

## **Most Companies Don't Erase Sensitive Data, Risking Breaches**

By Melissa Klein-Aguilar

16 November 2010

*Compliance Week*

Most businesses don't properly erase sensitive data from old computers and hard drives, leaving them highly susceptible to data breaches, according to a survey by Kroll Ontrack.

Only 49 percent of more than 1,500 respondents polled worldwide say their businesses are systematically deploying a data eraser method. Among that group, 75 percent don't delete data securely, according to Kroll.

Maybe they didn't hear about the digital copier incident that resulted in one company notifying more than 400,000 people that their personal or medical data may have been compromised. As Compliance Week previously reported, in April, Affinity Health Plan had to send a breach notice to more than 400,000 of its costumers after CBS News, as part of an investigation, purchased a digital copier previously owned by Affinity from a wholesale warehouse and discovered that the copier's memory contained individual medical records and non-medical documents including driver's licenses and Social Security cards.

In a May letter in response to a request from Rep. Ed Markey, the Federal Trade Commission said it would reach out to copier manufacturers and others to determine whether they're addressing such privacy risks and also provide further guidance for consumers and businesses about protecting personal information that may be storied on hard drives.

According to the Kroll survey, three-quarters of businesses are deleting files, reformatting or destroying drives, or don't know how they are erasing sensitive data. None of those methods ensure that sensitive information isn't longer on the drive, says Jim Reinert, Kroll vice president of product development. Deleting files from a hard drive only marks the files to be rewritten; reformatting only removes the entries in the index or table of contents that point to the data, and physically destroying a drive doesn't guarantee protection, since data can be recovered from severely damaged drives.

So, what's the risk? A separate Kroll study issued earlier this year found that U.S. businesses suffer an average of at least one data breach a year. Moreover, the latest study by the Ponemon Institute estimates that data breaches cost U.S. companies an average of \$6.75 million.

In addition to helping companies comply with data privacy and retention laws and regulations, Reinert says data wiping is fundamental to reducing the risk of security breaches.

"It is a must - regardless of the size of the organization - and needs to be incorporated into overall data security and business continuity plans," he says.

Certified data wiping software that overwrites all the data on the hard drive or a degausser, which wipes the data using a strong magnetic force rendering the device no longer usable, are the two safest methods to ensure private data is wiped, according to Reinert.

Only 19 percent of those responding say their company deploys data eraser software and just 6 percent use a degausser to erase media. Roughly a third of businesses "do not know" how they ensure their data has been erased from an old device, while 22 percent say they "reboot the drive" to see if the data is still there.

In total, Kroll notes that more than 60 percent of all old business computers are fully intact with proprietary business data in the second hand market. Forty percent of those polled say their companies gave away their used hard drive to another individual, and 22 percent don't know what happened to their old computer.

When asked if and how businesses verify their data has been deleted, 16 percent reported relying on a product or service report to confirm all of their data had been wiped. Reinert says reports that verify or confirm what the tool and/or service did are critical. Such reports should identify what's been wiped and the date and time, the serial number, make and model information of the wiped hard drive, and the amount of information wiped.