TELEHEALTH:
Chat and video applications transform how healthcare professionals collaborate
How to responsibly destroy hard drives

Five ways to ensure your valuable documents never get into the wrong hands.

By Andrew Kelleher

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 advice I hear about how to destroy used drives. Here, paraphrased, are some comments I found online recently:

"I just take my old hard drives out to the parking lot and bash them with a big hammer."

"Id toast them with a blowtorch if I were you."

"Cook them in the oven at very high heat and then plunge them into a bucket of ice water."

"An acid bath is the way to go."

"Shoot a hole through each one with a pistol -- the larger the caliber, the better."

Businesses that have to deal with liability, workplace safety and the disposal of multiple hard drives will have a problem with these methods.

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. The U.S. National Security Agency (NSA) has developed guidelines that require hard drives used by federal government agencies or their contractors to be degaussed (demagnetized) and physically damaged prior to disposal.

But don't think that because you aren't a government agency you don't need to be vigilant about the disposal process. There is a real risk of information falling into the nefarious hands of identity thieves, and there is the possibility of a lawsuit from an employee, customer, patient or other individual harmed by the release of his/her private

An NSA-evaluated degausser can completely erase hard drives with no chance of data recovery.

information. Hard drives can also contain information your competitors would love to see, such as price lists, sales figures, customer data, engineering data and memos drafted in preparation for bidding. The list goes on and on.

We all have to replace computers from time to time -- more frequently as newer technology makes them obsolete. Although hospitals, healthcare providers, insurance companies, banks and government/military entities are subject to codified standards of confidentiality, every business has employee records and proprietary information. But different facilities have different security needs.

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. I favor a "belt and suspenders" approach, two proven methods of data destruction. But there is more to information security
than choosing the right destruction equipment. What you do with old drives prior to destruction is just as important. Keep them in a secure location prior to destruction, or they could be long gone before you even know they are missing. 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

When is a hard drive sufficiently destroyed to prevent recovery of the confidential/proprietary/sensitive data it once held? Let’s take a look at some choices for the safe removal of data:

1. Overwriting the drive: Disk-wiping software is used to replace stored data with a pattern of meaningless characters. I felt obligated to mention this method, but I do so with reservations. There are many versions of such software on the market, so it is important that the chosen version be compatible with the drive to be overwritten. One overwriting pass is not enough, so this method must be carried out by a trusted individual who is patient and careful and understands the process.

2. Degaussing: There are two major methods of degaussing. The first method permanently erases data from a hard drive when it is passed through the magnetic fields of powerful rare-earth magnets. The second method uses a powerful electromechanical pulse that instantaneously generates a powerful magnetic field to permanently erase data from a drive in an enclosed chamber. The degaussing device must have a high enough coercivity rating (magnetic power) to overcome the drive’s magnetic field and completely erase its stored information. If it doesn’t, the whole process is a waste of time. Degaussing is more effective than overwriting, but here, too, training is essential.

3. Crushing: This method subjects drives to extreme pressure from a conical steel punch or similar device. Good for a low volume of drives, these relatively inexpensive units are available in manual and powered models. Although a deformed drive is inoperable, some information residing on its platter could still be intact, albeit much harder to retrieve.

4. Shredding: Hard-drive shredders rip drives to randomly sized strips. The process is much the same as in a paper shredder, but these machines are more robust and capable of destroying multiple types and sizes of drives. Some data could be retrieved from the shreds by a determined thief, but with great difficulty.

5. Disintegration: Mechanical incineration by a heavy-duty disintegrator (rotary knife mill) cuts items into smaller and smaller pieces until they are unrecognizable. For hard drives, this is typically done after shredding.

While all of these methods can be effective, I favor a two-stage approach that combines degaussing with crushing or shredding. For the ultimate, choose degaussing, followed by shredding, followed by disintegration.

A certificate of destruction does not free you from your legal responsibility. If a destruction contractor certifies that your confidential data was destroyed, yet the data resurfaces somehow, you are still liable for damages suffered by the injured parties.

The outsourcing option

Degaussers, shredders and disintegrators all come in different sizes and capacities. While some of these units are relatively inexpensive ($1,000 to $5,000), others could run as high as $50,000. For some businesses, the investment is worth the peace of mind that comes from knowing sensi-
tive records will never leave the facility intact. Other businesses cannot justify purchasing their own equipment for the relatively few items they need to destroy. These businesses may choose to outsource hard-drive destruction.

If you only destroy 10 hard drives a year, by all means find a reputable destruction service. If you choose this option, be sure to do your homework – thoroughly evaluate a service provider before signing the contract. Here are some questions to ask:

1. If the service will pick up your hard drives, how will it transport them to the destruction facility? Does the service offer locked, trackable transport cases with tamper-proof security tags?

2. Does the service require a long-term contract or a monthly minimum?

3. Upon arrival at the facility, will your items be inventoried by serial number (or barcodes correlated with serial numbers) and stored in a locked, monitored area? How long are they likely to remain there awaiting destruction?

4. Are job applicants thoroughly screened? 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. Will the destruction of your items be logged and certified in writing?

This heavy-duty shredder is capable of destroying up to 2,500 hard drives per hour.

is a good idea to pop in from time to time for a surprise inspection.

And please note that a certificate of destruction does not free you from your legal responsibility. If a destruction contractor certifies that your confidential data was destroyed, yet the data resurfaces somehow, you are still liable for damages suffered by the injured parties.

Methodical choices protect your business

Sometimes the best overall destruction/disposal solution is a combination. For example, you might choose to degauss your hard drives in house and then send the degaussed drives to a service for the next stage, such as shredding and/or disintegration. You still get “belt and suspenders” – by choosing two (or more) destruction methods, you protect yourself against human error at one stage or the other.

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. Confidential patient records are just as important to a small medical practice, for example, as proprietary product designs are to a large corporation. A wide selection of effective equipment is available to help a facility meet its particular needs. Part and parcel of the data management arc, data security is an ongoing process; if you understand the options, you will be in a much better position to protect yourself and your business.

HMT