The Paper Paradigm: A Call for a New Electronic Standard to Govern Digital Data Destruction

By Roger Hutchison
President, CD ROM, Inc.
August 2009

Summary: Without exception, all major pieces of legislation which address privacy of information in some form to include HIPAA, SOX, GLB, FACTA call for the safe destruction of the digital content on electronic media once that data has reached its end-of-life usefulness. These legislative milestones did not anticipate recovery techniques available for the reconstruction of data on damaged electronic media, nor advancements in technology which now permits literally millions of pages of data to be contained, for example on a CD-ROM disc. The obsolete processes used in nearly all government agencies and businesses is shredding, based on an antiquated and dangerous paper shredding model. In all cases, there is a lack of definition on what constitutes the safe destruction of digital records on electronic media. This briefing paper establishes a specific paradigm of best safe practice of digital records and calls for a new national standard to govern sensitive or classified information.

Background: On November 4th, 1979, the American Embassy in Teheran was overtaken by forces loyal to the Ayatollah Kohenmeni. Fifty-three unlucky American citizens, also diplomats, were kidnapped and held hostage for 444 days. During that same time, I lived in a mud hut in Botswana and virtually all my information about World events was from three short wave broadcasts: Voice of America (USA), Peace and Progress (Moscow) and BBC (London). That date was also the birth of the new electronic paradigm governing technical processes we could as a Nation use to destroy the digital data contained on electronic media which held classified materials up to and including Top Secret. The reason for this paradigm shift is based on a little known and even less discussed fact that the Ayatollah commissioned a large number of carpet weavers use to dealing with 300-400 strings per inch to go into the communications room of the Embassy and to reconstruct the paper documents which contained some of our Nations' secrets.

Case Study: Fast forward to May 2006, when a single laptop computer containing unencrypted information on the social security numbers of 26.5 million U.S. veterans was stolen from a Veterans Affairs analyst's home. The VA employee clearly violated the then existing VA policy by removing the sensitive information from his office. Soon after, on August 3, 2006, a computer containing personal information on 38,000 veterans went missing. The computers were eventually recovered and on August 5, 2006, two men were charged with theft. While the second missing computer only contained 38,000 or so records, compared to the first one which contained 26.5 million, the cost to tax payers was $160 million for the Senate approved funds to monitor the credit reports for those 26 million veterans, and it is widely reported that the VA itself spent over $25 million internally to send letters notifying the veterans of the compromised personal information they may have suffered. This case study would have identified the value of the information, which was not classified but simply "sensitive" as a Tier 3 project. However, the damage caused to the VA and the extraordinary cost to repair the damage would, in hind sight, have recommended to their security team a Tier 5 process governing the entire chain of custody of the sensitive Veteran's personal information.

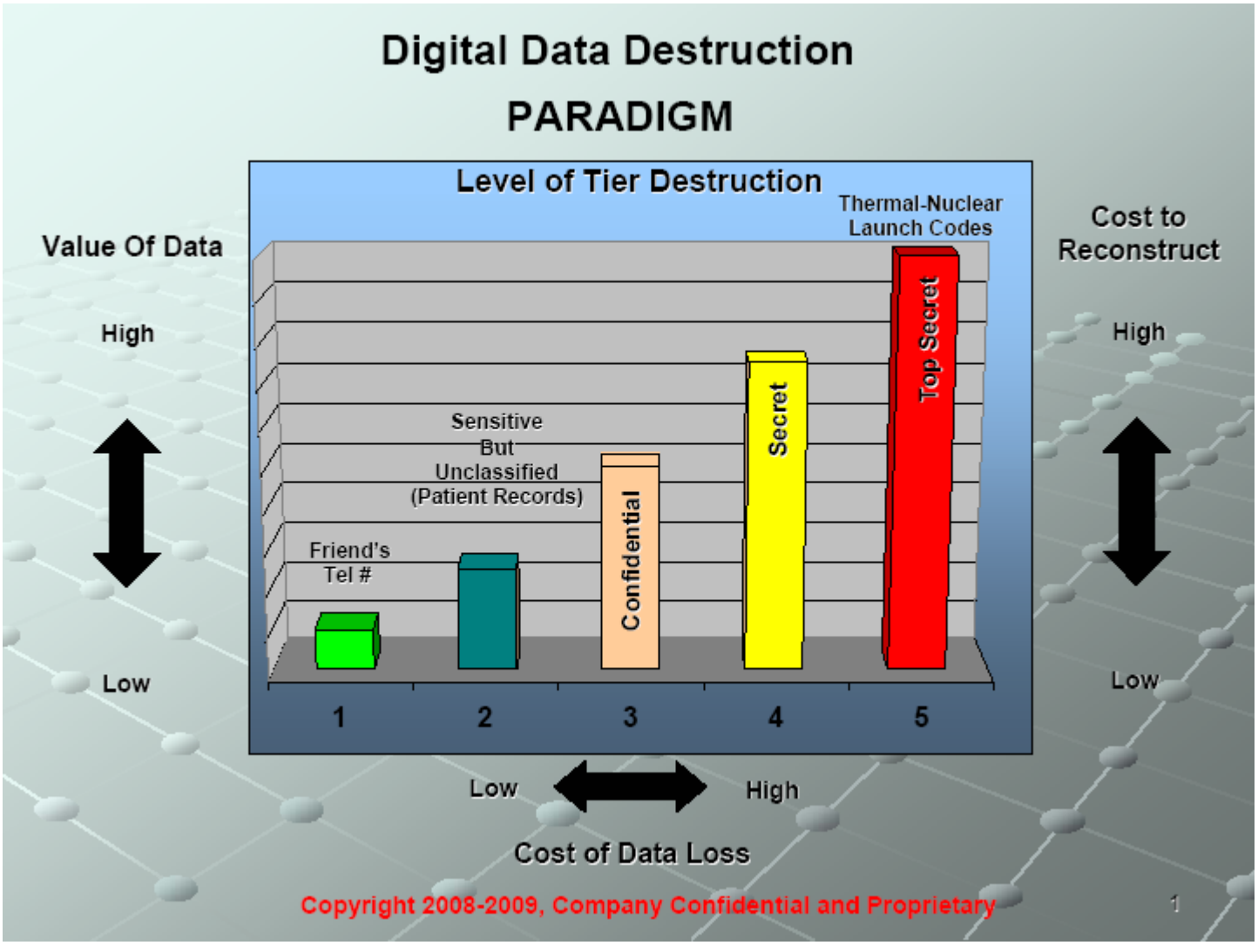
National Standard Missing: The fact of the matter is that short of a very few well informed government agencies and even fewer still commercial enterprises, who deal with electronic media destruction processes and recreation techniques, there is still no national standard which governs the best safe practices to destroy digital data on electronic media once it has reached its end-of-life cycle and is no longer useful. What can we do, and perhaps more importantly, what should we do, to protect the digital information of our Nation and those who work and serve within our Country? We need a concise, easily understood and implemented National Standard which governs both sensitive corporate information on digital media, as well as one for Government agencies who deal with classified data.

To address this important and timely question, we have to break this complex problem down into reasonable and well-defined components. Surely, protecting your friend's telephone number on your cell phone that you just threw away is not the same issue as protecting the launch sequence codes for thermo-nuclear weapons. However, I would argue based on a multi-year academic study of this esoteric field and several years of experience building "fail safe" systems for our classified military to use which renders digital data "beyond forensic recovery", that the friend's phone number and the nuclear launch codes lie on a continuum, and specific tools and processes should be applied to the destruction of digital data based on the simple concept of "best safe practice".

Today what do we have as alternative technologies to think about the problem? Unfortunately, we have the old paper model, the analog paradigm, to consider.

This model is also fortunate in that it gives us a starting point and way to conceptualize a vastly enormous process and make it readily understandable both intellectually and visually. When you go to your favorite office supply store, you instinctively buy a paper shredder based on the sensitivity of the paper you will be shredding. The paper model has a 5 tier approach. Tier 1 is the simple cross cut shredder while Tier 5 is the much more expensive paper shredder whose only technical characteristic differentiator is “size of the paper piece”. A Tier 5 paper shredder uses a 1mm by 5mm permissible size and this translates (remember that Ayatollah guy) into a paper shredder suitable for classified data.

What we can implement as a working model, until such time as a new National standard emerges, is an adoption of this Tier 1 to Tier 5 model as applied to electronic media with reference to the sensitivity of the information, as well as the cost and effort to reconstruct. See the insert “Paradigm” below which offers a new approach and way to move forward to develop such a new National Standard.



First, define the sensitivity of the information. A good way to do this is to imagine that your corporate rival, or military adversary, had access to the information, or part of it, through forensic reconstruction techniques. If your business rival had access to your friend's phone number, would it hurt your business interests? If you had a medical condition which became known to the public from improper destruction of your medical records on a CD disc, would you be harmed and what would the cost be to revalidate your reputation? If an adversary of the United States could reconstruct the list of foreign operatives working for us in remote corners of the world, what harm and what cost would be forced upon us to recover from such a breach of military secrets?

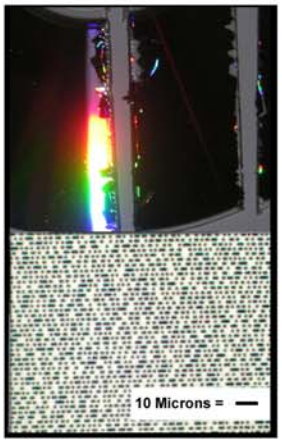
When we consider both the products and the services for electronic media destruction of media containing sensitive or classified data, outside of the few three digit Government agencies who are very well aware of this issue, there is no mechanism or paradigm in place beyond the paper model. This Tier 1-5 paradigm for electronic media can be applied on a media specific basis. For example, in this second graph on "Summary of Alternative Technologies for Data Destruction on Optical Media", we show 5 technical approaches based on 5 increasingly secure technical processes with relative ease to reconstruct data on the left, or Tier 1 and virtually impossible to reconstruct data on the right, or a Tier 5 methodology. This can be applied to hard drives, see graph 3 below, tapes, in graph 4 below, and in flash and other solid-state media, graph 5 below .

Summary of Alternative Technologies
for
Data Destruction on Optical Media

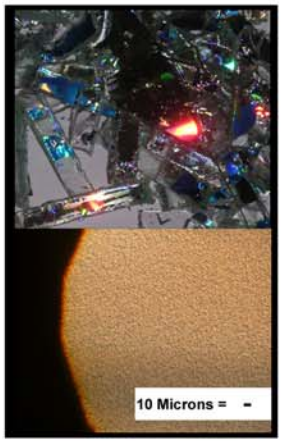
Tier 1	**Dimpling**- a process which puts a square impression on the surface of the discs
Tier 2	**Strip Cut Shredding**- a modified paper shredder which cuts straight across the length or width of the discs in various widths the smallest being about 7mm
Tier 3	**Cross Cut Shredding**-a modified paper shredder which cuts squares or rectangles in various lengths and widths the smallest being @ 5mm by 5mm
Tier 4	**Disintegration**-used for currency destruction; a cross cut type of process which in currency produces rectangle or square pieces about 4mm by 4mm.
Tier 5	**Grinding**-a process which grinds the entire coating layer and chemical substrate from the surface of the discs. In the case of DVDs, they must first be split, then ground.

Tier 1
Dimpling
85-100% of
data remaining

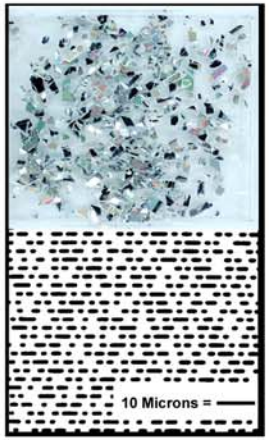
Tier 2
Strip-cut Shredding
65-85% of
data remaining



Tier 3
Cross-cut Shredding
35-65% of
data remaining



Tier 4
Disintegration
15-40% of
data remaining



Tier 5
Grinding
0% of
data remaining

Dr. Roger Hutchison
E-mail: rshutch@cdrominc.com T: 952.832.5424

Summary of Alternative Technologies for Data Destruction on Hard Drives

Tier 1	**File Deletion/Erasure** via computer Operating system only removes the file index - data remains
Tier 2	**Physical Alteration** prevents the hard drive from being accessed from a conventional computer – data remains and can be accessed via forensic procedures
Tier 3	**Overwrite** replaces data with non-sensitive data. Software required to accomplish this overlays the operating system and, therefore, is vulnerable to malware attack. Additionally, reallocated (error) sectors and extra partitions are usually missed.
Tier 4	**Secure Erase** is built in to the hard drive firmware making it less susceptible to malware attack. Completely erases all data to include reallocated sectors.
Tier 5	**Degauss & Disintegrate** neutralizes the magnetic signal that represents data. Disintegration results in disk pieces too small to recover useable data. Combination of these two processes completely eliminates the possibility of forensic recovery with any known technology.

Tier 1
File Deletion

- Indexing removed, data remains

100% of Data Recoverable

Tier 2
Physical Alteration

- Drill Hole in Platters
- Crush Electronics (platters intact)

50-60% of Data Recoverable

Tier 3
Overwrite

- NIST SP 800-88 Single Pass
- DoD Directive 5220.22 (Triple Pass)

10% of Data Recoverable*

Tier 4
Secure Erase

- (Proposed for Classified Secret or Corporate Sensitive Information)
- Secure Erase
- Degauss Non-NSA Equipment (<5,000Oe)

3-5% of Data Recoverable*

Tier 5
Degauss & Disintegrate

- (Proposed for Classified Top Secret or Corporate Confidential Information)
- Degauss NSA Evaluated Equipment (5,000Oe)
- Disassemble and Recycle Components

0% of Data Recoverable

*Based on human error and age of drive

Dr. Roger Hutchison
E-mail: rshutch@cdrominc.com T: 952.832.5424

Summary of Alternative Technologies for Data Destruction on Tape Media

Tier 1	**Overwrite** only removes the file name, data remains 100% intact
Tier 2	**Physical Destruction** via cutting only prevents the data from being retrieved where the tape is spliced.
Tier 3	**Chopping** is only a soft means of destruction if the particle size is beyond superior recovery tools including MFM microscopes
Tier 4	**Degauss** with low strength degaussers will only damage the digital signal. Forensic tools including MFM microscopes can be used to remove large amounts of content
Tier 5	**Degauss & Disintegrate** neutralizes the magnetic signal that represents data. Disintegration results in pieces too small to recover useable data. Combination of these two processes completely eliminates the possibility of forensic recovery with any known technology.

Tier 1
Overwrite

- Only removes file name, Data still 100% intact

100% of Data Recoverable

Tier 2
Physical Destruction

- Cut Tape - Large amount of data remains

95% of Data Recoverable

Tier 3
Chopping

- Chopping a tape
- Data is still recoverable

25-75% of Data Recoverable*

Tier 4
Degauss

- Degauss non-NSA Evaluated Equipment

25-50% of Data Recoverable**

Tier 5
Degauss & Disintegrate

- (Proposed for Top Secret or Corporate Sensitive Data)
- Degauss NSA Evaluated Equipment
- Disassemble and Recycle Components

0% of Data Recoverable

* Depends on particle size
** Depends on field strength of magnets

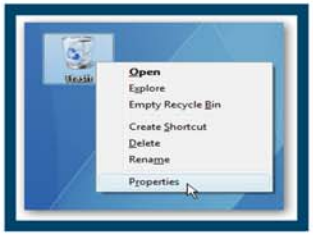
Dr. Roger Hutchison
E-mail: rshutch@cdrominc.com T: 952.832.5424

Summary of Alternative Technologies
for
Data Destruction on Flash Media and Solid State Hard Drives

Tier 1	**File Delete** 100% of the digital information remains. Good only for cosmetic purposes.
Tier 2	**Physical damage of the case** Breaking the flash device in half can leave up to 100% of the digital data retained on the solid state medium inside the flash or solid state HDD. Requires re-assembly of memory medium in a new external case.
Tier 3	**Physical damage of the memory component** This requires lab level reassembly. Due to file structure on flash and solid state devices, and based on the extent of the damage, this would be considered safe for sensitive information.
Tier 4	**Physical destruction of the entire drive or flash unit** If physical destruction is conducted to a 1mm by 1mm particle size, it would take heroic efforts to reconstitute any information. Proposed for Classified Secret containing data
Tier 5	**Disintegration and melting, or autoclaving** This alters the material composition of flash and solid state memory. The physical alteration removes all digital records. Proposed for Classified Top Secret containing data.

Tier 1
File Delete

- Only removes file name,
- Data still 100% intact
- Good only for cosmetic purposes



100% of Data Recoverable

Tier 2
Physical Case Damage

- Breaking the case reults in digital data retained on the solid state medium
- Requires reassembly of memory medium in a new external case

Up to 100% of Data Recoverable

Tier 3
Physical Damage of Memory Component

- Requires lab-level reassembly
- Due to file structure on flash and solid-stae devices and based on extent of damage, this would be considered safe for sensitive information

Percentage recoverable by lab analysis in process

Tier 4
Physical Destruction of Entire Drive or Flash

- (Proposed for Classified Secret or Corporate Sensitive Information)
- Physical destruction results in pieces 1mm by 1mm or less
- Would require laboratory level forensic recovery

Percentage recoverable by lab analysis in process

Tier 5
Distintegration, Melting or Autoclaving

- (Proposed for Classified Top Secret or Corporate Confidential Information)
- Alters material composition of flash and solid state memory
- Physical alteration removes all digital records

0% of Data Recoverable

Dr. Roger Hutchison
E-mail: rshutch@cdrominc.com T: 952.832.5424

Conclusion: Based on this lack of definition, we propose that all electronic media be categorized first in terms of sensitivity of the information. Second, we propose that all technical processes and equipment be categorized in terms of these same levels or tiers of differentiation. Third, we propose that a national standard be developed, possibly under the auspices of NIST on the commercial side and the National Security Agency on the classified side, which suggests a specific guideline and process to follow based on the "tier" of the data. In this new electronic paradigm, we also have five tiers of data sensitivity and we apply the best safe digital data destruction practice to the level of sensitivity of the data.

Surely, however, serious consideration needs to be given to just how much it costs to correct problems once they occur from data which we could easily classify as Tier 3 sensitivity. I would place the VA medical records and social security numbers in the Tier 3 category. The question to ask yourself, as perhaps a security specialist who deals in this realm on a daily basis, is what is the current practice of your organization or business within this new electronic paradigm?

The obvious answer is, given the sensitivity of the information and the ease of retrieval, not good enough.

To contact the author: rshutch@cdrominc.com