

# Data and Hard Drive Destruction

Data that you erase, reformat, wipe or degauss can be restored. You already know that erasing is not 100% safe, no matter what the software promises. The actual data remains. Information thieves can restore the data you thought was destroyed. Improper destruction could lead to a costly breach.



**Reduce Reuse Recycle**



Stockpiling old hard drives leaves you vulnerable. Whether it's your IT closet, or an offsite storage facility, confidential information stored on hard drives, back-up storage and other eMedia is the target of data thieves.

Storing confidential information, in any form, is putting your organization at risk of a security breach and liability. On average, a security breach will cost a business \$5.5 million\*, not to mention reputation damage and loss of business. Why put your company at risk? The cost to destroy your hard drives is minimal compared to the potential risks you face when you don't. R3 will permanently destroy your information at a low cost that will fit your budget. Destroying a hard drive 100% is the effective way to permanently render its information inaccessible. R3's secure chain of custody ensures pick up and destruction within 2 business days (NAID). And you receive a Certificate of Destruction for your files.

\*Ponemon Institute © Research Report (March 2012) – 2011 Cost of a Data Breach Study: United States

- 1. Documenting the serial number of each hard drive for destruction, and providing a copy of the log sheet for your records.**
- 2. Securely transporting your hard drives to our destruction facility.**
- 3. Logging the manufacturer and serial number of each device before destroying your hard drives.**



- 4. Completely destroying your hard drives in our secure location.**
- 5. Sending an itemized Certificate of Destruction for your files following destruction of your hard drives.**

**Contact R3 today for your data information security solutions.**