

Security Concerns With Used Equipment

By Dan Heilman

8 April 2011

Processor

Be Smart About What & Where You Buy To Prevent Security Breaches

When it comes to used or refurbished equipment, much attention is given to the quality of the pre-owned equipment and how much it will cost to maintain it, and rightly so. However, there is another factor that deserves just as much—or more—attention: security. Here is a look at how both buyers and sellers of used and refurbished equipment can sidestep security problems.

Start with a clean slate. No matter what it is you're selling, from PCs to server hardware to even printers, chances are there's private company data on it that has to be gotten rid of. Experts advise being extra careful and thorough in doing so.

The two main methods of "wiping" machines are via software packages or physical destruction/degaussing. There are free programs that promise to erase data from hard drives, but using freeware for something this important can be risky, according to Jeff Pederson, manager of data recovery operations at Kroll Ontrack (www.krollontrack.com).

"The more in-depth software you can buy produces a report that details exactly what it's done and provides a serial number of what media was removed for accounting and compliance purposes or for destruction or reuse," Pederson says.

Degaussing removes the magnetic fields from the media itself and is probably the most reliable way of ensuring that the data that once resided there can never be used again. "The hard drive becomes physically inaccessible—it doesn't work anymore," Pederson says. "All the zeroes and ones are removed from the media. You can also physically shred the latters themselves."

Even printers and multifunction peripherals can be risky to sell, according to Pederson—most newer models come with their own operating systems and hard drives that, unbeknownst to most owners, contain the data from every document printed on that machine.

Consider compliance. Risks exist for buyers of used equipment, as well. In many regulated industries, if a used piece of equipment has data on it, compliance rules might dictate that the data must be disclosed. "If you just overwrite the data without checking first if that's OK, it could be a problem," Pederson says.

Beware of unwelcome surprises. A greater risk is the remote but realistic chance that the equipment you're buying is a Trojan horse of sorts, equipped to provide outside parties with your sensitive data.

"A great number of the computer and laptop tracking software that is currently on the market will not get destroyed in a format and OS reinstall," says Lenny Fuchs, principal of consultancy firm My IT Department. "Most allow root-level access to the computer."

Fuchs says keyloggers or other software can be used to track the location of the owner and even perform nefarious acts such as deleting the contents of the hard drive.

"On the purchasing side, there is a risk that used media contains malware," adds Joe Fisher, president of Affinity IT Training. "It would be wise to scan refurbished drives using the latest antivirus software, especially if [the drives] are used to boot the machine."

"You never really know how a piece of IT equipment has been used—or abused," Fuchs says.