

Digital Copier Security, Inc.

INFOShare

Identity Theft: Are Your Tax Records Safe?

Did You Know?

- Digital copiers used to scan, fax, print or copy your tax returns may retain your personal information even after the machine is removed from your tax accountant's office?
- Used copiers are routinely re-marketed to both foreign and domestic buyers without steps being taken to purge sensitive data?

No single set of documents contain more sensitive data than do our individual tax returns. Names, addresses, social security numbers, employer and earnings information reside there along with information about how and where we invest and to whom we make charitable donations. Taken in their entirety, our tax returns offer a detailed picture of our personal and financial life. That's why many of us entrust that information only to a professional.

A CPA is, after all, bound by law and ethics to maintain the confidentiality of their clients. They carefully safeguard their paper and computer files, but how many accounting professionals are even aware that their

client's information may also exist on their copier's hard drive? Ask your accountant if he or she takes steps to periodically purge information from the unsecured drive on their copier. We would be pleasantly surprised to find even one who does!

Because of the proliferation of electronic filing, the copier (or multi-function peripheral) is a key component in most accounting operations. They are used to scan, print, fax and copy tax records, often creating a recoverable copy of the entire document within the machine.

At DCSI, we have tested hard drives from copiers previously used by accounting firms. In doing so, we



have found thousands of individual tax return documents. These hard drives were taken from machines that were headed for the resale market!

For more information, visit us at www.copiersecurity.com or call us at 530-672-9300, ext. 101.

Inside this issue:

ITRC Issues 2008 Breach List	2
Private Information Shipped Overseas?	2
What's New?	2
Biotech Records Saved From Dumpster	3
IRS Offers Identity Theft Resources	3
Ask Your Tax Professional	4

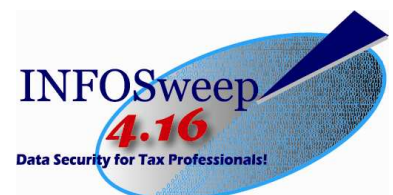
Digital Copier Security Inc. has launched a version of its INFOSweep process designed specifically for tax professionals. "INFOSweep 4.16," named for the day following the tax filing deadline of April 15, is intended to provide tax preparers with the ability to protect their client's data while maintaining the full functionality of their multi-function peripheral, or copier.

DCSI Launches INFOSweep 4.16!

"Tax Accountants need to understand the potential liability of allowing their client's personal information to reside on their copier's unsecured hard drive" says Bill Feigles, DCSI's Chief Executive Officer. "Unfortunately, most tax professionals are not aware of this threat. We've tested used machines that came from accounting firms and found

thousands of pages of personal tax documents just sitting on the hard drive", he adds.

For more information, please visit the DCSI web site at www.copiersecurity.com.



ITRC Issues 2008 Breach List: Reports of Data Breaches Up 47% from 2007

The Identity Theft Resource Center (ITRC) has issued its 2008 Data Breach List. The ITRC has been tracking security breaches for the past three years and reports a dramatic increase in 2008 over the previous year.

The report, published on the ITRC web site, identifies 656 data security breaches in 2008 compared to 446 reported incidents in 2007, an increase of 47%.

According to ITRC statistics, only

2.4% of breaches involved data that was protected by encryption or some other form of substantial data protection. Only 8.5% of breaches involved data that was password protected.

“Of course, the vast majority of data that is compromised is data that is unprotected” says John Juntunen, DCSI’s Founder and Chief Operating Officer. “That’s exactly why the threat of data breaches in digital copiers is so great. Not only is the data largely

unprotected, but at the end of its useful life, a copier is typically removed from the control of its user and sent into the resale market with sensitive data still intact” he adds.

According to the report, over 82% of data security breaches were from electronic sources and about 18% from paper records.

For more information, and to see the complete Data Breach List, visit www.copiersecurity.com and



follow the link to the Identity Theft Resource Center.

Is More Private Information Being Shipped Overseas?

As economic conditions worsen, copier resellers are finding it more difficult to sell their used machines on the domestic market. Warehouses across the country are filled with used digital copiers awaiting buyers. However, only the very best machines are finding homes as domestic businesses face budgetary constraints. “It’s safe to assume that wholesalers of used machines are facing a slow-

down” says Bill Feigles, DCSI’s Chief Executive Officer. “Unfortunately, there has not been



A typical warehouse filled with used copiers.

a commensurate slow down in the flow of machines into their warehouses” he adds.

The difficult economy means that a lot of companies are downsizing, consolidating locations or going completely out of business. All of

these actions cause more used office equipment to flood the market. Included in that flood are digital copiers filled with business and personal data.

One of the ways that wholesalers liquidate excess inventory is to sell machines to foreign markets. These machines can be stripped and sold for their component value where labor is cheap enough to



make that activity profitable. “The problem is that we don’t

really know what happens to the storage devices inside these machines once they are shipped overseas” says Feigles. “What we do know for certain is that many of these machines contain vast amounts of really sensitive information.”

“The difficult economy means that a lot of companies are downsizing, consolidating locations or going completely out of business. All of these actions cause more used office equipment to flood the market.”

“I don’t care how much power, brilliance or energy you have, if you don’t harness it and focus it on a specific target and hold it there you’re never going to accomplish as much as your ability warrants.”

— Zig Ziglar

What’s New?

DCSI Issues New Publication

Digital Copier Security has issued the most comprehensive and up to date publication available dealing specifically with the issue of digital

copier data security. To obtain your copy for just \$19.95 (plus tax), call 530-672-9300, ext 101 or go to www.copiersecurity.com.



Sensitive Biotechnology Records Rescued from Dumpster

At DCSI, we spend a lot of time performing research on digital copiers. Our analysts and technicians continually probe machines looking for stored information and documenting the vulnerability of various copier makes and models. We apply our proprietary forensic techniques and, when necessary, develop new procedures in order to recover stored data. At our test

relationships with copier dealers and wholesalers who allow us to test the used machines that they acquire on trade-in. Sometimes our search for test units takes us down some interesting paths.

Recently, our COO and Founder, John Juntunen, was visiting a dealer's warehouse looking for likely test candidates. During his search, John spotted an external print control unit that had previously been attached to one of the used copiers in the dealer's warehouse. These external units provide enhanced document management and print capabilities and are common on high-end copiers. They often take the form of a small box sitting adjacent to, or mounted on the back of, a copier. What many people don't realize is that these units also contain computer hard drives.

The metal box that John spotted was approximately fifteen inches wide, fifteen inches long, and two inches high. It had been removed from a used copier and was sitting on a shelf gathering dust. When John inquired as to the disposition of the unit, he was told that it was being discarded. When he asked about taking the unit for testing, he was told to keep it since it was just being sent to the dumpster.

DCSI has had considerable experience with these devices, so it was no surprise when our technicians announced that the internal drive was filled with data. The output from our forensic process yielded thousands of pages of documents and images.

The machine had previously been in service at a biotechnology firm and, as is the case with most machines we investigate, it was filled with a combination of business and personal documents. Included among the business documents were handwritten clinical notes, scientific test results, correspondence and other sensitive corporate data. The personal information included hundreds of photos, a passport,



A Mountain of Electronic Waste

"We have had considerable experience with these devices, so it was no surprise when our technicians announced that the internal drive was filled with data."



John Juntunen extracts the hard drive from a digital copier

center, our team disassembles and reassembles units, from a variety of manufactures.

Our passion for research means that we must have access to a variety of copier makes and models. We have developed

variety of business sectors" said Juntunen. "We are very concerned about what we're seeing from both the financial services and medical care sectors" he added.

DCSI has informed the biotechnical company of the security breach and is awaiting a response.

For more information visit www.copiersecurity.com.



A typical print controller attached to the back of a digital copier.

personal correspondence, and even images from a personal webcam.

"This case is very typical of what we find as we test copiers from a

Digital Copier Myth #2: Even if a copier has a hard drive, it's small and can't store much data.

Fact: Most copier hard drives range in size from 20GB to nearly 200GB and are capable of storing tens of thousands of pages of data. Some copiers even contain multiple hard drives.

IRS Offers Identity Theft Resources

The IRS has a department, the IRS Identity Protection Specialized Unit, which deals specifically with identity theft issues. The unit is available if

you have been in contact with the IRS about identity theft issues that have not yet been resolved. You can contact the unit by calling the Identity Theft Hotline

at 800-908-4490 Monday through Friday from 8:00 am to 8:00 pm local time (Alaska and Hawaii follow Pacific Standard Time).

4191 Business Drive, Suite F
Shingle Springs, CA 95682

Phone: 530-672-9300
Fax: 530-677-0925
E-mail: billf@copiersecurity.com



*The Cutting Edge of Digital
Copier Data Security*

**Visit Our Web Site at
www.copiersecurity.com**

**Special Tax
Time Issue!**

Ask Your Tax Professional: Is My Identity Protected?

Dear Reader,

Identity theft is a complex issue. The criminals behind this growing crime prey on their victims in so many ways that there is no single solution to the problem. One thing is certain, anytime you compile your highly confidential personal information into one place, it needs to be safeguarded.

Tax returns provide a wealth of personal and financial data and care must be taken to ensure that the information does not fall into the wrong hands. The IRS, and most tax professionals, are sensitive to securing their computers and computer networks. However,

most of those same tax professionals are doing nothing to protect your data stored on the hard drive inside of their digital copiers. If you don't believe us, just ask your accountant. If he or she isn't taking appropriate precautions, have them call us for a free security screening.

If you are intrigued, or maybe even a little concerned about this issue, spend a few minutes browsing through INFOShare. If you would like more information, please visit our web site at www.copiersecurity.com or call me directly at 530-672-9300, ext. 101.

If you would like to be removed from our

mailing list, simply drop us an email at newsletter@copiersecurity.com. If, however, you would like to stay informed about this emerging security threat, we will send you future issues of INFOShare at no cost to you.

Thank you!

Bill Feigles
Chief Executive Officer

