Why care about data destruction and asset disposal? According to the US Department of Commerce, data security breaches cost US companies more than $250 billion per year! A few examples will help illustrate the importance of proper data erasure and asset disposal practices.

A Loyola University (Chicago) computer with the Social Security numbers of 5,800 students was discarded before its hard drive was erased, forcing the school to warn students about potential identity theft.

A survey by data forensics experts, Garfinkel and Shelat, found that over 40 percent of hard drives collected from eBay and other places had recoverable data and over 30 percent contained sensitive information, including credit card numbers.

A BBC documentary revealed that bank account details of potentially thousands of UK residents were being sold in West Africa for less than £20. Sensitive information was contained on the PC hard drives exported to Nigeria (2006).

To combat this problem, companies need to have a good policy for data destruction and asset disposal. A good policy recognizes that different types of media require different disposal policies. To understand the differences in HDD and SSD data destruction, we need to look at how data is written to the media. From there we need to examine the different types of data destruction available and the effectiveness of the different methods of data destruction for the different types of media.

Data is stored magnetically on traditional hard disks (HDDs). As the read/writes heads pass over the magnetic substrate, bits of data are magnetically aligned and oriented in such a way that they can be interpreted as 0’s and 1’s (binary data). A collection of these bits of data are put together to form bytes which are in turn grouped together in what is traditionally referred to as a sector (usually 512 bytes of data).

In SSDs, data is written electronically and not magnetically. This data is stored in pages that vary in size from SSD to SSD. These pages are then grouped together into erasure blocks. These erasure blocks are then zoned together based on the physical address in the flash chip. Data is not written to the pages sequentially; rather the data is striped across the erasure blocks and is managed by the wear-leveling controller. When the data stored on the disk is modified, the wear leveling controller moves the entire block to a new location and schedules the original block for erasure. In short, the user has no control over where the data is written and updates to files will more often than not end up in new locations on the media.

With this basic understanding of the way data is written, we can now look at the different erasure methods and their impact on both HDDs and SSDs. Data destruction can be categorized into three methods: software based data erasure, degaussing and physical media destruction.

Software based erasure has been around for a long time and has become more accepted as a method for data destruction as more and more data erasure standards are created and adopted. Built for HDDs, traditionally this method writes a pattern of data to each sector of the disk in a sequential manner, overwriting the original data and making it unrecoverable while still leaving the HDD functional. This makes software a viable solution for HDDs you
want to reuse. For media that stores data like the SSD, this is not a good method for data destruction. The erasure software is not able to control the specific region the data is written to, as this is controlled by the wear-leveling controller. Arguments have been made that using the TRIM command or other commands built into the SSD, will ensure a secure erasure can be performed, but research has shown that these methods are not always successful in removing the data from the drive. So while software erasure is a good solution for HDDs, it does not yet seem to be the right solution for data destruction for SSDs.

Hardware based degaussing has gained traction in recent years as an alternative to software erasure. Pricing for degaussers has dropped and the physical units have gotten better at destroying media. The degausser works by sending a magnetic pulse through the media. For HDDs, this is a very quick solution that reorients the bits on the disk thus destroying the user data and in most cases rendering the HDD inoperable. For SSDs, this is not an effective solution as the data is not written magnetically, but rather stored electronically.

The best way to destroy data on both HDD and SSD drives is physical media destruction. This typically involves shredding the media. As long as the process “shreds” the SSD media into pieces that are small enough that a single chip cannot escape damage, this is the ultimate data destruction method. Care should be taken however, to make sure that the shredding is done in such a way that no loose chips end up untouched in the shredded mass. If the chip is not damaged by the shredding process, it would be possible to recover data from it.

It is important to keep in mind how data is written to different types of media when developing your data destruction and asset disposal plans. Not all erasure and destruction services work with all of the different types of media. The next article in this series will discuss best practices and help you develop your own plan for asset disposal.