

# InsideCounsel

## Data Destruction

From *InsideCounsel Magazine* | [December 2007 Issue](#)

By Keith Ecker

December 1, 2007

Gordon Moore, co-founder of Intel, made a prophetic observation in 1965. In what has become known as Moore's Law, he theorized that computers' storage capacity would double about every 18 months for the indefinite future. So far his theory seems to be holding true. Whereas several years ago a terabyte—1,000 gigabytes—hard drive was a thing of science fiction, it's now readily available.

As amazing as this technology is, it's created some unforeseen problems. ¶ “Software manufacturers want to use as much of this capacity as possible, so newer versions of software require newer equipment,” says Robert Johnson, executive director of the National Association for Information Destruction (NAID), a trade association for information destruction service providers. “In turn this means companies have to dispose of more and more hardware to keep up.”

In many cases the IT department handles the disposal of old hardware. And that old hardware often ends up in landfills. The problem, though, is that the hard drives in the computers aren't properly erased and still house sensitive customer and company information—all of which has the potential of creating serious legal problems for the company.

“Clearly, within any company, someone such as the general counsel should look at hardware disposal, make a statement about policy and ensure employees comply and are aware of the legal reasons for doing it that way,” says Daniel Bayha, vice president and CFO of Back Thru The Future Computer Recycling Inc., a data destruction service provider. “The old practices just don't cut it any longer.”

### Who's in Charge

It is these old practices that are getting companies into trouble. According to NAID, 60 percent to 75 percent of hard drives bought on the secondhand market still contain information. Many of these devices come from corporations that hand off old equipment to low-level IT personnel. These employees often donate the devices to schools, resell them to make extra cash for themselves or simply toss them in the garbage.

“Companies rarely charge the right person with handling hardware disposal,” says Angie Keating, vice president of compliance and security at Reclamere, a digital data destruction company. “The right person should be someone such as the CLO, the CEO or the CIO, but no one lower than those positions should be making those decisions.”

These executives should then work with the varying department heads to create a disposal plan for old equipment—whether it is a computer, a fax machine or PDA, all of which have hard drives that can contain documents or sensitive information.

“It shouldn't solely be the IT department that gets handed this responsibility,” says Bill Millican, director of IT and professional resources at ARMA International, a professional organization for records managers. “It should be a collaborative effort between IT, records management and in-house counsel.”

In some cases a company may also want to bring in outside help to dispose of used equipment. This is

especially true in cases where a company doesn't have the resources to erase old hard drives, or in businesses that handle a lot of sensitive data such as financial institutions and insurers. The most common form of outside help are companies that shred old equipment.

### **The Garbage Men**

Bayha's Back Thru The Future is one such company. His company specializes in the complete decimation of hardware. What arrives at his business as a set of intact hard drives leaves as a pile of shredded aluminum, thanks to a three-ton paper shredder on steroids.

"We take the material to the shredding machines and feed them in," he says. "After we are done shredding the drives, we capture the material; we record the date, number of drives and weight; we take a photo of the waste and put it in an affidavit; the technician signs off on it; then we send it to an aluminum smelter where they smelt it, which we get records of as well."

Complete and absolute destruction may be Bayha's business, but it's not the only service he provides. On the front end of every project, his company maintains a detailed audit trail of all incoming materials.

First, clients receive a steel container that can fit more than two dozen hard drives. The client records the manufacturer, model and serial number of every hard drive sent for destruction and then ships the container, noting its security tag to Back Thru The Future.

Next, Back Thru The Future photographs the container and its security tag and then takes inventory of the containers contents by manufacturer, make and serial number. It then e-mails all this documentation to the customer, which reviews and confirms it before Bayha's company destroys the hardware. Bayha's customers include companies that operate in highly regulated industries, such as financial services.

"With any highly secure procedure you have to be redundant, so that if one method fails, the other one will accomplish what you need it to," Bayha says.

Because Back Thru The Future makes most of its money off of selling the aluminum scrap, the service is cheap. Fees never go above \$10 per device, and the company reduces this price when destroying in bulk. Back Thru The Future also will destroy old tapes and CD-ROMs for \$.50 a pound.

### **Due Diligence**

Back Thru The Future is only one of many companies that offer hardware destruction services. However, not all vendors are created equal. Johnson recommends that in-house counsel shop around and ask the right questions before contracting a vendor.

"The most important decision of disposing of IT equipment is really the qualifications of the company that you hire to do it," he says. "Anyone in that business is going to say they can get rid of electronically stored information, but you have to do more than just believe what the vendor is telling you."

Johnson recommends investigating the process the company uses to destroy hardware. The vendor should keep detailed audit trails that clients can use to ensure destruction is thorough and conduct criminal background checks on all employees to ensure hardware won't get stolen.

In addition someone from the company should visit the vendor to witness the destruction process.

"Someone from the company should definitely visit the vendor the first couple times hardware is sent for destruction to find out for certain where the devices go and how the audit process works," Millican says.

"Even after this, someone should make periodic, unannounced visits to witness what's going on."

(c) 2007 *InsideCounsel*. A [Highline Media](#) publication. All rights reserved.