

Friday, June 18, 2010

Smart Strategies

It's getting personal

e-End partners with Advance Business Systems to destroy hard drive data

Printers, copiers, fax machines are the next frontier in fighting ID theft

by Rachel Bernstein, Staff

Just shredding paper bills and confidential documents for your business doesn't cut it anymore.

Throwing away old copiers and fax machines — or even selling them — can be a hazard to your business, your identity and the identities of customers or clients.

With technology becoming more advanced for copiers and fax machines, these pieces of equipment are basically mini-computers, storing such information as Social Security numbers, credit card information, addresses and clients' personal information. Combine that with the movement to get more patient information online, and scam artists' new techniques for mining cyberspace for personal information, and few businesses or consumers are entirely safeguarded from some form of identity theft.

But businesses that use these machines — printers, copiers, fax machines and others — can protect themselves and their customers from such damage by making sure that data is completely erased after the end of the machine's life. After all, the success of the business could depend on it.

Elliot M. Wagonheim, managing partner of [Wagonheim and Associates](#) in Hunt Valley, has heard of too many companies lose data because of unscrubbed hard drives. "I'm certain there are a number of institutions that run afoul without even knowing it, just because of their copiers," Wagonheim said.

Wagonheim's six-attorney firm works with clients to make sure hard drives are erased or shredded when drafting contracts with vendors. Many businesses often rent copiers and fax machines from a vendor, who may not necessarily know how to properly remove hardware or reformat a hard drive.

That's where Advance, the Cockeysville office equipment dealer formerly [Advance Business Systems](#), is trying to help. The company recently began offering the option of erasing hard drives for its customers. The service can cost up to \$300 for the full destruction and shredding of hard drives.

Advance erased data and shredded hard drives from about 150 used copiers last month in its first major effort to increase awareness about the problem for businesses.

The company offers three different types of hard drive erasing or destruction to protect information. What kind of protection you need depends on what you use your equipment for, and the type of company. Protection can be as simple as erasing information on a hard drive to the complete magnetic erasure of data and physically shredding the drive.

“If you own a candy store, it’s different for copying bills for Tootsie Rolls as opposed to patient records,” said Jeff Elkin, chief operating officer of Advance.

Wagonheim’s firm works with the vendor for the copy machine to maintain and reformat the machine’s hard drive. For its fax machine, which the firm owns, an IT consultant removes the data at the end of the machine’s life before sending the fax machine to an electronics recycler. At [Johns Hopkins University](#) and [Johns Hopkins Hospital](#), numerous hard drives from different machines have been lost or stolen over the years. In 2009, federal authorities investigated the theft of patient information, possibly by a former Johns Hopkins Hospital employee, as part of a scheme to make fraudulent Virginia driver’s licenses.

The employee, who worked in the patient registration area, would have had access to information such as patients’ names and Social Security numbers as part of her job duties, according to a letter the hospital sent to the identity theft unit of the state attorney general’s office.

Johns Hopkins sent a warning letter to 46 victims, 526 possible victims who were to receive credit monitoring at the hospital’s expense and 10,200 patients whose information was accessed by the unnamed employee of the hospital’s patient-services department.

“That’s caused a lot of heartburn,” said Darren Lacey, Johns Hopkins University’s chief information security officers.

The Baltimore university works with several vendors for its copiers, computers, fax machines and other equipment, but has learned its lesson that end-of-life storage of any kind of digital media needs to be dealt with in a cautious way.

Copiers and fax machines that store your medical records or fax your birth certificates, driver’s license information and other personal documents are just as prime for stealing information.

They get sold or traded in.

Advance, which works with many government agencies and companies that need full protection with confidential information, anticipates its hard drive shredding business to increase as more companies become aware of the information kept on all kinds of hard drives.

“It’s the whole consciousness of what you’re doing with your confidential information,” Elkin said.



Photo by Christopher Myers, Contributor

Jeff Elkins’ Advance recently began offering to erase hard drives for its office equipment clients. Shown in bin are hard drives that had their data sanitized then shredded by e-End.

e-End provided secure data sanitization and destruction of all electronic media. www.eendusa.com