

Skeletons on your hard drive

By Matt Hines

URL: http://news.zdnet.com/2100-1009_22-5676995.html

Tax records, resumes, photo albums--the modern hard drive can keep increasingly larger volumes of information at the ready. But that can turn into a problem when it comes to effectively erasing the devices.

There are a number of options for cleansing the drives of unwanted computers, from special wiping software to destruction services to [manufacturers' recycling programs](#). But what many PC owners don't realize, experts say, is that these methods are often not enough.

"For people who want to sell or donate a computer, who are trying to protect their checkbook or medical info, you can expect to protect yourself against all but the most sophisticated attacks with wiping," said Stephen Lawton, the director of marketing at Acronis, a maker of wiping tools, backup and recovery software. "But you have to use the software the right way."

News.context

What's new:

It can be tougher to clean data off a discarded hard drive than many people realize, experts say.

Bottom line:

Sensitive data could be left on donated or sold PCs. The only way to erase drives is to use wiping software plus material destruction.

[More stories on hardware security](#)

"Even the people who destroy disks will tell you (that) unless you do that correctly, there are always people who can get the data off," he added.

That means that passwords, logins and other personal information could still be lurking on machines that have supposedly been cleaned--a risk that strikes a chord amid reports of [laptop thefts exposing sensitive information](#) on thousands of Americans.

Two weeks ago, the National Association for Information Destruction announced that it could not endorse the use of wiping applications alone for deleting data from hard drives. Bob Johnson, executive director at [NAID](#), said the data-destruction industry group would like to be able to recommend the tools, but that tests had left reason to doubt the wiping products.

"Our position, ultimately, was that we will only give our approval to physical destruction of the hard drive," Johnson said. "We know that unless that is done a certain way, even that can be an ineffective approach."

Johnson also distrusts the ability of companies offering mass computer wiping services to have sufficient methods of testing to see if data exists on the drives even after their processes have been run.

Remains of the data

There are signs that people are not aware of the risk from discarded drives. Last year, German encryption technology specialist Pointsec tested hard drives bought on eBay to see if they still carried data and discovered that seven out of every 10 devices it tested still bore readable information.

That study followed similar research published in 2003 by graduate students Simson Garfinkel and Abhi Shelat, who found that only 12 of the 129 working [computer hard drives](#) they bought in secondhand stores and on auction site eBay had been adequately cleansed of sensitive data from their previous owners.

"You have all kinds of data being stored in the hard drive, in the Web browser and in application files, and these are all affected by the same problem--you delete something on the computer, but it doesn't really ever get deleted completely," said Garfinkel, a doctoral candidate at the Massachusetts Institute of Technology.

"You have to distinguish between deleting occasional files and truly wiping a machine clean," he added. "There's really a significant difference."

The first step for many people would be a low-level reformatting of the operating system on their PC, even though doing that with Microsoft's Windows or Apple Computer's Mac OS operating systems won't destroy data completely, experts said.

"What we've seen with a lot of clients is that they think that reformatting a drive gets rid of the data, and that's just not true," said Kathy Ferguson, a business unit manager with IBM's Asset Recovery Solutions Group. "In a typical scenario, that only overwrites partitions, or sectors of data. At the end of the day, you can recover that data readily if you have the right tools."

Wiping software is the obvious next choice. Everyone from security giants such as Symantec to freeware vendors such as [MXC Software](#) offers applications meant to help people hide the data they once wanted stored on their computers. Most of these technologies revolve around software meant to overwrite the information on the devices with a random series of numerals, in particular the numbers 0 and 1.

The difference between people who use wiping software correctly to erase their hard drives and those who do not is most often a matter of attentiveness, [Acronis'](#) Lawton said. By using multiple overwrites featuring different character sets, he said, consumers can approach the same level of protection required by the U.S. Department of Defense. The department requires a minimum of at least four passes with wiping tools, in cases where it does not mandate that a drive is destroyed.

Data-cleaning tips

The only way to completely erase data from a hard drive is to use wiping software and then destroy the drive, experts say. Here are examples of available resources.

Wiping software

McAfee QuickClean 2.0 Promises to clear up disk space and remove unwanted data. Costs \$9.95.

Acronis Drive Cleanser 6.0 Acronis' purpose-built disk-cleaning software, sold for \$49.99.

Clean Machine Plus 2.0 Made by HFK Creative Enterprises, offers Internet security and wiping tools for \$49.95.

Smash 2.0 Includes encryption and decryption utilities plus wiping tools. \$24.95.

iSafeguard Freeware 5.0 A version of MXC Software's e-mail encryption and wiping applications, available for free download.

Recycling programs

Apple Computer For a \$30 fee, Apple will take back your computers and destroy them.

Dell For \$10, Dell will take delivery of old machines for destruction.

Hewlett-Packard For \$13 to \$34, depending on the equipment, HP will ship and trash your old gear.

IBM For \$30, IBM will take your old PCs back and recycle them.

Seagate Technology Provides information on its hard-drive recycling programs.

Lawton believes that taking such a meticulous approach with the software, which could take as long as several hours, often takes more time than most consumers are willing to wait.

"For a consumer who is going to be getting rid of a disk, giving it away or passing it along, if you overwrite seven times, chances are that you're doing pretty well. While a company might look at running a wiping application 35 times," Lawton said. "On the other hand, a fast wipe is pretty insufficient."

The need to keep at it means those people who go to the trouble of employing outside technology to erase their sensitive data could still be doing too little. In general, experts agreed, the best approach in trying to completely erase information is to use a combination of data removal software and material destruction.

"If you've got truly classified info, then you're going to crush or degauss the drive somehow," Lawton said. [Degaussing](#) is a form of magnetic storage device cleansing used primarily on large groups of machines by businesses.

All of the major PC makers and most hard-drive makers offer recycling programs where, for a fee of between \$20 and \$30, they will professionally destroy used devices. Though these programs have traditionally attracted primarily business customers, executives running the programs at Dell and IBM said consumers are increasingly taking advantage of them.

"PCs and hard drives are ripe with information that is sensitive or confidential, so we go to great lengths to make sure everything is destroyed as part of our asset recovery programs," said IBM's Ferguson.

Garfinkel, whose thesis focuses on computer security, chiefly blames companies making [operating system software](#) for failing to build in adequate tools to help clear data from every corner of their products' memories.

But some hardware makers said they can understand why software vendors don't make it easy for customers to delete every trace of their information.

John Frey, an environmental strategies and solutions manager at PC giant Hewlett-Packard, pointed out that when drives were easily wiped during the DOS era, people saw it as a liability rather than a benefit. Frey said hardware and software makers have made data hard to eradicate because customers have demanded that they do so.

"You have to consider: What is the benefit to ease of use versus what is the chance that users will do it by mistake?" Frey said. "We've taken the approach that we value our customers' privacy so much, why give anyone reason to doubt? If the disk drive gets to us, we shred it."

The IT market continues to hunger for everything from operating system software that somehow allows end users to completely delete their information, to more powerful wiping tools that do a better job in less time than the current products on the market. In the meantime, consumers will be forced to consider their best alternatives when faced with the decision to save, sell or recycle old hardware.

For Charles Smith, the founder of EDR Solutions, the problem isn't going away anytime soon. The company has developed the Hard Drive Crusher, a refrigerator-size contraption that punches holes in disk drives to make them harder to read. Though the Hard Drive Crusher isn't designed for sale to consumers, Smith believes people may want to take such drastic measures into consideration before parting with their old hardware.

"With the technology that's out there, who knows what people will be able to do in the future? I can punch a hole in the drive for now, but someday someone could still be able to read it," he said. "I think people want proof that the device won't be coming back online with the same data on it, and this is the best I can do."