It's no secret that our computer hard drives contain information we'd rather keep secret. Because the information security field is my home turf, I'm troubled by all the bad online advice for destroying used drives. "Bash them with a hammer in the parking lot," says one blogger. "Toast them with a blowtorch," says another. "An acid bath is the way to go," says a third.

Effective hard drive destruction is best accomplished with proven equipment that is safe, easy to use, and reliable. You deserve the assurance that no one is going to recapture a bit of data off your discarded drives. This is not as paranoid a view as it used to be. Data-recovery technology continues to advance by leaps and bounds, and there are many techniques for recovering information from seriously damaged drives.

If account numbers or other sensitive records fall into the hands of identity thieves, there is the possibility of a lawsuit from an individual harmed by the release of his/her private information.

We all have to replace computers from time to time — more frequently as newer technology makes them obsolete. But different facilities have different security needs, and that is why there are different kinds of safe and effective hard-drive-destruction equipment on the market.

A Job Worth Doing

Just one hard drive can contain hundreds of thousands of files. When a digital file is "deleted" from a computer, the information actually remains on the drive, as do "deleted" e-mail messages and records of all online activity. Lock old drives in a secure location prior to destruction. And keep records!

I strongly recommend instituting a comprehensive information-security program — written, mandatory procedures carried out by trusted, properly trained employees or a security service and supervised by management. Such procedures should include detailed recordkeeping and labeling that states, for example, the serial number of each drive, the computer from which it was removed, the date it was removed, destruction date and method(s), and a plan for in-house monitoring/verification.

TOOLS OF THE TRADE

Let's take a look at some choices for the safe removal of data:

OVERWRITING THE DRIVE

"Disk-wiping" software, when carefully chosen and used with patience by a trained and trusted individual, can replace stored data with a pattern of meaningless characters.

DEGAUSSING

The degausser must have a high enough coercivity rating (magnetic power) to overcome the drive's magnetic field and completely erase its stored information. Degaussing is more effective than overwriting, but here, too, training and careful choice of equipment are essential.

CRUSHING

Crushers deform drives with conical steel punches or similar devices. Good for a low volume of drives, these relatively inexpensive units are...
available in manual and powered models. Some information remains on a deformed platter, but it is much harder to retrieve from the shreds by a determined thief, but with great difficulty.

DISINTEGRATION
Rotary knife mills cut shreds into smaller and smaller pieces until they are unrecognizable and unreconstructible.

While all of these methods can be effective, I favor a “belt and suspenders” approach that combines degaussing with crushing or shredding. For the ultimate, choose degaussing, followed by shredding, followed by disintegration.

THE OUTSOURCING OPTION
Degaussers, shredders, and disintegrators all come in different sizes, capacities, and prices. Some decide the investment is worth the peace of mind that comes from knowing sensitive records will never leave the facility intact. Others, because they cannot justify purchasing their own equipment for the relatively few drives they need to destroy, outsource destruction.

If your data resurfaces somehow, you are still liable for damages suffered by injured parties, so if you choose outsourcing, be sure to thoroughly evaluate a destruction service before signing the contract. Here are some questions to ask:

1. Will the service pick up your hard drives and transport them in locked, trackable transport cases with tamper-proof security tags?
2. Upon arrival at the destruction facility, will your items be carefully inventoried and stored in a locked, monitored area?
3. Are job applicants thoroughly screened?
4. Is the facility monitored around the clock by security cameras?
5. What destruction methods will be used?
6. What proof will you have that items were actually destroyed?
7. Is the facility fully bonded and insured, and to what limits?

METHODICAL CHOICES PROTECT YOUR SCHOOL
Sometimes the best solution is a combination. For example, you might choose to degauss your hard drives in house and then send them to a service for the next stage, such as shredding and/or disintegration.

Although information-security programs will differ according to facility size and mission, every field of endeavor these days must address the disposal of sensitive electronic records. CSP

Andrew Kelleher is president of Security Engineered Machinery (SEM).