RECLAMERE
The Data Security Experts

Destroying Data the DoD Way

By Angie Singer Keating, CISA, CIPP, CISM

Military Standards Help Ensure Compliance for Electronic Data Security

The unauthorized use of confidential or sensitive information contained on computer hard drives is a serious problem facing most healthcare organizations. Organizations that do not require proper hard-drive sanitation as part of there information destruction program face regulatory violations resulting in large fines, imprisonment, or public relations nightmares.

One of the most efficient and effective ways to sanitize or physically destroy computer hard drives is to follow the stringent standards established by the US Department of Defense (DoD). This article will compare digital sanitation and physical destruction and help you determine which method is best for your organization.

Comparing Digital Sanitization and Physical Destruction

Digital sanitization-also know as overwriting-is the most common, cost-effective process for secure destruction of data without rendering the hard drive useless. Overwriting replaces existing data on a hard drive with meaningless data in such a way that the original data can not be recovered. [1]

Overwriting can be performed using any number of software tools that meet the DoD overwriting standard. In addition to overwriting, the DoD standard specifies that qualified technicians attempt data

Destroying Data the DoD Way (cont.)

By Angie Singer Keating, CISA, CIPP, CISM

recovery on random drive samples as a quality control measure. Overwriting is approved for unclassified information only. The information the DoD designates as unclassified is highly sensitive- as sensitive as the types of information that healthcare entities handle every day.

Overwriting does not work and can not be verified on hard drives that are broken or damaged, and it is not appropriate for hard drives containing classified information. In each of these situations, physical destruction of the hard drive is the only method approved by the DoD. Physical destruction entails damaging the medium so that it is unusable in a computer and so that no data can be retrieved.[2] The DoD standard lists several ways to physically destroy a hard drive with differing levels of safety and practicality.

Reputable IT asset management companies have been providing DoD-compliant hard-drive sanitization and hard-drive destruction to customers such as healthcare providers, insurers, large retail organizations, financial institutions, and government agencies for some time. These organizations perform careful due diligence and base their services on internal research or by consulting IT professionals.

Can Overwritten Data Be Retrieved?

It is possible to retrieve meaningful data from a hard drive that has been overwritten to DoD standards. However, the possibility is slight, and debate exists over what is considered “meaningful” data as well as what constitutes reasonable methods to retrieve it.

“Meaningful data” is the term the DoD uses to differentiate between information that could cause harm and data that simply

Destroying Data the DoD Way (cont.)

By Angie Singer Keating, CISA, CIPP, CISM

exists in its primitive state of iron particles and requires extensive and expensive recovery methods. [3]

Magnetic force microscopy (MFM) photography is the most commonly cited technology capable of recovering data from a drive that has been overwritten to DoD standards.[4] This technique involves opening the hard drive and examining the platters with a magnetic force microscope, which is used in conjunction with a camera to produce pictures of the drive. MFM then scans the entire surface of the drive, moving from region to region, with each region yielding a picture.

With the proper equipment, this process seems feasible-until you investigate the level of effort and expertise required to perform this highly specialized type of data recovery. The process is complex, and any small error in interpretation can result in useless data. As there appear to be no documented and verified private-sector MFM recoveries of meaningful data, it is highly unlikely that it has been performed successfully in the private sector and therefore cannot be considered a threat.

Effective and Secure, Despite Misconceptions

Another perceived limitation of hard-drive sanitization is the risk of human error. For example, a drive can be lost, not verified, or not properly wiped. However, when properly followed, the DoD standard virtually eliminates human error and provides a highly reliable means of data destruction.

Not every IT asset management company or computer recycler has the capability to perform DoD-compliant hard-drive

Destroying Data the DoD Way (cont.)

By Angie Singer Keating, CISA, CIPP, CISM

sanitization. Therefore, criteria must be in place to create processes and standards that will dramatically reduce the chance of data breech due to human error. The DoD standard provides explicit instructions for chain-of-custody processes, documentation, process control, and quality control. These procedures should be formally documented and made readily available by any reputable IT asset management company.

There is also a misconception that hard-drive sanitization cannot be visually verified. However, the DoD standard requires that o fewer than 20 percent of overwritten drives be sampled at random to verify the integrity of the overwriting process. This important quality-control step must be performed by a trained technician other than the one who performed the overwrite process.[5] Although the vast majority of DoD-compliant overwriting software produces a verification report at the end of the wipe, the only true way to know if recoverable, meaningful data remains is to attempt recovery. In addition, independent validation of the data destruction and data recovery quality-control program must be performed periodically by sending drives to an independent expert data recovery service.

It is easy for those unfamiliar with information technology to assume that if a company is able to recover data from catastrophic damage, data could be recovered from a hard drive that merely had a DoD-compliant sanitizing overwrite. However, recovery of any usable data is highly unlikely.

There is a perception that data are regularly being recovered by hackers, criminals, intrepid IT students, and reporters eager to advance their careers with the intention of exposing recovered data from high-profile organizations. This notion is patently false,

RECLAMERE
The Data Security Experts

Destroying Data the DoD Way (cont.)

By Angie Singer Keating, CISA, CIPP, CISM

as documented by two MIT graduate students who catalogued five different widely cited cases where sensitive or confidential information was found on donated, sold, or discarded computer systems and hard drives.[6]

It is important to note that in each of these cases there was no indication that a DoD-compliant overwrite had been performed. Even more important is the fact that data-recovery tools weren't necessary to find the data on the majority of the drives. The systems were simply powered on. Complete operating systems were intact, and sensitive files were there for anyone to view. The computers had simply been discarded with no attempt made to destroy the data.

For people responsible for the proper destruction of data on computer hard drives within their organizations, digital sanitization is a safe, highly secure, cost-effective practice when performed properly to the DoD standard. By partnering with a qualified IT asset management company, the proper destruction of data on computer hard drives can be accomplished so that the organization is compliant with privacy laws, and data never come back to haunt them.

Angie Singer Keating, CISA, CIPP, CISM
Co-Founder and Vice President of Compliance and Security

[1] Defense Logistics Agency. "Defense Reutilization and Marketing Service Guide for Disposal of IT Equipment." Available online at www.dla.mil.

[2] Defense Reutilization and Marketing Service. "Turn-in Guidance for Disposition of Unclassified Computer Hard Drives." Available online at www.drms.dla.mil/turn-in/cputurnin41905.pdf.

[3] Gutmann, Peter. "Secure Deletion of Data from Magnetic and Solid-state Memory." USENIX Security Symposium Proceedings, July 1996

[4] Ibid

[5] Department of Defense. "Disposition of Unclassified Computer Hard Drives." Available online at www.drms.dla.mil/turn-in/cputurnin41905.pdf

[6] Garfinkel, Simson, and Abhi Shelat. Remembrance of Data Passed: A Study of Disk Sanitization Practices *IEEE Security and Privacy* 1, no.1 (2003): 17-27. Available online at www.cs.unibo.it/~montroeso/doc/papers/AStudyOfDiskSanitizationPractices.pdf