Written by Marco Attard
17 February 2011

Since 2002 nearly every digital copier has a HDD-- one potentially full of highly-personal or sensitive data.

As a copier scans documents, it stores a copy of that image in its memory. US company Digital Copier Security Inc. (DCSI) warns such copies remain in the HDD-- and easily retrievable if a hacker cracks the copier's encryption. Some machines even allow users to simply reprint anything on the printed job list.

Many copiers also contain sensitive IT data-- email addresses, outgoing fax numbers, contact names, IP addresses and even secure logon passwords. Their HDDs also lack firewalls or filtering.

A lot of copiers leave businesses and end up shipped overseas, with all such sensitive data intact. Copiers can easily become a major sourc eof illegally obtained non-public information.

DCSI suggests a process involving not only purging a unit's HDD of data, but also destroyiing it, in order to install a new, formatted HDD. Its INFOSweep process also includes deleting all data stored in areas other than the HDD, which may include all forms of sensitive company network data.

Since even manufacturers' warnings falling on deaf ears, it's best administrators start taking their own precautions on a potentially dangerous security breach.

Go Digital Copier Security Inc.