

Digital Photocopiers Loaded With Secrets - CBS Evening News

(CBS) At a warehouse in New Jersey, 6,000 used copy machines sit ready to be sold. **CBS News chief investigative correspondent Armen Keteyian** reports almost every one of them holds a secret.

Nearly every digital copier built since 2002 contains a hard drive - like the one on your personal computer - storing an image of every document copied, scanned, or emailed by the machine.

In the process, it's turned an office staple into a digital time-bomb packed with highly-personal or sensitive data.

If you're in the identity theft business it seems this would be a pot of gold.

"The type of information we see on these machines with the social security numbers, birth certificates, bank records, income tax forms," John Juntunen said, "that information would be very valuable."

Buffalo Reacts to CBS News Investigation

Juntunen's Sacramento-based company Digital Copier Security developed software called "INFOSWEEP" that can scrub all the data on hard drives. He's been trying to warn people about the potential risk - with no luck.

"Nobody wants to step up and say, 'we see the problem, and we need to solve it,'" Juntunen said.

This past February, CBS News went with Juntunen to a warehouse in New Jersey, one of 25 across the country, to see how hard it would be to buy a used copier loaded with documents. It turns out ... it's pretty easy.

Juntunen picked four machines based on price and the number of pages printed. In less than two hours his selections were packed and loaded onto a truck. The cost? About \$300 each.

Until we unpacked and plugged them in, we had no idea where the copiers came from or what we'd find.

We didn't even have to wait for the first one to warm up. One of the copiers had documents still on the copier glass, from the Buffalo, N.Y., Police Sex Crimes Division.

It took Juntunen just 30 minutes to pull the hard drives out of the copiers. Then, using a forensic software program available for free on the Internet, he ran a scan - downloading tens of thousands of documents in less than 12 hours.

The results were stunning: from the sex crimes unit there were detailed domestic violence complaints and a list of wanted sex offenders. On a second machine from the Buffalo Police Narcotics Unit we found a list of targets in a major drug raid.

The third machine, from a New York construction company, spit out design plans for a building near Ground Zero in Manhattan; 95 pages of pay stubs with names, addresses and social security numbers; and \$40,000 in copied checks.

But it wasn't until hitting "print" on the fourth machine - from Affinity Health Plan, a New York insurance company, that we obtained the most disturbing documents: 300 pages of individual medical records. They included everything from drug prescriptions, to blood test results, to a cancer diagnosis. A potentially serious breach of federal privacy law.

"You're talking about potentially ruining someone's life," said Ira Winkler. "Where they could suffer serious social repercussions."

Winkler is a former analyst for the National Security Agency and a leading expert on digital security.

"You have to take some basic responsibility and know that these copiers are actually computers that need to be cleaned up," Winkler said.

The Buffalo Police Department and the New York construction company declined comment on our story. As for Affinity Health Plan, they issued a statement that said, in part, "we are taking the necessary steps to ensure that none of our customers' personal information remains on other previously leased copiers, and that no personal information will be released inadvertently in the future."

Ed McLaughlin is President of Sharp Imaging, the digital copier company.

"Has the industry failed, in your mind, to inform the general public of the potential risks involved with a copier?" Keteyian asked.

"Yes, in general, the industry has failed," McLaughlin said.

In 2008, Sharp commissioned a survey on copier security that found 60 percent of Americans "don't know" that copiers store images on a hard drive. Sharp tried to warn consumers about the simple act of copying.

"It's falling on deaf ears," McLaughlin said. "Or people don't feel it's important, or 'we'll take care of it later.'"

All the major manufacturers told us they offer security or encryption packages on their products. One product from Sharp automatically erases an image from the hard drive. It costs \$500.

But evidence keeps piling up in warehouses that many businesses are unwilling to pay for such protection, and that the average American is completely unaware of the dangers posed by digital copiers.

The day we visited the New Jersey warehouse, two shipping containers packed with used copiers were headed overseas - loaded with secrets on their way to unknown buyers in Argentina and Singapore.

©MMX, CBS Interactive Inc.. All Rights Reserved.

Follow us on Twitter »

— <http://lab.arc90.com/experiments/readability>