POWERED BY meap

CANON GENUINE TONER, DRUM & CARTRIDGE

SGS

you can
Canon

Canon (UK) Ltd
Woodhatch, Reigate
Surrey RH2 8BF
Telephone No: 08000 353535
Facsimile No: 01737 220022
www.canon.co.uk

Canon Ireland
Arena Road, Sandyford Industrial Estate
Dublin 18, Ireland
Telephone No: 01-2052400
Facsimile No: 01-2958141
www.canon.ie

WWF
Canon Europa NV
Conservation Partner

© Canon UK Edition, January 2007
Part No: 0066W148

you can
Canon

Simple defence for your business

SECURITY

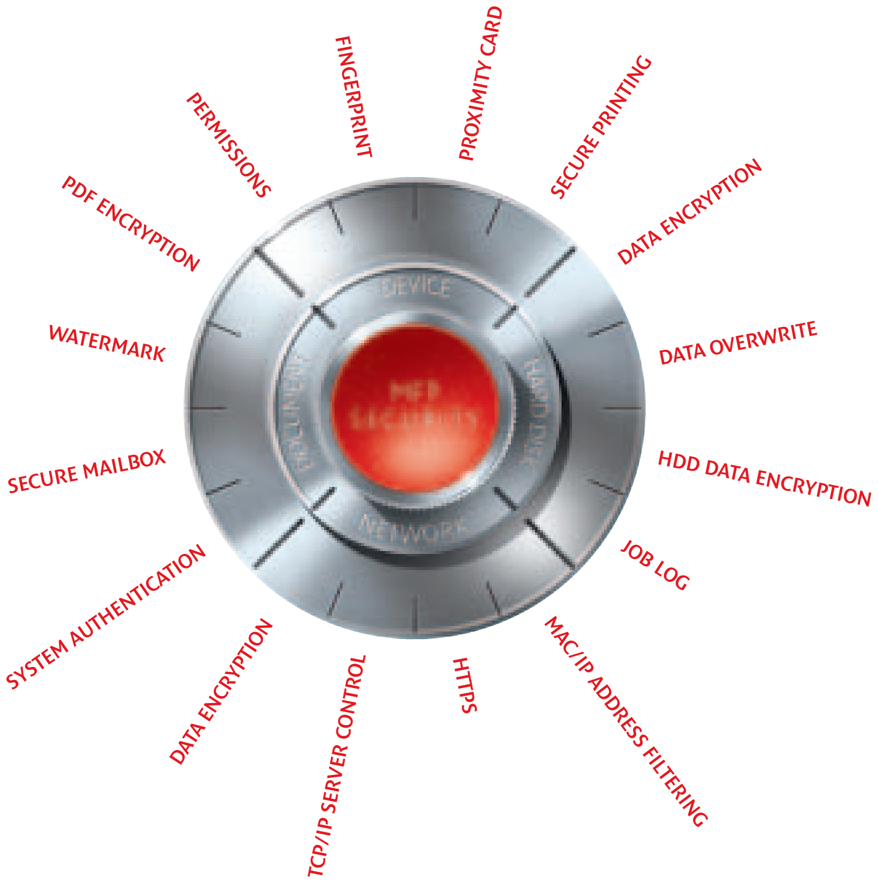
53% of office employees have found confidential documents on the printer.*

Your current printing environment

These days, most businesses protect their technology by investing in a robust firewall, up-to-date anti-virus protection, software updates and more. However, they fail to extend that protection to their multifunctional printers (MFPs).

But just like a PC or server, MFPs operate across a network, can connect with the Internet, and keep data stored on hard drives.

So what are the risks? It could be someone unauthorised trying to view the information stored within your MFP hard drive, or a hacker gaining access via the network. Or, it might be as simple as leaving confidential documents uncollected, for all to see.



* IDC Survey, 2005.

Canon – simple, secure printing solutions for your business

Canon has created security solutions to protect your printing environment in two areas:

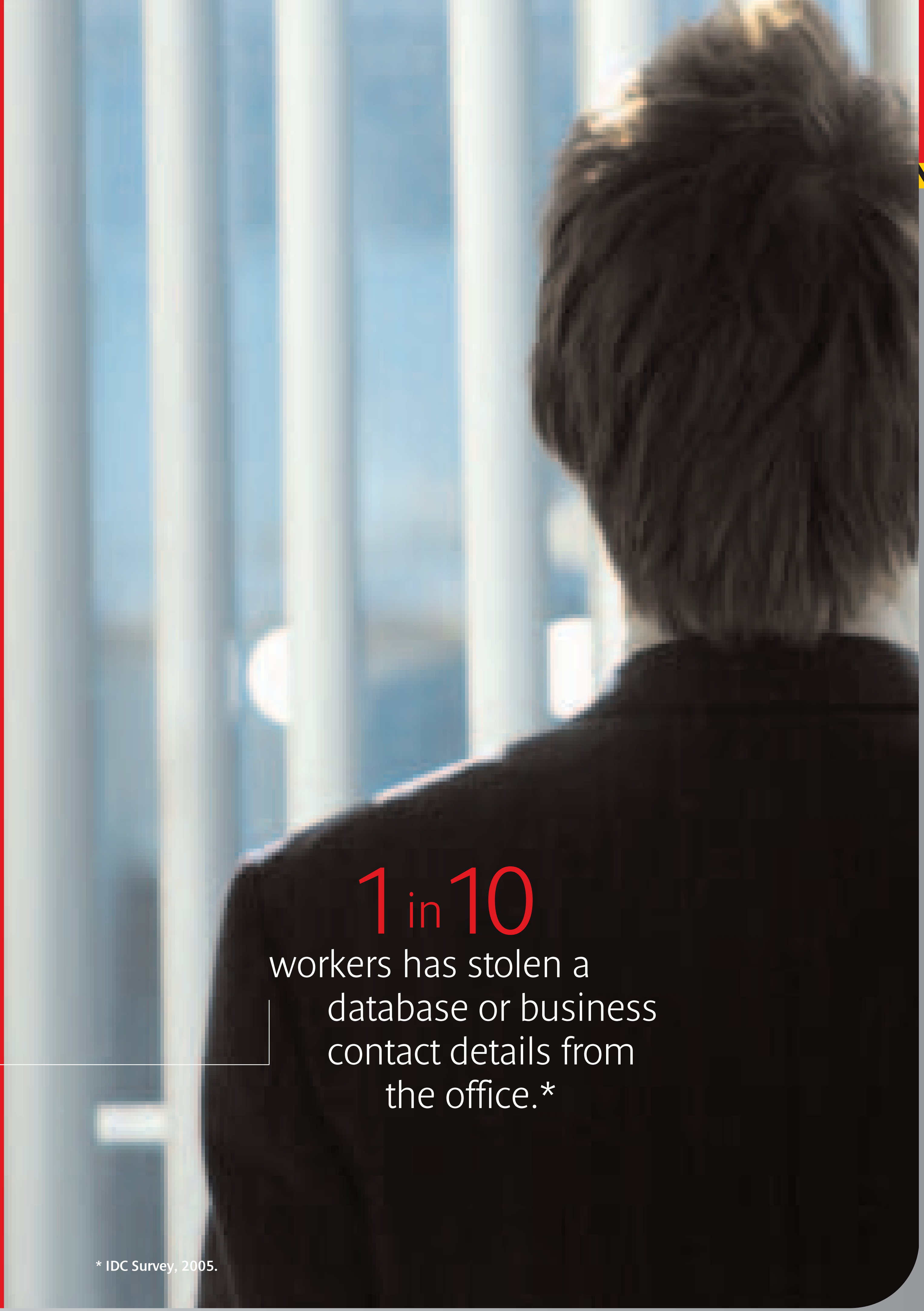
- Document and Hardware Security Solutions protect your hard-copy documents, as well as the printers that produce them.
- Network and Data Security Solutions protect your data while it is stored, and as it travels between the various devices on your network.

Internationally Recognised Standards

Canon can offer a range of products that have been evaluated against the Common Criteria Program, the recognised global standard for IT security set by international security agencies.

So you can rest assured Canon's security solutions will keep your information safe and secure.

Common Criteria



1 in 10 workers has stolen a database or business contact details from the office.*

* IDC Survey, 2005.

80%
of business fraud is perpetrated by employees.*

Add more with MEAP

MEAP, Multifunctional Embedded Application Platform, is a Java platform that runs on Canon multifunctional printers, enabling software applications to be loaded on to the device, so you can add extra security capabilities quickly, easily and cost-effectively.

* Gartner, 2006.

Document and Hardware Security

Could someone walk off with sensitive documents from your printer?

It's all too simple to send a document to print, get distracted and end up forgetting about it. By the time you get round to picking up the document, someone else could have taken it, read its contents or even made a copy.

It's also easy to forget that modern multifunctional devices are more than simple printers and copiers. They're also scanners and sophisticated communication hubs, giving unauthorised users the opportunity to scan confidential documents and email them off to someone else.

Canon offers a range of security solutions to keep your documents and hardware safe.

*Secure Watermark**

Prints an invisible watermark on documents so that, when copied, the word "confidential" appears across the document.

Confidential Watermark

Manually selected by users to print a visible watermark on print and copy output.

Electronic Signature (PDF)

User Signature: Identifies the author who sent a document.

Device Signature: Identifies which device a document was sent from.

Secure Document Release

Holds confidential documents at the print server for personal retrieval at the device. Documents can be released using various identification methods such as password, PIN, magnetic card, contact-less card and even fingerprints.

Secure Mailboxes

Lets employees save documents in a password-protected mailbox, then access the mailbox at the printer to select and print the documents they want.

Secure Printing

Allows staff to choose a password at their PC and use it at a device to print documents.

Department ID Codes

Lets administrators or security managers allocate each department its own code, so that only authorised users can access the MFP.

Single Sign-On

Ensures that only those users who can log on to the network can access the printer(s).

Job Log Conceal

Hides the details of recent print jobs so people can't 'pick the brains' of the device.

Simple Device Log in

Ensures that users log in and have their details matched against authorised user lists before using a device.

Cassette Locks

Enables only authorised persons to change media. Useful if only specific media is to be used through a particular device for designated jobs.

*Must be set up at device and is a default printer setting that applies the watermark to all output.

Network and Data Security

Could someone unauthorised gain access to your network?

Over the last few years, simple printers have evolved into multifunctional imaging devices that store data on a hard drive in exactly the same way a computer does. However, without adequate protection, unauthorised users can simply extract or reprint any confidential documents that have just been printed.

At the same time, external threats have grown too. With the amount of sensitive data now being sent over IP networks, high performance security on all your networking devices is vital, which includes only authorised computers and devices which can connect to your network and printers.

Canon offers a range of security solutions to keep your network and data safe from internal and external attacks.

Activation/Deactivation of Network Protocols, Ports and Applications

Allows any device to be blocked from communicating with Internet protocols deemed to be insecure.

IP Address Range Setting

(IP blocks) Ensures that only print jobs that come from authorised computers will be accepted and printed.

MAC Address Filtering

(Hardware blocks) Even more secure than IP Address Range Setting. Restricts printing access to a pre-defined list of network cards. Ensures access is only available to the users that you specify.

TCP/IP Service Control

Allows the administrator to disable specific network functions.

Encrypted Communication

HTTPS ensures that passwords and confidential information entered on a device are kept secure. Print jobs sent to the device via the Internet are protected by the secure version of the Internet Printing Protocol (IPPS).

Disk Erasure

Lets user totally erase data from the hard disk after a job has been completed. Also allows you to completely conceal the list of jobs processed from everyone except the system administrator.

Secure Data Transfer

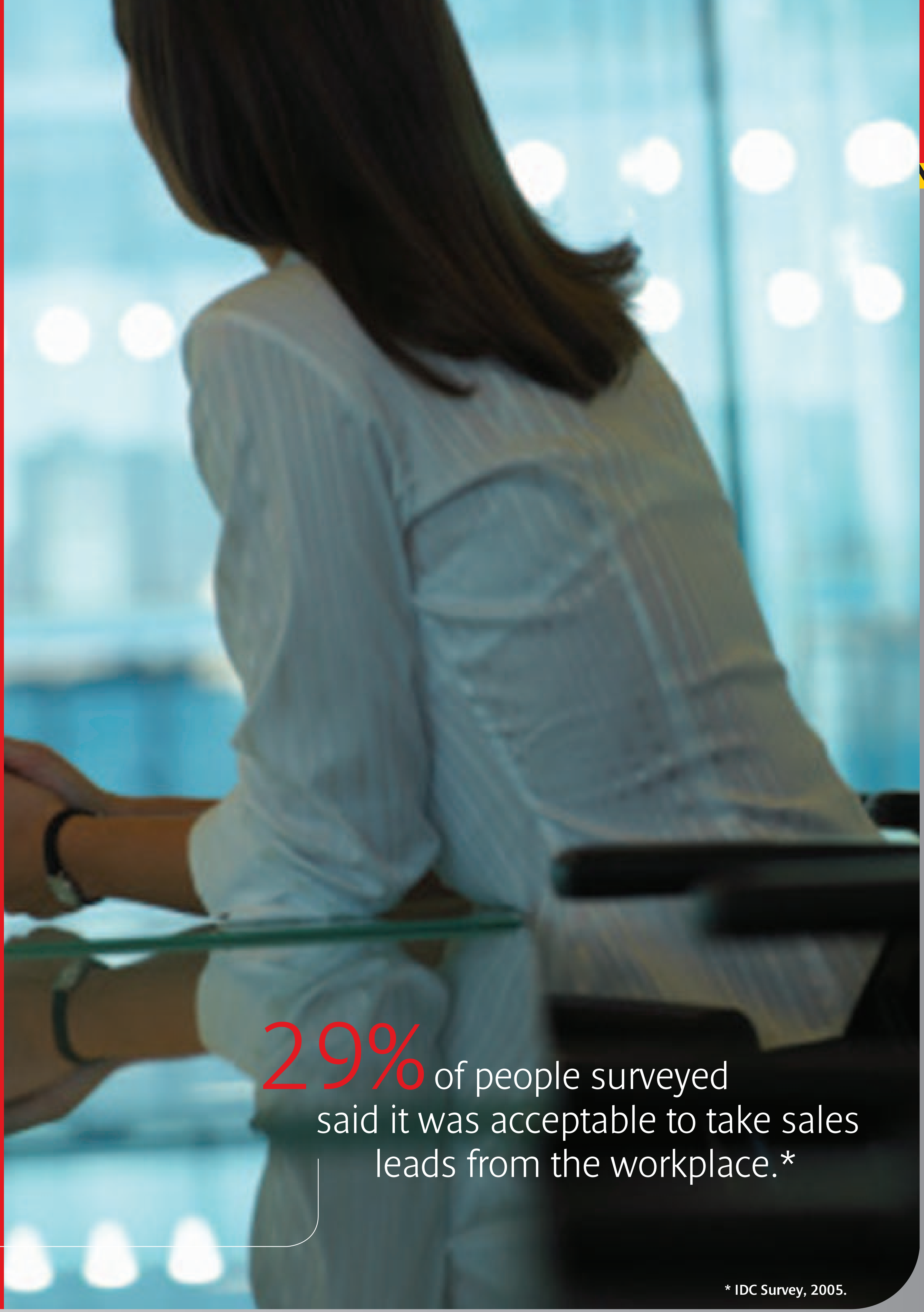
Wherever your data and documents are headed, across the office or around the world, HTTPS and IPPS mean they're protected in transit.

Hard Disk Data Encryption

High-security 168-bit encryption means that even if someone steals or hacks the hard disk from your printer, you can be sure they won't be able to read it.

Hard Disk Removal

In environments where data security is a major concern, Canon is able to remove the hard drive from a device for secure disposal at the end of its service life.



29% of people surveyed said it was acceptable to take sales leads from the workplace.*

* IDC Survey, 2005.

How Canon protects your print environment

Different businesses – and individual departments within the same organisation – demand different levels of security. Canon has four levels available and can help you choose the level that's right for your business. Let's take a look at some typical examples below of how we keep your print environment secure every day.

CANON'S FOUR LEVELS OF SECURITY:

🟦 Standard Security
Entry-level Document and Hardware security solutions.

🟩 Enhanced Security
An enhanced level of Document and Hardware security solutions.

🟧 Advanced Security
Network and Data security solutions for larger organisations.

🟥 Ultimate Security
Far reaching security across Document and Hardware, and Networks and Data security solutions.

🟧 Unauthorised users accessing your system

Personal Mailbox MEAP application using Single Sign-on for all devices means documents are only printed when authorisation is received at the printer – so sensitive material isn't left lying around.

🟧 Printing confidential information leaves a trail

Job Log Conceal removes all traces after confidential material is printed, so no trail is left.

🟥 Printer Hard Drive targeted by data thieves

Hard Disk Overwrite and Encryption conforms with Common Criteria EAL3, giving you an internationally certified level of document protection.

🟦 Hot-desking staff unable to keep confidential documents secure

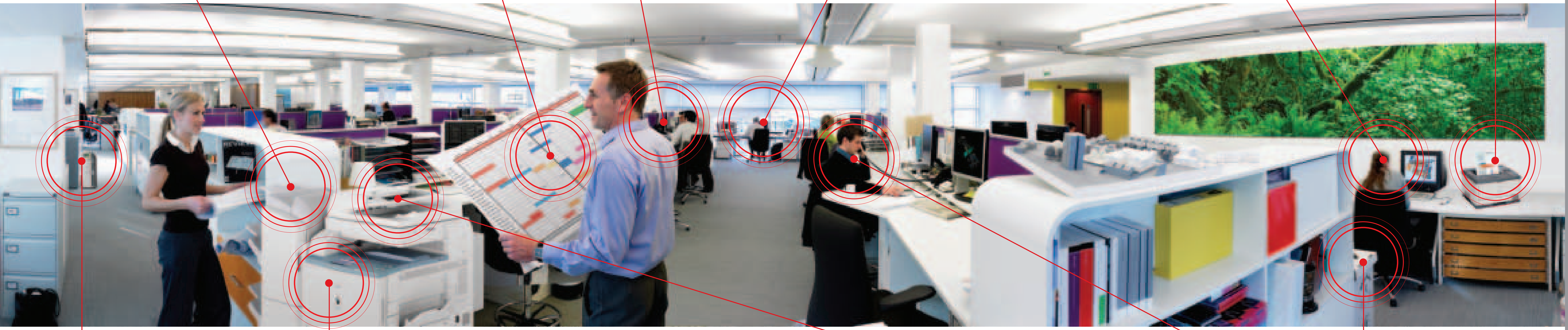
Staff that don't have a mailbox can still ensure confidential material is not left exposed on a printer, by using the Secure Print option.

🟥 Unsecure personal and sensitive details

SSL communication encrypts data so it can't be read by unauthorised persons.

🟩 Sensitive material left on the out-tray

Personal Mailbox functionality means print jobs are sent to a folder on the hard drive of the device and retrieved for printing by the user.



🟧 Unauthorised user hacking into your network

IP and MAC Address Filtering ensures that only jobs from authorised computers are printed.

🟥 Lack of control over which jobs are printed where

With uniFLOW Output Manager you can reroute jobs to the most appropriate printer, plus you have a full document accounting system enabling you to track who is printing what, and where.

🟦 Misplaced faxes

Cassette Locks control use of media, to ensure the correct media is used for each job, such as printing faxes on coloured paper for easy identification.

🟥 Confidential documents end up in the wrong hands

Optional MIND (Modular Identification Network Device) box allows users to release jobs using either proximity card, swipe card, PIN code or fingerprint ID at the device to retrieve the document.

🟩 Confidential documents ending up in the recycling bin

Secure and Confidential Watermarks clearly mark sensitive information and discourage unauthorised copying.