



Modern business security challenges and how to solve them

The flexible workplace issue



Modern businesses need to access, move and share information at a speed and scale that's greater than ever before. Employees expect more flexible, efficient and collaborative ways of working. As the workplace expands beyond the traditional office walls, you need your information to be as mobile as your workforce.

These are scenarios almost every business faces today – and while they offer great opportunities for business productivity and innovation, they also pose potentially serious threats to the security of your business data.

How do you balance employee expectations with the need to keep your information safe? This playbook explores the challenge of building a flexible yet secure digital workplace, outlines the security risks to consider, and offers some tangible solutions for addressing them.

RICOH
imagine. change.



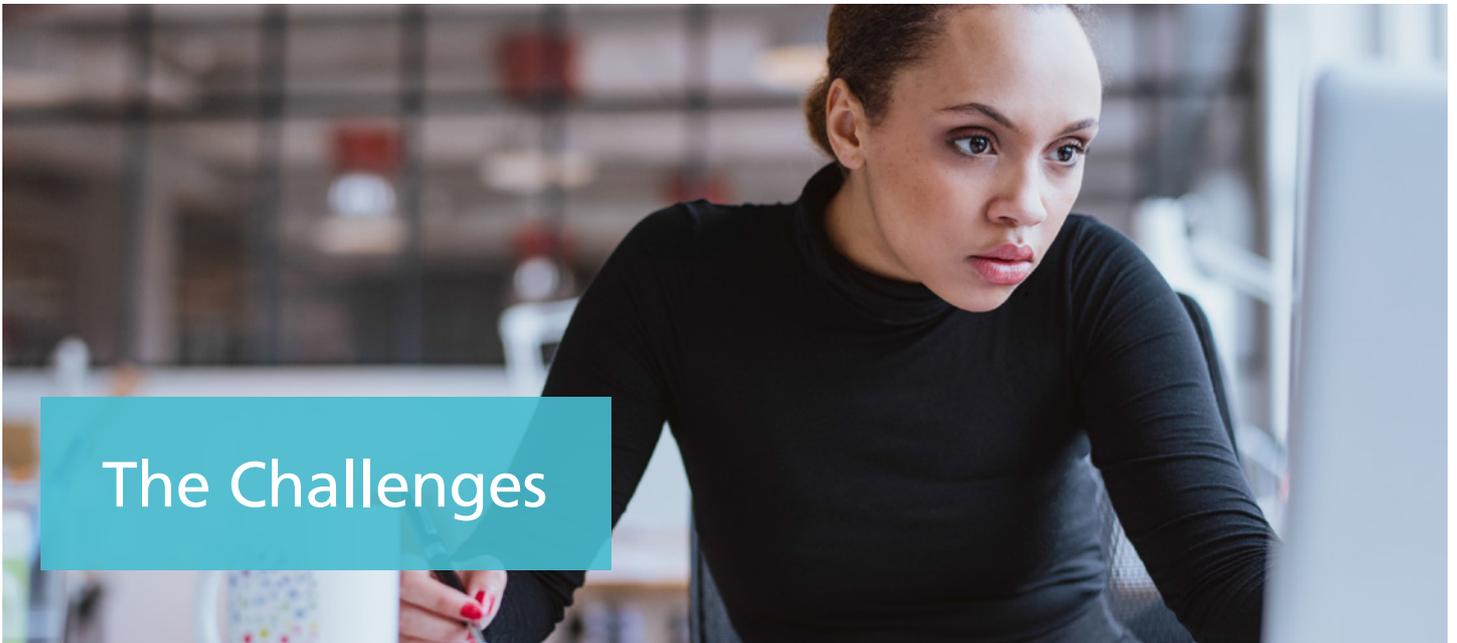
The Situation

Your employees expect a flexible workplace and greater mobility.

Today's workers have been empowered by technology to expect that they can work from anywhere.

Even if you don't have remote staff, the proliferation of mobile and cloud technology means that work is no longer confined to the desk. The mobility ideal for professionals is a lot more than just email on your phone – it's seamless access to documents, data, colleagues and customers, whenever and wherever needed. This freedom has become a table-stakes expectation, so locking it down isn't an option if you want to attract and retain talent.

Yet enabling a truly flexible and mobile workplace can expose your business to a new realm of potential security threats. What happens when a laptop or phone is lost or stolen? How do you manage the security of your information when employees can access it from personal devices? How do you defend against prying digital eyes when workers connect to public WiFi?



The Challenges

Having an inadequate system for storing and sharing information with employees inside and outside of the office can have a drastic impact on both productivity and security.

Feeling that they don't have the tools they need at their disposal, your employees turn to what they know to fill the gap. Files are emailed to personal accounts and accessed on home computers. Documents are stored and shared using consumer cloud solutions. Unsanctioned adoption of different cloud services can quickly turn a well-designed information system into a fragmented mess.

These workarounds can lead to the ominously named phenomenon of 'data leakage' which represents a steady loss of control over your information.

Well-meant workarounds expose your valuable information

84% of employees use personal emails to send sensitive files¹

The 'Bring Your Own Device' approach is increasing

More than half of North American and European companies are developing BYOD programs in response to workforce demand²

Many data breaches are accidental

More than 28 million data records were compromised in the UK in 2017. Of these, 38% were attributed to accidental loss³

Public WiFi is a minefield

It's estimated that as few as 5% of public WiFi hotspots are encrypted, but 95% of people use them for work at least once per week⁴

You may not know the extent of the risk

Over half of IT managers lack any visibility into file and data transfer within their organisations⁵

1. Ipswitch File Transfer, 'Are Employees Putting Your Company's Data at Risk? Survey Results Exposing Risky Person-to-Person File Sharing Practices: An eBook report' www.ipswitchft.com. 2. [www.forrester.com/Bring-Your-Own-Device-\(BYOD\)](http://www.forrester.com/Bring-Your-Own-Device-(BYOD)). 3. www.theregister.co.uk/2017/09/20/gemalto_breach_index/ 4. gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/ 5. Ipswitch File Transfer eBook report www.ipswitchft.com



The Solutions

Building secure mobility begins with an understanding of how information flows through your organisation, where it's stored and how it's used. As data moves around your business through potentially a myriad of devices, it needs to be protected with sophisticated security measures.

Get your info into the system

The best file sync and share system isn't going to do much good when the information you need is sitting in a filing cabinet. A scan-to-cloud solution can intelligently send documents straight to your service of choice and enable secure storage.

Scan-to-cloud easily and securely with Ricoh's Streamline NX software solution.

Get it out when you need it

Despite the convenience and flexibility of digital files, there's a time and place for hard copies. Ensure that the right information always falls into the right hands with **secure print solutions such as Ricoh's Streamline NX**

Print2Me functionality.

Mobile and guest printing

The urgent need to print by visiting staff and guests is often satisfied by sending attachments to a contact on site. This can increase the risk of viruses and malware being passed inadvertently. Peer to peer communication between the device and mobile phone and cloud based pull printing mitigates this risk. **Learn more about Ricoh's MyPrint mobile printing.**

Manage your information

Implementing a document management solution can ensure that each employee has an appropriate level of access to information. It can also provide intelligence about how, when and by whom documents are being viewed or edited.

Discover how Ricoh and DocuWare work together to enable secure and efficient document management.

Ask an expert

Visit us at ricoh-europe.com or contact your local Ricoh representative to learn how we can help you on your way to a workplace that's as secure as it is flexible.



Ricoh Europe PLC
20 Triton Street,
London, NW1 3BF



+44 20 7465 1000



ricoh-europe.com

RICOH
imagine. change.

The facts and figures shown in this brochure relate to specific business cases. Individual circumstances may produce different results. All company, brand, product and service names are the property of and are registered trademarks of their respective owners. Copyright © 2017 Ricoh Europe PLC. All rights reserved. This brochure, its contents and / or layout may not be modified and / or adapted, copied in part or in whole and / or incorporated into other works without the prior written permission of Ricoh Europe PLC.