



Rethinking the Vulnerabilities of a Data Wiping Process

Tech Commentary

Michael Cheslock

DestructData, Inc.

Vice President –

Technology & Sales

March 31, 2017



Rethinking the Vulnerabilities of a Data Wiping Process

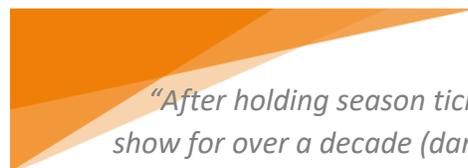
By: Michael Cheslock, DestructData, Inc.

1 MISDIRECTION

I have been professionally focused on hard drive sanitization for 11 years. Throughout that time, the most common theme that I have observed, especially in the electronics reuse community, has been that organizations' priorities related to data destruction decisions are almost always reactive to new information irrespective of relevance. In other words, decision-makers have a habit of reacting to the newest piece of information - be it a new standard, guideline, or even press-release or marketing message, and reviewing their data destruction operation with the new information as a top priority, sometimes to the point of losing sight of much more critical considerations. Unfortunately, this practice is extremely ineffective, and also often unnecessarily expensive.

Let's start with an example (or a symptom, depending on how you look at it): When discussing a media sanitization process with someone in the industry, whether a client, partner or otherwise, what kinds of questions do we most often ask? "What software do you use?" "Do you do DoD, or NIST?" "How many passes do you do?" These questions are about a mechanism involved in the data wiping process: the software. They are all about one of the tools used in the process of wiping drives. I've never once heard someone ask, "How often do your technicians go through retraining on sensitive data handling practices?" Or, "What procedures do you use to separate, unwiped, passed, and failed devices from one another?" If I told you that this latter set of questions points to areas of a data wiping operation that are more than 10 times as likely to cause a breach-level failure than does the former set of questions, would you believe it? Maybe not, so let's look at it a different way:

If you were hiring a contractor to build an addition on your house, you'd ask for insurance information, check BBB ratings, ask for some examples of recently completed projects and maybe some customer



"After holding season tickets to this same show for over a decade (darn good seats, by the way), the most obvious question to me has become, 'Does any of this impact the elements of a data wiping operation that are reasonably likely to cause a data breach.' I'm writing this because I know that the answer is a pronounced 'NOPE!'"

testimonies. What you wouldn't do is ask, "What brand of framing hammers do you use?", or "What kind of tires do you have on your utility vans?" Well this is exactly how misdirected our priorities can be when it comes to data destruction. To focus on one of the tools used to perform one of the tasks associated with the data destruction process is incredibly shortsighted. More than that, it's misguided. Based on more than a decade of experience solving problems wiping drives, I can say with

confidence that the brand of data wiping software, or the erasure algorithm being used aren't even near the top of the list of critical elements of an effective overall media sanitization process. So, how did our priorities become so out-of-order? The short answer: Marketing.

It's not surprising that the more often something is repeated, or the more loudly it is stated, the more relevant that thing appears to be. If you need any evidence of the previous statement, critically review any recent "scandal", whether it be sports, politics, or any other polarizing field. It's "more probable than not" that, through unbiased analysis, you'll see a massive gap between the conveyed magnitude of a particular fact or allegation, and its actual real-world importance.

Back to data destruction, in the United States in particular, we have only general guidelines to help us make decisions about how to wipe data from electronic storage media. We don't have any commercial certifications for data wiping tools (which provide nominal value, anyway) and the only *process* certifications for data wiping, in my experience, tend to permit some very dangerous behavior (unsupported or out of date data wiping tools, nondescript device handling practices, marginal personnel training, etc.). So we're left with little dependable guidance as to what really matters when it comes to the process of wiping drives. Data wiping software companies are of course obliged to answer the call for guidance.

Since I started in the field of media sanitization in 2006, I've seen data wiping solution-providers paint a picture of security that is (surprise, surprise) based almost exclusively on the unique features of their respective products. I was guilty of the same thing when I was selling the first commercially available tool dedicated to performing ATA Security Erase on drives. The product was insanely expensive, but the belief was, unless you could perform this one data erasure method, you'd be at risk. Fast forward a few years (when the aforementioned product was no longer relevant), and data wiping software companies began the EAL (Evaluation Assurance Level) race. They worked to develop a government standard against which their products could be tested, and then would receive a sort of certification that the product performed the wiping procedure on a set of drives to that standard. First was EAL 3. Then EAL 4+ (which is obviously one-third again as good as 3, and then some... right?) Most recently, we have companies claiming, and even patenting, exclusive capabilities to perform erasure algorithms that will effectively wipe SSDs, including areas of the SSDs simply not accessible using lesser methods. After holding season tickets to this same show for over a decade, the most obvious question to me has become, 'Does any of this impact the elements of a data wiping operation that are reasonably likely to cause a data breach.' I'm writing this because I know that the answer is a pronounced 'NOPE!'"

2 "WHAT'D I MISS?"

I've seen data get out... many times. We call it a breach-level failure. I've seen unsanitized drives shipped to customers, despite having been "successfully wiped". I've analyzed how and why it happened, and helped



"Perhaps most interesting is that even while we impugn the security reliability of multi-billion dollar software and OS providers that have massive regression and vulnerability testing budgets, we take as gospel the testimony of a data wiping software that may have been developed by, at most, a handful of engineers in a lab environment that may not even have access to the type of storage we're wiping."

organizations take corrective action and eliminate the original vulnerabilities that led to the process failure(s). The causes for the various failures have varied somewhat, though they all share one commonality. We'll get to that later, but first: The causes.

2.1 SOFTWARE

We're generally conditioned to believe that if a reputable data wiping software reports a successful or "Passed" wipe, that the drive has indeed been successfully wiped using the specified erasure algorithm. There should not be any original user data remaining on the drive. From repeated personal experience (especially since the Validator was introduced), I've witnessed multiple versions of multiple brands of professional, popular data wiping software tools report successful wipes in the field, and found the drives to not only contain logical user data, but in some cases to not have been wiped whatsoever. In one instance, the same software vulnerability existed for nearly two years without a recall, bug fix or even a technical bulletin or guidance document from the developer.

In no other industry will you find a critical process executed with the kind of blind faith that data destruction professionals place in the erasure results reported by data wiping tools. Perhaps most interesting is that even while we impugn the security reliability of multi-billion dollar software and OS providers with massive regression and vulnerability testing budgets, we take as gospel the testimony of a data wiping software that may have been developed by, at most, a handful of engineers in a lab environment that may not even have access to the type of storage we're wiping. To use a phrase President Reagan famously borrowed, everything we know about the nature of software development tells us we should take a "Trust but verify" approach to data wiping.

Third party testing and certifications can tell us how the product is capable of performing under the specific available set of test conditions. While this is useful data, by no means is it a replacement for internal quality control practices. Independent lab testing by a third party has minimal relevance to how the product will perform in a different environment, on different storage, using a different release or version.

2.2 MEDIA SEGREGATION

The vast majority of cases in which improperly sanitized, failed, or entirely un-sanitized devices (we often generalize all of these as "Red" status devices – they're still likely to contain user data) have made it through the data wiping process as "wiped" have been a direct result of an individual physically putting unsecured drives in the wrong place. Unloading large quantities of drives from a data wiping appliance or a bank of servers becomes a very repetitive task for technicians. It's not reassuring to consider that, on Thursday, the second-shift technician will put five un-wiped drives in the "Passed" pile, but most of the time that's exactly how it happens.

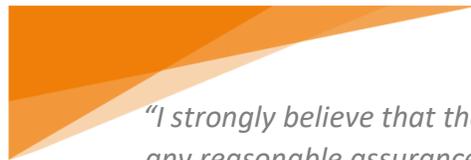
Another cause of failure related to segregating "Red" status devices is a systemic inability to actively track the media through the wiping process. In other words, how clear is it to everyone in the building when "Red" devices are not yet under lock-and-key? How much time are they allowed to spend in receiving? Which employees may access them during these times? What tool can someone use to check the status of a particular device to determine whether it is "Red" or "Green" (sanitized of all user data)? These are examples of questions that can quickly measure the integrity of a process to

determine how vulnerable it is to a media-handling related failure. Many environments simply lack the asset tracking capabilities to monitor this at an adequate level, creating vulnerability.

2.3 HARDWARE

The most difficult type of data erasure failure to diagnose is a hardware error. Errors with the drives, enclosures, controllers, even the host system can create very unpredictable and sometimes (obnoxiously) inconsistent behavior in the data wiping process. So much so, in fact, that I've often coached clients that if the quality control procedure reveals a problem in the data wiping operation that makes no sense, it's probably hardware-related. As an example, I've actually seen a data wiping system write random, unexpected characters during an otherwise "repeating-sector" wipe because of what we eventually discovered to be a RAM error.

The point is that hardware issues can, and do, affect the performance of a data wiping operation, and sometimes the impact can be difficult to detect. Sometimes these errors are benign (as in the example above), and in some cases they can invite breach-level process failures.



"I strongly believe that there will never be any reasonable assurance that hardware, software, and media segregation procedures will be incapable repeating, in some form or another, the failures I've already seen many times."

3 IT WILL HAPPEN TO YOU

Whenever I am dealing with another discovered media sanitization process failure, the question I find myself asking most is: "How many times has this occurred prior to discovery, in this or any environment?" I often wonder how many people even know to look for a problem like the one we've discovered. How many organizations even have the tools or processes in place to *detect* it? The next question is, "How many types of process failures have I yet to see? What don't I know about yet?"

I strongly believe that there will never be any reasonable assurance that hardware, software, and media segregation procedures will be incapable repeating, in some form or another, the failures I've already seen many times. Furthermore, it stands to reason that each of them will, at some point, exhibit new problems that will need to be solved. Each of these operational elements is a perennial vulnerability in the data erasure process, and any organization that performs data wiping is susceptible to them. However, the fact that there are vulnerabilities associated with the individual elements of a data wiping operation does not mean that the overall process needs to be vulnerable. In fact, recognizing and accounting for these potential weaknesses is, in my opinion, the most important step in building an ironclad data wiping operation.

4 THE BULWARK

I mentioned before that, without exception, every breach-level data erasure process failure that I've analyzed had one thing in common: It could have been prevented through *process*; through a systemic, aggressive, realistic set of checks and balances that ensures that the integrity of the entire data erasure operation is not hinged on any one single component. Data destruction professionals must create an

overall process that does not rely on the flawless performance of the personnel or the tools in place; a process that accounts for technician errors, software misreporting, and physical security lapses, and still functions as needed to prevent such errors from becoming a breach-level failure.

A strong process of course requires quality tools, and seamless integration of those tools. It requires competent and trained (and retrained) personnel. It requires scrutiny, specificity and scalability in quality control. First and foremost, however, it requires realism on the part of its administrators. Any data destruction professional who believes that, because of the tools in which they've invested, or the manager they've hired, their operation is impervious to major security risks has thrown out the lynchpin of any strong media sanitization process: vigilance.

Michael Cheslock
DestructData, Inc.
Vice President, Technology & Sales