

## **INFORMATION SECURITY THROUGH PRUDENT DESTRUCTION PROCEDURES**

By Leonard Rosen - Chief Executive Officer,

Security Engineered Machinery

Information security is a challenge for every business and government agency. Not the least of many concerns in this field is the disposal of sensitive electronic or paper records that have become obsolete. A comprehensive “document security audit” can help establish routines that keep such records from falling into the wrong hands. The equipment selected to facilitate disposal will differ according to the nature and size of the facility.



An effective information security program might take a cue from new federal regulations implementing the Fair and Accurate Credit Transaction Act (FACTA). These far-ranging standards require lenders, insurers, and many other businesses — anyone who “maintains or otherwise possesses consumer information for a business purpose” — to properly destroy consumer information in order to protect against consumer fraud and identity theft.

A business might find it helpful to put one employee in charge of disposal of sensitive records. Centralization of responsibility/accountability can be a good thing when it comes to preventing unauthorized, unnecessary, and inadvertent disclosure of protected information.

Proper storage of sensitive information requires locking file cabinets, computer “firewalls,” and other measures. Proper disposal means destroying information-bearing materials to the point where no one can retrieve them later.

When records are destined for disposal, storage and disposal functions may overlap. Secure waste receptacles look like typical steel trashcans with hinged doors at the top, but they prevent the removal of material even if they are turned upside down. One design makes use of a curved chute to permit the deposit of bound reports or thick stacks of paper while preventing arms from reaching in. The hinged top is lockable, of course. Another type of receptacle looks like an attractive metal locker with a built-in file-cabinet drawer on top. Material can be dumped into (but not removed from) the “locker” below, the door of which has concealed hinges to discourage tampering. Inside, waste falls into a canvas bag with carrying handles, a rugged zipper, and a hasp for a small padlock.

Paper shredders are available in various sizes, speeds, horsepower, and capacities. Their cutting heads differ too, depending on the desired size of the shreds. Conventional strip-cut shredders produce strips that possibly could be pieced together later by unauthorized persons. Cross-cut shredders turn paper into small squares of varying sizes, depending on the model. Heavy-duty, high-volume shredders can destroy bound reports and large stacks of paper. As for capacity, there are three basic choices:

Personal: Desk-side shredders, some available on casters for portability, can shred roughly 6-20 sheets at a time. For offices with relatively few documents to destroy, the convenience of these models may obviate the need for pre-shredding storage containers. Shreds accumulate in plastic bags that can be combined with other trash.

Departmental: Larger facilities with more documents to dispose of may choose to install a more powerful shredder in every department or on every floor. These models can shred 20-50 sheets at a time. Instead of waste bags, some models have extra-large, wheeled bins inside, facilitating disposal to a central location.

Centralized: For high-volume shredding, a heavy-duty shredder can handle up to 500 sheets at a time, so these machines have no problem destroying bound reports and thick stacks of paper. Balers can be attached to some heavy-duty shredders.

Also on the market are powerful “disintegrators,” which destroy virtually any bulk material, pulverizing plastic items as well as books, binders, and bundles at the rate of up to two tons per hour. The rotary-knife mills in these machines cut items into smaller and smaller pieces until they are unrecognizable, so manufacturers of pharmaceuticals, medical devices, toys, textiles, and other goods use them to destroy “off-spec” or returned products, expired inventory, and prototypes. CDs, DVDs, computer diskettes, microfilm, x-rays, credit cards, ID badges, tape cassettes, circuit boards, cell phones, PDAs (“Palm Pilots” and the like), laptop computers, computer hard drives, and even entire CPUs (computer central processing units) — all of them end up as indecipherable fragments. These particles can be sized via interchangeable screens, through which pieces cannot fall until they are further reduced by the high-torque, two-stage cutting system. A disintegrator can be ordered with a conveyor belt, a noise-reducing enclosure, or a vacuum evacuator system that sends the particles through flexible tubing to a nearby bag, bin, dumpster, or truck.

It is important to remember that FACTA covers records stored on computers as well as paper documents. One hard drive or CD can contain thousands of files, and when a digital file is “deleted,” the information actually remains on the computer’s hard drive, CD, or diskette, 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, for example, and in some cases old computers are removed and resold by the vendor who installs replacement computers.

Machines designed specifically for optical media can completely remove data-bearing surfaces from CDs and DVDs. The inner disc hubs remain intact, furnishing proof of destruction and thus eliminating the need for detailed logs and witnesses where certification of destruction is required.

“Disk-wiping” software can prevent unauthorized recovery by overwriting entire drives/disks (or particular sections of them) before these magnetic media are discarded or reused. Overwritten areas should be unreadable, but some software packages are more thorough than others; look for a brand that meets or exceeds the Department of Defense standard for permanent erasure of digital information (U.S. DoD 5220.22).

To erase magnetic media, there are several types of degaussers, which remove all recorded information in a single pass, allowing hard drives, diskettes, audio and video tapes, and data cartridges to be reused many times with no interference from previous use. Hand-held degaussing wands erase both floppy and hard computer disks.

For businesses that only need to purge their files infrequently or for whatever reason would rather not destroy their protected materials themselves, there are shredding/destruction services that accept shipments or pick up material, destroy it on their own premises, dispose of the waste properly, and issue certificates of disposal. Many of these services offer regularly scheduled pickups, and a few even have truck-mounted machines for on-site shredding.

Although information security programs will differ according to facility size and mission, nearly every field of endeavor these days must address the disposal of protected information. A wide selection of equipment is available to help a facility establish a program that meets its particular needs.

Leonard Rosen is Chief Executive Officer of Security Engineered Machinery (SEM). In addition to its business customers, SEM supplies destruction equipment to every American embassy in the world and most U.S. military, intelligence, and law enforcement agencies. SEM also provides no-cost document-security audits to New England businesses. On request, with no obligation, a trained SEM expert will analyze document sensitivity in relation to facility size and other variables, then make recommendations regarding equipment and services.