The three pass data wipe requirement for hard drives is obsolete

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

By: Neil Peters-Michaud

December 14, 2017

Executive Summary

There is still a perception among information security professionals that the legacy 3-pass Department of Defense "standard" is the only sufficient method of data sanitization. In fact, this isn't really a standard at all, and it has become obsolete due to new data storage technologies and the proliferation of media with non-volatile memory that might contain sensitive data. Worse yet, if an organization only focuses on the data sanitization method used to wipe data, they may lose sight of the more likely threats to information breaches arising from the mismanagement of these assets. This paper provides information on how to extend best management practices for data security to IT assets designated for retirement, and it dispels some myths related to various data destruction options.

Keywords:

Data Security, IT asset disposition, ITAD, NIST 800-88, HIPAA, FACTA, Wipe, DoD 5220.22-M

The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

Threats to data security

Cyber security attacks that lead to data breaches are well known. Those are the big stories that hit the news – Equifax, Target, and Sony Entertainment. They also garner the most attention and investment from risk management programs at companies.

But there are also numerous examples of security incidents involving the improper destruction of data on media storage devices that are retired from use.

The National Association for Information Destruction purchased more than 250 tablets, phones and hard drives from places like Ebay, New Egg, and Amazon – resellers that may source this equipment from consumers, but more likely from businesses. They found overall that 40% still retained some amount of personal information.[i]

Blancco Technology Group purchased 200 second-hand hard disk drives and solid state drives before conducting a forensic analysis to find out what data was recoverable. Two-thirds (67 percent) contained personally identifiable information and 11 percent contained sensitive company information, it said.[ii]

The cause of these security incidents is not likely due to ineffective data sanitization, but more due to mismanagement of these data bearing assets during the disposal process.

In a report published by Compliance Standards, Retire-IT (an ITAD chain of custody management firm) evaluated 4,812 ITAD projects, combining a total asset volume of 402,363 units, across 732 companies. From this data set, they found that 22% of the assets could not be traced to a serial number in the company's asset repository. In addition, 38% of the companies were unable to account for all their devices and didn't know if their missing assets were lost by the company or stolen. These figures are exceedingly alarming because they represent higher incidences than the reports that 24% of firms have recently experienced network hacking.

After evaluating this information, Barbara Scott of Compliance Standards, concluded "Companies appear to put greater emphasis on network security than on device security, as if the latter carried lesser risk."

Indeed, there is an ongoing threat to security from the improper management and disposal of IT assets that store data. In the past two years, there were 389 active data breach investigations reported on the Health and Human Services website. Of those reported incidents, 19% could be tied to the asset management program, because they relate to the loss, theft or improper disposal of assets.[iii]

These examples illustrate the fact that enterprises are vulnerable to data theft even after their IT assets are disposed. Many companies fail to recognize the prevalence of their data storage devices – from hard drives to back up tapes to smart phones to VoIP phones with contacts and messages stored on flash memory. Any media that records data provides an opportunity for identity theft until it is destroyed.

While there are many reported cases of sensitive data showing up on disposed hard drives, there are no published examples of the exploitation of data from drives properly sanitized. Let's look closer at why that is the case.

Data sanitization and the "3-pass wipe"

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.[iv]

Beginning in 2001, ATA hard drives with a size typically greater than 15 GB were built on a platform

© Cascade Asset Management, LLC, 2017. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

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."[v]

The DoD "standard" is not really a standard

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. It was again re-published on May 18, 2016 and marked with "Change 2."[vi]

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."

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.[vii] This original document was revised in December 2014 to cover additional media storage devices.

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:

> "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)[viii]

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 occasionally 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."[ix]

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

NIST updated its "Guidelines" document in December 2014 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 *magnetic* media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders 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 memory-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. 7)[x]

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.

Assessing various data destruction methods

The NIST Guidelines establish three levels of data destruction that can be applied to different data storage devices. Organizations should pick the physical destruction of electronic sanitization method that meets their tolerance for risk. The destruction method may be different for each class of storage devices.

Clear is the method that uses software or hardware products to overwrite user-addressable storage space on media with non-sensitive data, when available. This is done by writing "0's or 1's" over all sectors in a drive or storage device. If this isn't possible (such as in a basic cell phone or piece of office equipment), manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device. Items that are Cleared may be able to be reused after they are sanitized.

Purge may be an overwrite, block erase, or Cryptographic Erase through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the typical read and write commands. Items that are Purged may be able to be reused after they are sanitized.

Destroy is a physical process that makes data retrieval infeasible using state of the art laboratory techniques. Destruction methods include shredding, incineration, melting and pulverizing. Degaussing is also considered a destruction technique when used properly. Bending, cutting and drilling holes through a storage device are NOT considered destruction techniques. Destroyed items are not able to be reused.

What's the right choice for data destruction?

Your specific security needs should be evaluated in relation to your organization's regulatory requirements, corporate governance standards, the overall level of risk you find acceptable and the resources you have available to affect a solution.

Data destruction services exist on a continuum from least effective to most. The most elaborate solution is not always the best for every situation.

Failing to comply with your fiduciary, environmental and social responsibilities is dangerous and not recommended. However you must arm yourself with knowledge and analyze the benefits of any solution to avoid being "over-sold". Carefully weigh the realistic threats against the benefits of various solutions and evaluate the cost and benefits of each.

The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

Recognizing “Back Door” security threats

What happens to the obsolete equipment the day after the big rollout when much of the focus is on managing new equipment? In too many cases this equipment is stored in public access hallways, garages, or unlocked basements until decision makers can schedule its disposal, leaving critical information available for employees, visitors and customers to view, copy or steal.

Some firms still toss their IT equipment in the garbage where it can easily be hauled off by social engineers or dumpster divers. Simple data retrieval programs can often hack into information left unprotected by firewalls and network protocols. Sometimes, users make a theft easy when they mark their passwords on the equipment making the process more accessible to malicious activity.

In order for an enterprise of any kind to have a truly secure information system it must have a method of disposal for retired equipment that prevents data from being recovered once it leaves its securely managed environment. This safely closes the circle that is the life cycle for an IT asset as well as responsibly manages the chain of custody for information held by an enterprise. To overlook this critical phase of the system life cycle is to waste all of the investments to purchase and implement the security of your present system. Expensive consultants, sophisticated software and powerful hardware will have done you no good if data is retrieved from even one data storage device and used against you maliciously.

Maintaining physical custody of retired assets and archived data

Physical access controls during the use phase of IT assets is intuitive and managed by placing the asset in a secure environment, populated work area or by virtue of its electronic status or continuous use. No one can steal a router, or server that is in constant operation and is monitored by access logs without raising some kind of alert.

Any time equipment is replaced, attention needs to be paid to archiving and securing the data on the old system. This may take place through a network backup, external tape, disc or drive back up, or physical removal of the hard drive. The archive should be cataloged, stored and secured for later retrieval. In addition, a backup inventory and archive schedule is an essential part of a security system to ensure backups are accounted for and stored only as long as is absolutely necessary. Once any reasonable need to store the archived data has passed, a method for secure destruction and disposal is in order.

Once the data on retired units have been archived, it is important to quickly neutralize or destroy the data on that equipment. Simple encryption programs can be run from the desktop on the unit prior to the final disconnection of the computer from an enterprise network. These programs lock access to a computer by scrambling the data.

More costly and time-consuming data wiping programs can also be run on hard drives. A typical one-pass overwrite of a 500-GB IDE hard drive takes about 4 hours to complete, depending on the setup. More secure 3 to 7 pass wipes take proportionally longer.

Finally, some companies open computer, laptop and server cases to physically destroy hard drives with drill presses or sledge hammers, among other tools. While effective at immobilizing the device, data can still be retrieved through forensic recovery, and the time and attention and potential safety risk involved in performing this task is typically not appropriate for an IS technician.

The more typical method for securing old data is through physical controls. Just as document destruction companies set up collection bins in offices with slotted and locked lids, electronic media destruction firms can offer those same totes for the collection of pulled drives, tapes, and other media for later destruction. If hard drives are kept in the existing system, the collection of older computers for off-site data destruction and media destruction could be coordinated to coincide with the deployment of the new

The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

systems. In this scenario, a secure media management firm takes custody of the equipment just as it is removed from the enterprise security system. The next best option is to package and store the equipment in a locked and secure room.

Here's where an asset management system provides value. If your company tags and tracks IT assets throughout their lifecycle at the enterprise, a simple scanning or notation of retired assets in the system and indication of their status will provide a wealth of information when looking for redeployment or retirement options. It will also provide documentation of the assets removed from your on-site security system and transferred to another responsible party. Asset management is now a required feature of maintaining a responsible chain of custody for electronic media. This information can be shared with off-site IT retirement firms who can provide reasonable costs or values for this equipment and who can demonstrate that the information on each asset was destroyed properly. Tracking and cataloging assets can greatly reduce handling and disposition costs later.

Off-Site Destruction of Information

Although there are low cost and even no cost methods of disposing of your IT equipment, they often come with a great deal of risk and expose you to liability which far exceeds the short term financial benefit. The primary goal of responsible care in destruction of information is to do it as soon as possible. The further data travels through the disposition process, the greater the risk.

From the truck driver willing to pilfer his or her load of laptops on the way to the disposal company, to the overseas computer refurbisher using the licensed software on a PC "recycled" from the US, to the social engineer actively hunting for information to exploit, there are numerous threats to information throughout the disposal process. The effects of using inferior and risky disposition methods are essentially cumulative.

When contracting with off-site vendors for destruction services, inquire about the following practices:

- What information security management practices and technology do they employ? Their level of investment and attention to their own security needs is often indicative of their handling of other's information.
- What type of insurance or bonding does the vendor carry to cover data leaks?
- What asset management system does the vendor use to effectively track and report on the disposition of equipment?
- What technology does the company use to electronically wipe or physically destroy equipment? Where does this technology exist and what steps must the equipment go through before it is destroyed?
- Can destruction of personal assets be witnessed?
- What happens to the destroyed assets after the vendor completes its work?

Transferring title and responsibility of equipment to a third party also includes a transfer of risk. Certain regulations require third parties handling personal privacy information to commit to a Business Services Agreement that outlines the responsibilities and activities of the vendor when managing information transferred to them.

When many enterprises audit their IT asset retirement company or recycler they look to assess the vendor's environmental management system to determine potential liability exposure related to hazardous waste treatment and disposal activity. More and more enterprises are also including security audits of vendors to ensure compliance with privacy requirements and to demonstrate a comfort level with the way their security systems and asset management services intersect.

Selecting a third party processor of disposed IT assets cannot be viewed as a nuisance, but must be recognized as an important extension of the management of information technology security systems.

Conclusion

When developing an information security system for your IT equipment, don’t forget about managing IT equipment after it is removed from service in your company. These items often contain a wealth of information that is vulnerable through electronic recovery or physical theft. All of the investment in infrastructure security can be wasted if attention is not paid to maintaining a secure archiving and disposal system. While the wiping standard you select is important, it is not the only consideration to make when ensuring data are destroyed on retired assets. For most situations, developing a secure chain of custody within the organization with a trusted IT asset manager will go a long way to ensuring information is less vulnerable to theft or misuse.

About the Author

Neil Peters-Michaud is co-founder and CEO of Cascade Asset Management, LLC. He earned a Masters in Business Administration from the University of Wisconsin in 1999 and a Bachelors of Science from the UW in 1993. Neil has been involved in electronics recycling since 1994 and has authored numerous papers and presentations on environmental, health and safety impacts of electronics recycling. He is a Certified Hardware Asset Management Professional, he has participated in standards development with NSF and IEEE for the EPEAT Server Standard, and also is a member of an iNEMI workgroup addressing hard disk drive design, reuse and remanufacturing. Neil grew up in Silicon Valley and immersed himself in the IT industry through positions with several prominent electronics manufacturers.

[i] "Personally Identifiable Information found on 40 Percent of Used Devices in Largest Study To-Date," National Association for Information Destruction, March 24, 2017.

[ii] The Register, June 28, 2016. https://www.theregister.co.uk/2016/06/28/ebay_hard_drives_still_contain_sensitive_data_study/

[iii] Search conducted on 11/1/2017, US Department of Health and Human Services, Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[iv] Much of the historical information in this section was originally reported in the whitepaper, "Closing the Back Door: Managing IT Data Security During Equipment Disposal," Myrant and Peters-Michaud, April 28, 2005. https://cascade-assets.com/documents/closingthebackdoorwp.pdf

[v] http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html#recommendations

[vi] http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf

[vii] *http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf*

[viii] ibid

[ix] http://www.scribd.com/doc/7156294/Disk-Sanitization-Practices

[x] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.