The Nine Things You Should Be Destroying

By Andrew Kelleher

By now, most people have gotten the message about the need to shred important papers. The issue of identity and data theft is so widely discussed, and paper shredders are now so widely available and affordably priced, that it's hard to imagine anyone just throwing important documents into the trash. So, kudos to all of you responsible people who do the right things to protect yourselves and your businesses from information theft.

You've figured out paper, but what about other threats you might not be aware of? What about all those electronic records floating around your office? If you're not dealing with them, paper is the least of your worries.

As computers and other electronic devices become obsolete sooner and sooner due to new technology, disposal of sensitive information is of serious concern. Just one hard drive, CD, or DVD can contain thousands of files. When a digital file is "deleted" from a computer, the information actually remains on the hard drive, as do deleted e-mail messages and records of all online activity. These days it all can be recovered with sophisticated tools. This is worth remembering before donating old computers to a school or local charity, for example. In some cases, old computers are removed and resold by the vendor who installs the replacement computers.

Likewise, "dumpster divers" can obtain proprietary information from prototypes and off-spec batches of toys, clothing, and pharmaceuticals that are merely discarded instead of thoroughly destroyed.

The following chart lists some obvious and not-so-obvious items that could cause significant problems if not disposed of properly. All of these items can be rendered harmless by one or more of five methods:

1. Shredding — Reducing items to small strips/particles.
2. Degaussing — Using powerful magnets to permanently eliminate data from magnetic media.
3. Disintegration — "Mechanical incineration" that continually cuts items into smaller and smaller pieces until they are unrecognizable and unreconstructible.

Computer parts and other metal waste end up as "e-scrap," some of which can be recycled. Powerful shredders reduce metal to strips (left) that can be run through a disintegrator and pulverized to tiny bits (right) for added security.

PHOTOS COURTESY OF SEM

After passing through a disintegrator, computer hard drives end up as tiny bits of "e-scrap."

4. Declassification — Physically grinding the data-bearing surfaces from CDs and DVDs.
5. Crushing — Destroying hard drives by subjecting them to extreme pressure from a conical steel punch or similar device.

What about cost? Ideally, the decision to purchase destruction equipment should not be based on cost, but on potential risk. For some businesses, the peace of mind that comes from knowing sensitive records will never leave their facilities intact makes the investment worthwhile. Even so, many companies simply cannot afford to purchase this equipment for the relatively few items they need to destroy. These businesses may choose to outsource such destruction.

Outsourcing can be affordable and safe when done properly. If you choose this option, be sure to do your homework to learn just how secure the destruction facility is. Here are some questions to ask:

1. How are materials transported to the destruction facility? Does the facility offer locked, trackable transport cases?
2. Does the facility require service contracts or monthly minimums?
3. Upon arrival at the facility, will your items be inventoried and stored in a locked area?
4. Are job applicants thoroughly screened? Is the facility monitored around the clock by security cameras?
5. What destruction methods will be used? The facility's equipment should make short work of computer hard drives (or even whole central processing units), CDs, DVDs, diskettes, microfilm, credit cards, ID badges, audio and video cassettes, circuit boards, PDAs (Palm Pilots and the like), cell phones, x-rays, flash media (digital camera "thumb drives," etc.), and key tape. Everything should end up as "e-scrap" — tiny, unrecognizable fragments.
6. Has the facility's equipment been approved by the U.S. National Security Agency?
7. What proof will you have that items were actually destroyed? Would you be allowed to watch the destruction in person or via IP video camera?
8. Will the destruction of your items be certified in writing?
9. What happens to destroyed waste? Is any of it recycled in accordance with pertinent regulations?
10. Is the facility bonded and insured?

If you don't like the answer to any of these questions, look for another facility.

Data security is an ongoing process, but by being aware of threats and understanding destruction options, you will be in a much better position to protect your institution and yourself.

Andrew Kelleher is president of Security Engineered Machinery (SEM), a supplier of document destruction equipment, based in Westboro, MA. He can be reached at *info@semshred.com*. This is his first article for *Facilities Manager.*

THE 9 THINGS YOU SHOULD BE DESTROYING

ITEM	THREAT	METHOD OF DESTRUCTION
1. COMPUTER HARD DISK DRIVES	Data Theft — Documents, Spreadsheets, Databases, etc.	Shredding, Crushing, Disintegration, or Degaussing
2. THUMB DRIVES/FLASH DRIVES/ MEMORY CARDS	Data Theft — Documents, Spreadsheets, Databases, etc.	Shredding or Disintegration
3. CELL PHONES/BLACKBERRIES & OTHER PDAS	Data Theft — Contact Lists, Call Logs, Images, etc.	Shredding, Crushing, or Disintegration
4. OPTICAL MEDIA — CDS/DVDS	Data Theft	Shredding, Disintegration, or Declassification
5. OTHER MAGNETIC MEDIA — FLOPPY DISKS, ZIP DISKS, COMPUTER BACKUP TAPES	Data Theft	Shredding, Disintegration, or Degaussing
6. EXPIRED INVENTORY, OFF-SPEC PRODUCTS, PROTOTYPES	Data Theft — Corporate Liability, Brand Degradation, Industrial Espionage	Disintegration
7. CREDIT CARDS/ID BADGES	I.D. Theft — Data on Magnetic Strip	Shredding (paper shredder okay for low volume) or Disintegration (high volume)
8. AUDIO, VIDEO & MICRO CASSETTES	Data Theft — Meeting Records, Sales Aids/ Training Materials	Disintegration or Degaussing
9. LASER PRINTERS & FAX MACHINES	Data Theft — Remnant Data on Drums & Internal Memory	Shredding or Disintegration