Why the three pass data wipe requirement for hard drives is obsolete

. . . and why it takes the focus off the real security threats to an institution

The genesis of the 3-pass wipe theory

In 1996, Dr. Peter Gutmann of the University of Auckland presented a paper about recovering data from hard drives using “magnetic force microscopy.” This was possible due to a magnetic shadowing effect which permitted data to be reconstructed when it was thought to be destroyed. In response to this security threat, he recommended a specifically defined 35 pass wipe process so that data on wiped drives could not be uncovered. The report was widely cited and spawned a whole host of wiping standards (including what is referred to as the DoD 3-pass wipe) to try to better manage this data security risk.

Beginning in 2001, ATA hard drives with a size typically greater than 15 GB were built on a platform that makes this type of data recovery obsolete. Dr. Gutmann eventually revised his earlier conclusions about the potential for data recovery when he updated his paper in 2011. “Looking at this from the other point of view, with the ever-increasing data density on disk platters and a corresponding reduction in feature size and use of exotic techniques to record data on the medium, it's unlikely that anything can be recovered from any recent drive except perhaps a single level via basic error-cancelling techniques. In particular the drives in use at the time that this paper was originally written are long since extinct, so the methods that applied specifically to the older, lower-density technology don't apply any more.”
http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html#recommendations

The DoD “standard” is not really a standard at all:

Many enterprises continue to base their data sanitization program on what is known as the “Department of Defense (DoD) 5220-22.M Standard”. This is not actually a standard, but is a reference to the National Industrial Security Program Operating Manual (NISPOM) which was originally published in January, 1995 and reissued in February, 2006. *(The original document is no longer published on government web pages, but is archived at: http://www.fas.org/sgp/library/nispom/nispom2006.pdf).*

The NISPOM actually covers the entire field of government-industrial security, of which data sanitization is a very small part (about two paragraphs in a 141 page document). Furthermore, the NISPOM does not actually specify any particular wipe method. Standards for sanitization are left up to the “Cognizant Security Authority.”

The Defense Security Service produced a *Clearing and Sanitization Matrix* (C&SM) which at one time suggested that a 3- or 7-pass wipe was required to electronically clear a drive. This is the source of the widely cited DoD 5220-22.M 3-pass wipe standard. In 2007, the standard was updated to say, “DSS will no longer approve overwriting procedures for the sanitization or downgrading of IS storage devices (e.g., hard drives) used for classified processing.” (*Again, this Matrix is no longer published on federal government web sites, but a copy is archived at: http://www.oregon.gov/DAS/OP/docs/policy/state/107-009-005_Exhibit_B.pdf?ga=t.)*

When did the wipe recommendation change?

The US government commissioned the National Institute of Standards and Technology (NIST) to devise a more comprehensive approach to data security. As a result, they published the “NIST Special Publication 800-88: Guidelines for Media Sanitization” in 2006. *(http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf).*

In this document, the authors recognized that technology had changed from when researchers like Dr. Gutmann originally purported the limitations of data overwriting tools. They wrote:

Madison, WI * Indianapolis, IN

608-222-4800 * 888-222-8399

info@cascade-assets.com * www.cascade-assets.com

> "Advancing technology has created a situation that has altered previously held best practices regarding magnetic disk type storage media. Basically the change in track density and the related changes in the storage medium have created a situation where the acts of clearing and purging the media have converged. That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack." (p. 14, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf)

This change in technology is further explained by Simson Garfinkel and Abhi Shelat of MIT in their detailed report, "*Remembrance of Data Passed: A Study of Disk Sanitization Practices"* published in 2003. "Given the current generation of high-density disk drives, it's possible that none of these overwrite patterns are necessary – a point that Gutmann himself concedes. Older disk drives left some space between tracks; data written to a track could occassionally be recovered from this inter-track region using special instruments. Today's disk drives have a write head that is significantly larger than the read head: tracks are thus overlapping, and there is no longer any recoverable data 'between' the tracks."
http://www.scribd.com/doc/7156294/Disk-Sanitization-Practices

There are more important security concerns than how many wipe passes you choose

NIST updated its "Guidelines" document in September, 2012 and reconfirmed the effectiveness of a one-pass overwrite, but also cautioned about new data security challenges posed by emerging media storage devices. "For storage devices containing Legacy Magnetic media, a single overwrite pass with a fixed pattern such as 0s typically prevents recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data. . . . Users who have become accustomed to relying upon overwrite techniques on magnetic media and who have continued to apply these techniques as media types evolved (such as to flash-based devices) may be exposing their data to increased risk of unintentional disclosure. Although the host interface (e.g. ATA or SCSI) may be the same (or very similar) across devices with varying underlying media types, it is critical that the sanitization techniques are carefully matched to the media. (p. 14, http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf)

The NIST Guideline provides an exhaustive overview of all the various storage media deployed today and offers recommendations for clearing, purging and/or destroying data on each one of them. Firms should match NIST's recommendations to their internal security processes to make sure all assets they own are effectively secured during disposition.

Cascade has your back – we fulfill NIST Guidelines for all media types

At Cascade, data security is of utmost importance. Our reputation is on the line every day. We provide secure data destruction for Fortune 500 clients and the Federal Government. A table explaining how we fulfill NIST guidelines for data security on a wide array of electronic media is made available to our customers and posted online at: http://cascade-assets.com/securityprocedures.html.

At the same time, we won't scare our customers to spend more on data security programs than is necessary. Since Cascade wrote our White Paper in 2005, "Closing the Back Door: Managing IT Data Security During Disposal", we've been telling the world that a 3-pass data wipe is not significantly different than a 1-pass overwrite. If a company has a policy to meet the obsolete 3-pass DoD 5220.22-M "standard", we'll try to talk them out of it. We can also perform this service, *for an added fee.*