



TIME IS MONEY

The true cost of using software to erase hard drive data.

Daniel F. Bayha, Vice President

Back Thru The Future Technology Disposal
150 Main Street
Ogdensburg, NJ 07439
973-823-9752
shred@backthruthefuture.com

June 19, 2009



Most commercial organizations use software erasure programs to destroy data on hard drives prior to disposal.

The software records meaningless data over the top of the previously recorded data. The more times you overwrite the entire surface of the disk, the more secure the data erasure effort.

DOD standards require at least three over writes. The purpose of multiple overwrites is to address the problem of data overlay. A hard drive does not always record a bit of data in exactly the same place.

Thus, a portion of a previously recorded bit of data may still be recoverable after a single pass over write effort. Forensic data recovery statistics show that approximately 12% of previously recorded data may be recoverable after a single pass, approximately 4% may be recovered after a second pass and less than 1% after the third pass. Keep in mind that this recovery can only be achieved by using very sophisticated and expensive data recovery tools.

It takes anywhere from 30 seconds to 3 minutes depending on the erasure software to make a single overwrite pass over one gigabyte of previously recorded data. Thus, it would minimally take 30 minutes to overwrite a 60GB hard drive once. A DOD standard (three pass) overwrite would take one and one half hours. As the capacity of hard drives grows, the amount of time required to erase the drives using overwrite technology grows proportionately. Under the best conditions, the largest hard drive commercially available today, 1.5 TB, would take nearly 5 days, 24 hours per day, to overwrite three times.

Under the best conditions, the largest hard drive commercially available today, 1.5 TB, would take nearly 5 days, 24 hours per day, to overwrite three times.

There are two advantages to using overwrite software.

- It can be performed onsite without any significant capital investment.
- It allows a hard drive to be reused.

There are two disadvantages to using overwrite software.

- It is not an absolute method of destroying all recorded data.
- It takes more and more of your limited technical resource time.

Save money while adopting best security practices as recommended in NIST Special Publication 800-88 "Guidelines for Media Sanitization".

- Use an onsite degaussing service for your hard drives
- Employ redundant data destruction tools. Redundancy of security procedures is a security best practice. Employ two different techniques to accomplish the same goal and have different entities employ the different tools.

The Economics:

Old technique:

100GB hard drive overwrite 3 passes = 4 hours @ \$20/hr = \$80.00

Sell reusable drive \$20.00

Total cost = \$60.00 per drive

Redundant technique:

100 GB hard drive onsite degaussing = \$3.00

Have hard drive shred @ \$10.00 per drive = \$10.00

Total cost = \$13.00 per drive

Savings = \$47.00 per drive

Allowing a hard drive to be reused outside of your organization's security perimeter is an all risk- no reward proposition.

Adopt the policy that all hard drives must be destroyed if they are no longer to be used within your organization. Shredding hard drives is recognized by the National Institute of Standards and Technology (NIST Special publication 800-88 Guidelines for Media Sanitization) as the best available technique for destroying previously recorded information.