

Sensitive data not being erased: survey

By: Mark Cox

22 November 2010

EChannelLine USA

<http://www.echannelline.com/usa/story.cfm?item=26362>

Half the companies out there don't erase data from old devices at all. And of the ones that do, three quarters don't do so securely.

That's the results of a recent global survey on data wiping practices done for Kroll Ontrack. It found that less than half of businesses regularly deploy a method of erasing sensitive data from old computers and hard drives. Of the 49 percent of businesses that are systematically deploying a data eraser method, 75 percent do not delete data securely, leaving most organizations highly susceptible to data breaches.

"Three-fourths of businesses are deleting files, reformatting or destroying drives, or 'do not know' how they are erasing sensitive data," said Jim Reinert, vice president of product development, Kroll Ontrack. Deleting files from a hard drive only marks the files to be rewritten, which may never occur. Furthermore, reformatting the drive only removes the entries in the index or table of contents that point to the data. And, physically destroying a drive is not a guaranteed method of protection, as Kroll Ontrack has been recovering data from severely damaged drives, such as the Columbia space shuttle, for more than 25 years.

Surveying more than 1,500 participants from 12 countries across North America, Europe and Asia Pacific regarding their data wiping practices also revealed that four in 10 businesses gave away their used hard drive to another individual and 22 percent did not know what happened to their old computer. In total, more than 60 percent of all old business computers are fully intact with proprietary business data in the second hand market.

"In addition to helping companies achieve compliance with laws and regulations regarding data retention and privacy, data wiping is fundamental to reducing the risk of security breaches," Reinert said. "It is a must -- regardless of the size of the organization -- and needs to be incorporated into overall data security and business continuity plans."

Only 19 percent of businesses deploy data eraser software and fewer, 6 percent, use a degausser to erase media. When asked if and how businesses verify their data has been deleted, very few (16 percent) reported relying on a product or service report to confirm all of their data had been wiped. Aside from businesses that "do not know" (34 percent) how they ensure their data has been erased from an old device, the next most popular response, reported by 22 percent of businesses, was "reboot the drive" to see if the data is still there.

"Reports that verify or confirm what the tool and/or service did are critical," Reinert said. "Not only do they inform you of what has been wiped, but they should identify the serial number as well as the make and model information of the wiped hard drive, the date and time of when the information was wiped, and a listing of how much information was wiped."