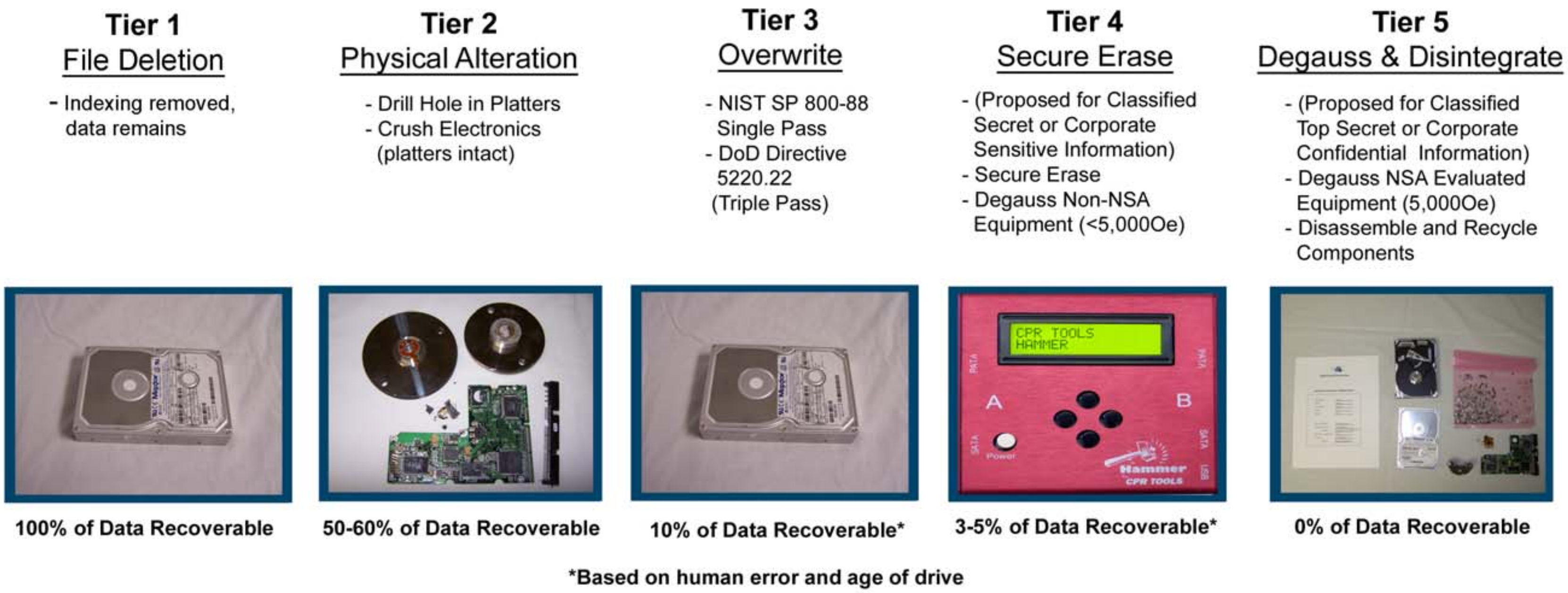
Summary of Alternative Technologies for Data Destruction on Hard Drives

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

Confidential & Proprietary
Excerpt from The Humpty Dumpty Scenario; Part III

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