Tech Commentary

Identifying & Correcting Failures in the Media Sanitization Process

Michael Cheslock
DestructData, Inc.
Vice President – Technology & Sales-
May 1, 2013

DESTRUCTDATA
MEDIA SANITIZATION SOLUTIONS

IT professionals and data security solution providers who perform hard drive sanitization are trusted to effectively and completely eradicate data, thus protecting sensitive information from being compromised. Data destruction standards and guidelines outline ways to properly execute this process. From those standards and guidelines, organizations create and implement processes and deploy solutions that enable them to sanitize a wide array of formats, often in very high volumes. In this way, a data destruction process is not unlike a manufacturing process: Identify the objective, create a process, deploy the tools to meet the objective and measure the result. Unfortunately, the one area where media sanitization processes have come up short (especially compared to manufacturing processes) has been in measuring the result; a step most commonly known as Quality Control.

In any manufacturing operation, you will find a rigorous QC process that ensures the entire manufacturing process has achieved the objective. In fact, there are industry certifications that focus on this QC process, as it is often the best litmus test for a successful manufacturing operation.

Before late 2012, such QC practices were almost completely absent from media sanitization processes, and there were no guidelines in place requiring it, and few even recommending it. The existing sanitization process was considered to be adequate, and quality control redundant. That situation is rapidly changings, as evidenced by the changes to the most recent revision of NIST Special Publication 800-88, which has become the lynchpin of data sanitization standards. Section 4.7 of the new document focuses specifically on the verification process and has been significantly expanded. This update reflects the increasing focus on total quality control for any data erasure process, reducing risk and providing higher levels of data security.

From this point forward, recognizing that media sanitization is a process with several potential points of failure, and that those failures have snowballing consequences, an independent quality control measure is clearly warranted. Without this, any operation can only hope that their entire process is perfect, and that it is perfect every time. But when it comes to data security “Hope is not a strategy.” Simply running a separate “verify” pass after the erasure [step] provides almost no added assurance that the sanitization was successful, as it is not an independent process.

Annual external audits performed by certifying authorities have often been regarded as the answer to this problem. The biggest shortfall to this solution is the infrequent periodicity of audits in contrast to the regularity with which the sanitization process is executed. In other words, these audits only tell you whether you got it right *that time*. Industry leading certification bodies have recognized this limitation, and have begun developing policy that holds media sanitization operations to a more rigorous standard. Organizations need a way to ensure they are consistently achieving complete data security: they need a quality control process. So, what does a media sanitization quality control process look like?

In order to answer this question, we will start by identifying each of the potential points of failure within a media sanitization process so the QC process can address each of them adequately. Those points of failure are the *Software*, the *Hardware* and the *Execution*.

Points of Failure

The Software

Many organizations use reputable, industry-recognized data erasure software. For these organizations, so long as the software is kept current and a valid support contract of some type is in place, there should be little to no concern about a potential failure of the software to perform. In addition to these products, many organizations have either developed their own data erasure software (either in-house or through a contractor or university lab), or utilize older software tools that are no longer supported or updated. These scenarios call for an increase in the frequency of auditing and quality control.

The broad install base of well-known data erasure software tools is one of their biggest advantages in terms of dependability. The industry's leading erasure software packages have been subjected to many times the number of different hardware configurations and storage platforms as have homegrown tools. In addition, these packages have often been independent tested by various private and government agencies in order to achieve various accreditations that validate their effectiveness on a sample of media. All of this helps to identify any anomalies or irregularities associated with various scenarios, and allows them to be corrected in the ongoing product development cycle. This process is very difficult to duplicate when software is only subjected to a limited scope of hardware in only a handful of operating environments, or when a dedicated development team is not maintaining the product. Changes in technology may outpace the development curve for an in-house tool, while driver limitations, chipset support, drive firmware and a host of other factors could limit the software's capabilities. In some cases, the result could be a false indication of complete erasure, where more extensively used software platforms are prepared for these situations.

The Hardware

In addition to the software, there is always a hardware factor. Every data erasure scenario is a little bit different. There are virtually endless combinations of hard drive interfaces, storage platforms, interconnects, chipsets, storage formats… components that are in between the erasure software and the data on the drives. This high level of variation introduces a level of uncertainty that increases the need for implementation of a quality control program. Consider that any quality manufacturing process, which by its very nature relies on the same hardware and software every day, involves QC. Why would an operation with as many variables as data erasure not also require such process validation?

The fact is the erasure software can only sanitize the storage it sees; it cannot make up for any limitations associated with the hardware on which it is hosted. Not all organizations

will use industrial data erasure appliances to execute data erasure, especially on PCs. So it is critical that an organization be able to verify that their process is working, on-demand, every time there is a concern, such as new drives or unfamiliar hardware.

The Execution (human error)

"Erased drives go here. Un-erased drives go here." "So, what are these?" "Um…"

Execution starts with having an ironclad policy and procedure for media sanitization, from the first touch to the last. Any certifying body that deals with data protection will require an organization to have this policy in writing. The next element is having the right tools to execute the written plan. These tools obviously include the software and the hardware. Lastly, trained, competent operators are needed. Folks who understand the value of the data they are protecting, are sensitive to the consequences of not doing so, and have the technical and organizational skills to implement the process as written… every single time.

In many equipment-processing environments where the media being sanitized is sold as refurbished storage, operators are normally encouraged to maximize production in an effort to fill standing orders. Sacrificing productivity for security is a very unlikely choice for an operator to make on his or her own, as throughput is the most evident measure of that operator's value to the organization. This creates a potential disconnect and even conflict between the organization's priorities and the operators'.

No organization can create a process that is immune to instances of improper implementation, and this is another primary driver for having a QC program. In a process that is "human-centric", training is paramount. An operator who makes a mistake is likely unaware of the mistake, and will therefore repeat the error. One miniscule step that isn't followed correctly; one option not selected in the software; one setting not changed in the BIOS, and the execution will not be correct. The end result may not affect security every time, but there is no arguing the inverse relationship between how closely execution is monitored and controlled, and the level of exposure to a potential breach.

QC Challenges

Given the three main points of failure against which a Quality Control process needs to be measured, it seems obvious that, in order for the QC to be effective, we'd need to exchange these variables for an independent perspective. In other words, we'd need to use different software, different hardware, and a different operator in order to say that we have effectively audited the media sanitization process and validated that it is working properly and as expected. Not doing so would simply invite a repeat of any process breakdown, and complete assurance of process effectiveness would remain out of reach. Unfortunately, there are some very real challenges with creating a media sanitization quality control process to account for all of these potential points of failure.

Cost

Relying on third-party audits as the exclusive quality control measure is cost-prohibitive when executed against an adequate sampling of processed media. At $300-$500 per drive for such a service, this simply is not a scalable option. An independent internal process is clearly more desirable.

Our ideal configuration would be a dedicated software program hosted on a dedicated hardware platform (or series of them, for that matter) run by a dedicated employee: A virtual duplication of the original data erasure operation, it would see. Yet, even though only a percentage of sanitized storage would need to go through QC, having dedicated hardware and software to perform this task could involve substantial cost. Furthermore, analyzing hard drives to validate that data was successfully erased (let alone erased using the intended method, and that any other aspects of the data destruction process were followed as specified (drive fingerprinting, HPA & DCO clearing, G-list tolerances, specific wipe algorithms, etc.) is likely to demand a very highly trained storage engineer.

Implementation

How much space will our QC equipment occupy? How many man-hours will it consume? If we are going to a customer location to perform on-site erasure services, how can we possibly execute this on-site? In addition to the direct costs of adding a complete QC process to a media sanitization operation, there are a host of other indirect factors, such as internal space or the portability of the process.

Process Control

Even though the dedicated QC equipment must use *different* hardware and software than the sanitization equipment, as discussed previously, it is still likely to be comprised of an operation system, storage controllers, chipsets, BIOS, and other 'moving parts' in the QC operation. It is therefore no simpler than the original sanitization equipment, and subject to its own points of failure. In other words, **if we audit one complex system with another complex system based on the dubious assumption that the points of failure between the two will not align simply because there are variances between them, we cannot assure that the QC is adequate.**

What is needed, then, is a simplified design that reduces the potential for systemic issues and can be rigorously tested and deployed repeatedly.

Introducing: The Validator

DestructData, an industry leader in the design, implementation and support of data destruction solutions for the industry's most demanding applications, has teamed up with

CPR Tools, one of the world's most respected data recovery firms, to develop the first commercially available data erasure QC appliance: the Validator.

The Validator is an ultra-portable, easy-to-use tool designed exclusively to analyze up to four hard drives at once to determine if and how they have been erased. It successfully addresses the need for independence in hardware and software, eliminates the need for a highly trained operator, and can be used anywhere to support on-site services or in-facility operations.

The Validator uses direct IDE or SATA connections (up to 2 of each) to cable directly to drives, eliminating the need for complex operating systems and hardware. It is purposely designed without the ability to write data to drives, so as to prevent any false reporting of failed erasures. The Validator not only checks to ensure that a drive was erased, but is able to determine whether the drive was erased to an intended specification. It looks for:

- Erasure type used (repeating random pass by sector or same character wipe, and even which character)
- Presence of Host Protected Areas and Device Configuration Overlays (can be disabled)
- Presence of a "fingerprint" or "stamp" on the drive's first block (can be disabled)
- The number of grown defects on the drive (can be disabled)
- Whether there is an ATA lock activated on the drive

These tests validate that an organization's procedure is being followed correctly and completely. This level of detail ensures that even small, unintended variations in the implementation of a media sanitization process can be identified and corrected *before* they begin to create risk. It can also highlight whether certain operators are more likely to make mistakes in process implementation, which can be an indication of overall process integrity, even if true security violations are not always identified.

Using the Validator as a standalone QC sampling tool to provide a quick "Pass / Fail" indication accomplishes a lot to strengthen a media sanitization operation, but its capabilities can also extend to the audit trail. With a complete reporting system that can produce validation reports in .html, as well as the ability to export logs for integration into an external asset management database, auditors, customers and/or managers can clearly see the frequency with which QC is implemented, and on which drives. Exporting the logs and reports is performed by connecting the Validator to any Windows PC on which the included Toolbox software has been installed. Aside from the reporting features, the Toolbox software plug-in allows users to actually view any sectors on failed drives that were found to contain data.

The Validator can be used to perform partial (1%, 5%, 10% or 25%) validation, or a complete, 100% erasure verification, all exactly according to the National Institute of Standards and Technology's (NIST's) sampling algorithm for sanitized media. Partial verifications are an effective way to execute regular, very fast checks to determine

whether drives are actually being processed. A drive that was "missed" completely by the sanitization process will likely fail even a 1% verification in less than one second, and a successful partial validation can be executed in as little as 30 seconds. Partial validation, however, is not adequate QC for the effectiveness of the hardware and software involved in the media sanitization process, as it does not check every sector for data. Partial validations should be considered a complement to periodic complete validations as opposed to a replacement for them. Performing occasional full validations (particularly when new hardware or software is being addressed) along with regular partial validations allows for both high sampling rates and complete QC.

As discussed, one of the major hurdles in implementing a complete media sanitization quality control process is the ability of the operator(s) to know what to look for, and how to look for it using the tools at their disposal. The Validator requires configuration only once, a simple procedure performed by answering a series of process questions. There is no guesswork involved for the operator. Operating the Validator is actually a simpler task than performing media sanitization and requires very little training. With a push-button interface and easy menu navigation, an inexperienced technician can be fully capable of administering a comprehensive media sanitization quality control process 15 minutes from opening the box.

Developed completely independent of and sharing absolutely no code with any data erasure software, the Validator is a true 3rd party auditing tool. So, no matter what erasure software is used, any limitations or bugs that may exist in the sanitization process are not duplicated in the tool. The same goes for the hardware. Its single-purpose design eliminates all the variables of using PC hardware or enterprise HBAs to address the target storage for erasure validation.

Every important process requires some level of quality control, and even the use of quality tools and solid operating procedure is no excuse to ignore this critical step. In the absence of a cost-effective, easy-to-implement process, organizations will always compromise, even at the sacrifice of data security. The Validator effectively addresses each of the potential points of failure in a media sanitization operation by creating an independent testing environment, and simultaneously eliminates the cost, implementation and process-control hurdles that would otherwise be associated with achieving this goal. As the data destruction community continues to realize that data security is no less important than the scores of industries that are heavily regulated and require strict quality control measures, and as certifying bodies like NAID, R2, e-Stewards, ADISA, and standards creators such as NIST recognize this through new, forward-thinking mandates to their respective industry-segments, the Validator is a timely solution to the external pressures and internal concerns of data destruction professionals.