Maine, Massachusetts, Minnesota and Washington, also have laws and regulations governing the disposal and recycling of electronic waste.

It is also important to note that the U.S. Environmental Protection Agency (EPA) generally holds the creator of the electronic waste responsible for inappropriate disposal. This means the EPA could fine the company whose name is on the computer's asset tag, even if the company itself was not the one that actually put the computer in the garbage dump.

The EPA has a pointer to an interesting and informational document, "Waste Management Guidance: Electronic Equipment" (http://www.deq.state.mi.us/documents/deq-ead-tas-elecequp.pdf) that contains good information for businesses to know. I am glad to see it directs readers to remove data from the electronic devices before donating them or throwing them away. See http://www.epa.gov/epr for more information about EPA standards and requirements.

Similar disposal rules are also found, and are emerging, in other countries. For example, the UK has the Data Protection Act that requires, among other safeguards, that confidential information must be securely disposed of. The British Standard for the secure destruction of confidential material, BS 8470:2006, applies to confidential information in all its forms and supports compliance with the Data Protection Act. Confidential materials include such things as paper records, computer hard drives, CDs/DVDs and even company uniforms.

Throwing away electronic information

Many organizations have had print disposal methods around for several years, but still do not have any procedures in place to dispose of electronic information. During a recent informal survey I found this to be especially true with small and medium sized businesses.

Electronic information can be destroyed in many ways, some more reliable than others. Some of these methods include:

- Overwriting (also known as wiping)
- Low level formatting
- Physical destruction
- Degaussing

If you do not want to get out the sledgehammer, want to ensure the data on the storage media is irreversibly removed, and do not plan to re-use the storage media, then degaussing is often considered the best option.


Note that degaussing is not effective for removing data from nonmagnetic media, such as compact discs (CD), digital versatile discs (DVD) and other optical media.

It has been a long time since I have seen degaussers discussed, so it is worth looking at more closely, particularly within those businesses that have nothing in place today to dispose of electronic data. So here is some information that you can use as a handy-dandy reference at your desk, and also help you to create your own electronic disposal policies and procedures if you do not already have some in place, or update the ones you have if you have not looked at them for a while.

A degaussing FAQ

Here is a set of degaussing frequently asked questions (FAQ) to help you make your degaussing policies, procedures and solutions decisions:

1. **What is a degausser?** A degausser is a device that, if a good one, provides a fast, efficient way to remove all audio, video and data signals from magnetic storage media such as tapes or hard drives. Degaussers come in many different sizes, from handheld to desktop models to huge corporate-sized machines.

2. **How does a degausser work?** A degausser produces a magnetic charge, through the use of permanent magnets or a degaussing coil, that wipes the magnetic fields that contains the recorded data completely off the media, effectively destroying the information. You know those warnings you used to get about not using magnets to attach backup floppy disks to your computer? It is because the demagnetization that would occur through the magnet's contact with floppy disk would wipe out the data, similar to how a degausser de-magnetizes magnetic storage media. This de-magnetization, also known as degaussing, is the physical process that occurs when magnetic storage media is sent through a powerful magnetic field. Generally, degaussing rearranges the magnetic domains on the media which removes the recorded signals, or data. Organizations should be aware that degaussed magnetic media can no longer be read by the original recording system. There have been many very interesting studies about computer forensics gurus trying to recover data from degaussed storage media in an attempt to do this, though. By degaussing magnetic media before re-using it, you are basically returning it to its original condition with all the particles orientated at random and none of your data remaining.

3. **When should I degauss my media?** If you are finished using magnetic storage media, such as tapes, hard drives and diskettes, you should degauss them before you give them away or throw them in the trash. You should also degauss magnetic media before you send them out for repair. There are numerous un-erase utilities available, so you shouldn't risk sensitive data getting into the wrong hands. You should also degauss electronic computer storage when you want to re-use it in a different department, or for a completely different business purpose. Establish an information security policy requiring all computer hard drives to be degaussed before sending them out for warranty repair, as well as before donating them to a charitable cause, putting them into the recycle bin, or using them within a different department at your organization.

4. **Isn't recording over, or rewriting, electronic media just as effective?** The data recorded on magnetic media form a series of lines. When you write or record over magnetic media, only new data is stored within these lines, leaving some of the remanents of the data that previously existed. These leftover data remanents cause what are known as "spurious signals." Spurious signals can cause poor quality, and downright horrible, sound and picture quality on audio/video tapes and read/write errors on data tapes. When doing re-recordings or re-writes, bad areas on the media can also be skipped, compounding the quality issues as well as leaving more data remanents. For these reasons, it is usually best to degauss instead of doing re-

writes, unless you are using a powerful re-write program certified to meet NIST standards.

5. **Why can't I just re-format my computer hard drive instead?** Formatting can take a significant amount of time to accomplish; making the computer unavailable for use during the formatting process, as well as contributing to wear of your expensive computer equipment. There is also the possibility that re-formatting will miss storage tracks, which could subsequently result in read and re-write errors. A degausser, in comparison, will not only completely remove the data from your media, it will also do so in a very short period of time; often in a matter of seconds for typical business degausser use.

6. **What are the benefits of degaussing?** There are at least three good benefits of degaussing:
    a. You will be able to re-use electronic computer storage media many times without read or re-write errors, potentially saving your organization a good amount of money.
    b. You can ensure that storage media can be thrown away or donated to other organizations without containing sensitive data, supporting compliance with numerous laws and regulations, as well as removing information security and privacy breach risks.
    c. For the radio and television broadcast industry, using degaussers on expensive magnetic broadcast media can allow them to be re-used many times with greater clarity, resulting in significant savings.

7. **What type of degausser do I want?** The type of degausser you need depends upon three factors:

    - The amount of magnetic media items you want to degauss at any one time.
    - How often you plan to use the degausser within a certain time frame.
    - How many different types of magnetic media you want to degauss.

    When shopping for a degausser, be sure you know this information, and ask the salesperson to show you only degaussers that meet your criteria.

8. **Do hard drives heat up in the degaussing process?** Indeed, hard drives can heat up during the degaussing process, so you need to consider this if you are going to use a degausser that requires the operator to hold the media being degaussed. If this is your choice, based upon the answers to question 7, then be sure you also get some heat-resistant gloves to use.

9. **Can I reuse a hard drive after I degauss it?** No, computer hard drives cannot be reused after they are degaussed. This is because the degaussing process erases the servo tracks, which are necessary to locate the data tracks, which leaves the hard drive inoperable. Degaussing hard drives should be used solely for disposal of those hard drives for security purposes.

10. **Can I reuse LTO tape after I degauss it?** LTO (Linear Tape-Open) is a tape standard that stores data in 384 data tracks, divided into four data bands of 96

tracks each. LTO technology was developed as an open alternative to the proprietary Digital Linear Tape (DLT). No, you cannot reuse LTO tape after you erase it. The degaussing process erases the factory pre-recorded servo tracks from the tape, making the tape unusable. Degaussing LTO tape should be done only for security when disposing of the tape.

11. **Can I reuse DLT tape after I degauss it?** DLT (Digital Linear Tape) is a magnetic tape data storage technology that was developed by Digital Equipment Corporation (DEC). Yes, you can reuse DLT tape after you erase it. DLT tape is quite popularly used for backups, so a degausser would be a good investment if your organization uses DLT.

12. **Is degaussing safe?** Yes, it is generally safe to use a degausser. However, individuals with a pacemaker should not operate or be in the vicinity of a degausser. It is also important to know that you should not wear a quartz watch while degaussing or it could be erased!

13. **Are there disadvantages to using degaussing instead of wiping or overwriting software?** Yes, there are a couple in addition to the issues previously discussed:
    a. A typical organization will only have a limited number of degaussers, making it hard for offices in different geographic locations to use the degaussers. Overwriting and wiping programs can be more easily distributed to remote locations.
    b. If you have a significant number of magnetic storage media to degauss on an ongoing basis, and within more than one department, then more areas throughout your enterprise can remove data from storage media simultaneously by using multiple licensed copies of wiping or overwriting programs.

See the NIST "Guidelines for Media Sanitization" (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf) for more good information about degaussing, along with other secure methods of information disposal.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She just released the quarterly employee awareness tool, "Protecting Information" (Information Shield) and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.