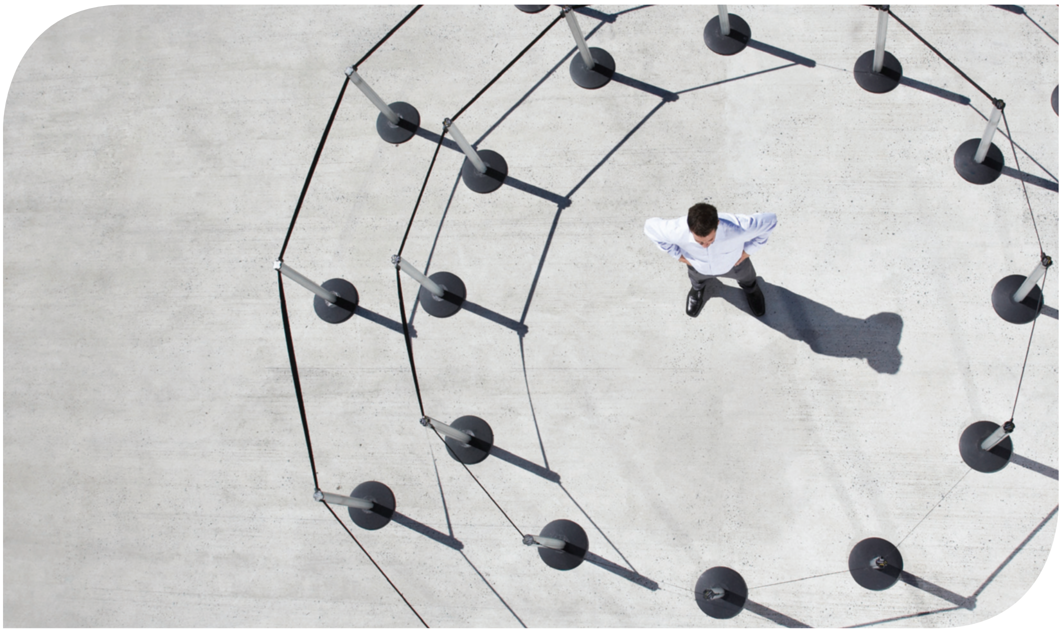
FUJI xerox Authorised Dealer

Stay secure



You know the value of your confidential data. Now just imagine the costs and damages if your information falls into the wrong hands. A breach in document security could result in unauthorised use or modification, harmful disclosure, or other unwanted outcomes – not to mention the average organisational cost of a data breach in Australia is $2 million.[1] 70 percent of companies reported accidental data breaches through printing, with a further 13 percent not sure if they had experienced a printing-related data breach.[2]

Technology has transformed the way employees conduct business. Today, documents take shape in not only the traditional hardcopy forms, but also in electronic forms on desktops and in email. Since employees create, produce, distribute and capture these electronic documents differently than traditional paper documents, this information is at high risk of theft or loss. And with security intensive information projected to represent 45 percent of all information created by the end of 2012,[3] companies must be prepared by securing the documents and document management systems that contain their most valuable asset – knowledge.

The average organisational cost of a data breach in Australia is $2 million.[1] 70 percent of companies reported accidental data breaches through printing, with a further 13 percent not sure if they had experienced a printing-related data breach.[4]

How can you keep your documents secure as well as ensure compliance to internal and external regulatory requirements?

Control access

Limiting who has access to your print device infrastructure is a key method of ensuring the security of documents that pass through it. Requiring authentication at the device using a swipe card or access code is a common method of ensuring unauthorised users can't access your networked print device. Your Fuji Xerox multifunction device can also be configured to integrate with your organisation's corporate directory to control destinations of scanned or faxed documents and prevent data loss.

Secure the document

Over 40 percent of office workers admit to picking up someone else's print-out by mistake.[4] Requiring authentication at the device using My Prints or other print-release technology solutions means that documents are not at risk of being collected from the device output tray – accidentally or intentionally – by another party. This means even the most sensitive information can be printed on a shared multifunction device without risk of the document falling into the wrong hands.

Even without a print-release solution, the secure print functionality embedded within Fuji Xerox multifunction devices allows users to set a password on their file at the time of printing and use the password at the device to release it.

Utilising watermarks can also protect and prevent unauthorised reproduction of sensitive material. You can set a watermark from the print driver settings to denote a confidential or internal-only document. The optional Secure Watermark Kit also prevents copying, scanning or faxing of documents that have been watermarked on other similar devices.

Using DocuShare as a document management system also allows you to control access to your archived documents, with the ability to set permissions on the viewing, downloading and editing of files, as well as keeping a record of document history for audit purposes. You can meet regulatory compliance requirements for record keeping without the burden of cabinets full of paper files, and in a much more secure manner.

Secure the device

When it comes to networked multifunction devices, vulnerabilities can be present because these devices can print, copy, scan to network destinations, send email attachments and handle incoming and outgoing fax transmissions. For those in IT, it's critical to the security of an organisation's network to make sure that security violations can't happen through network-connected devices – or at the devices themselves.

Fuji Xerox multifunction devices conform to the latest industry standards for network security, supporting IPSec to encrypt document content, SNMPv3 to securely transfer information to users and 802.1x to securely authenticate network devices before allowing document access.

The Data Security Kit available with Fuji Xerox multifunction devices gives administrators the option of encrypting, overwriting or deleting data from the device hard drive at any time or at defined intervals to ensure confidential information cannot be accessed by hackers through the network or from the device itself.

Monitor and audit

CentreWare Internet Services allows you to perform basic reporting on print, scan and fax activity history on any of your devices, so you can identify the source of a leak should one occur from within your organisation.

More sophisticated auditing of job history can be achieved when an authentication solution like My Prints is enabled, so you can be sure your documents are not being compromised.

Using a workflow automation solution such as Automate™ can also act as a record of document processes and approvals within your organisation. You can easily search for when an activity was approved, by whom, and bring up the relevant paperwork in the event of a problem occurring. Setting pre-defined workflows also ensures documents go through the required steps to meet any regulatory standards.

References:

1. 2010 Annual Study: Global Cost of a Data Breach, Research conducted by Ponemon Institute, LLC, Sponsored by Symantec, May, 2011. **2.** Quocirca "closing the print security gap" October, 2011. **3.** IDC, 2009. **4.** Cutting Paper: The SME FD's Guide to Document Management, Pegasus Software, 2008.

For more information or detailed product specifications,
Please call us on 02 4220 5000 or visit us at **fxillawarra.com.au**

FUJI XEROX BUSINESS CENTRE ILLAWARRA
87 Auburn Street, Wollongong NSW 2500
ABN: 62 096 607 135