Is your business secure?

Realities, risks and solutions in security:
essential reading for smart businesses

Cyber security is the biggest threat to the survival and success of modern businesses.

Companies of all sizes are at risk of falling victim to disruptive attacks such as phishing, DDoS or ransomware – the costs of which run into the millions. Government regulations such as the GDPR are increasingly looking to punish business with potentially crippling fines for failing to secure their systems and data appropriately. Meanwhile, the expansion and digitisation of the modern workplace compounds cyber challenges further; as workflows spread across devices, networks and geographies, information must be protected as it moves around a business.

At the same time, the capabilities of office printers and multifunction devices have increased ten-fold in recent years. They are now responsible for a huge proportion of business data input, output, transfer and storage. This makes them potentially one of the most dangerous, yet often overlooked, threat vectors in the workplace today.

Faced with these challenges, now more than ever businesses must have fundamentally secure document and data management systems – and be able to prove it.

60%

Businesses in Europe and USA that reported suffering a data breach through unsecured printing in the past year*

*Quocira Enterprise MPS Study, 2017. Data set: 240 organisations of 500+ employees from UK, France, Germany and USA across various industries.

€20m

Maximum potential fine for a GDPR non-compliant company*

*EU GDPR Portal, 'Frequently Asked Questions about the incoming GDPR' found at www.eugdpr.org/gdpr-faqs.

RICOH
imagine. change.

Four things to think about to secure your business

Is your data secure?

- Data storage
- Risk of loss / theft
- Risk of cyber attack
- Risk of alteration / corruption
- Unforeseeable events

Is your document management secure?

- Document sharing
- Document destruction
- Device management
- Secure printing

Is your digital workplace secure?

- Workflow management
- Mobile working
- Protecting data in transit
- IT infrastructure

Are you compliant?

- Regulatory compliance
- General Data Protection Regulation (GDPR) compliance

The reality

Your data is your business' most valuable asset. While it may be easy to have a head-in-the-sand approach towards threats like data theft, cyber attack or natural disaster, the impact of remaining unprotected against these could be devastating.

The reality

Your everyday document sharing, storing and printing could also be your security undoing. The humble office printer is an often overlooked vulnerability in secure document management.

The reality

With the great advantages of flexible and mobile working also come great risks – how do you manage a Bring Your Own Device approach? Insecure public wifi? Devices falling into the wrong hands?

The reality

In addition to existing regulatory obligations, the GDPR is coming in May 2018 – how do you know if you're ready, and how can you prove your compliance?

The risks

- Cyber attack – Ricoh repels around 8 billion firewall attacks per month
- Loss of business continuity through natural disaster
- Data theft from inside or outside the organisation

The risks

- Sensitive information falling into the wrong hands through insecure printing
- Release of confidential information through incomplete document / device destruction
- Device hacking

The risks

- Loss of confidential company information through weak links in a flexible working environment
- Data breaches through lack of visibility and control over device usage

The risks

- Huge cost in fines for non-compliant companies
- Reputation damage

This combination of security threats and legislative requirements means the potential for reputational and fiscal damage from cyber risk has never been greater. Now is the time to invest in the security of your digital workplace with a partner you can trust.
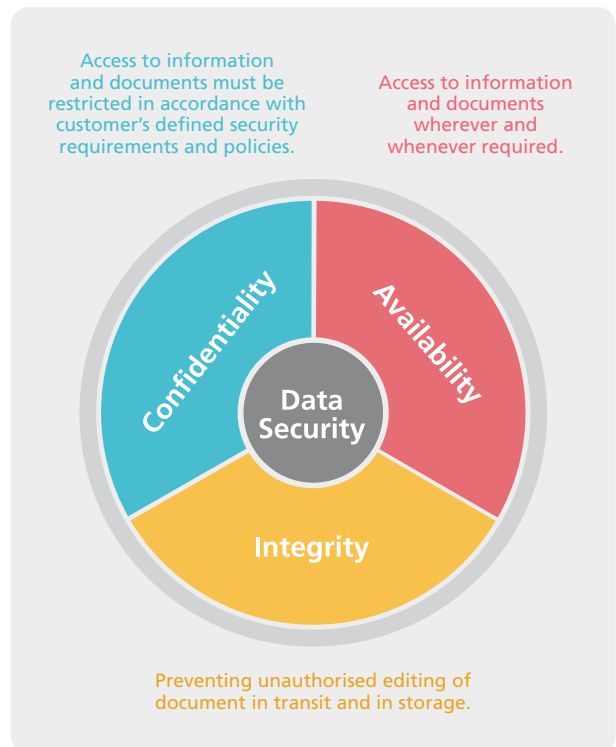
RICOH
imagine. change.

The good news is, Ricoh has already thought about security for you. We are expert in understanding these risks because we've spent decades developing ways to mitigate them, through state-of-the-art security measures embedded into every product and solution across our entire portfolio. Our printers, for example, have featured secure hard disk overwrite capabilities for over 20 years. Security is in the DNA of our entire digital workplace portfolio.

Ricoh provides a consistent worldwide service and support structure for customers that ensures threat intelligence is efficiently shared and acted upon. Not only is IEEE 2600 certification implemented as standard across our print-output devices, Ricoh is a leading member and key author for the IEEE Standards Association. Ricoh is also ISO 27001 certified, and committed to continuing to comply with this information security management system.
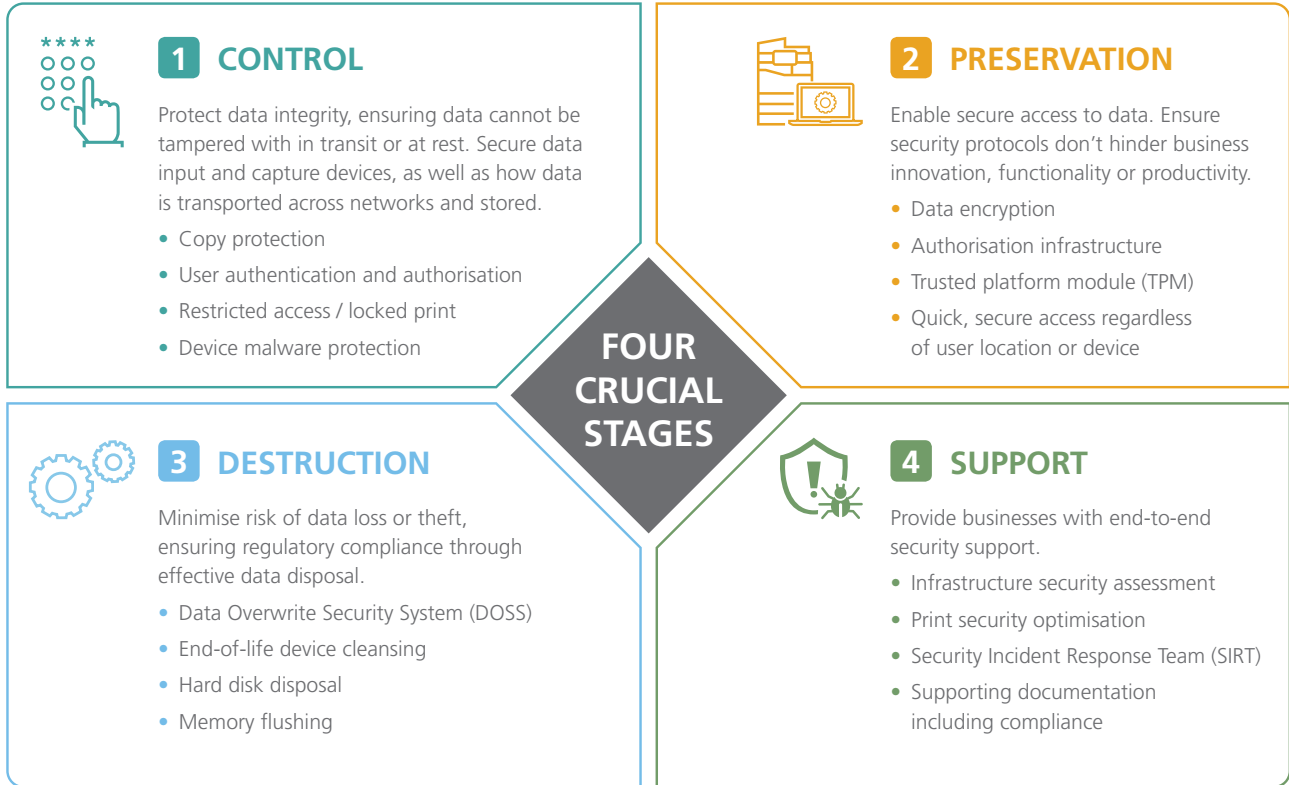
To meet the demanding requirements of effective, demonstrable cyber security best practices, security is included in every product and service in Ricoh's portfolio by design – never as an afterthought. We believe this holistic view of vulnerabilities is essential for survival in modern business.

Every aspect of our security approach is underpinned by our 'CIA' principles of privacy and security: confidentiality, integrity and availability.

Access to information and documents must be restricted in accordance with customer's defined security requirements and policies.

Access to information and documents wherever and whenever required.

Confidentiality

Availability

Data Security

Integrity

Preventing unauthorised editing of document in transit and in storage.

RICOH
imagine. change.

How Ricoh secures the digital workplace

We understand the importance of securing your digital workplace across the entire – and complex – lifecycle of business data. We achieve this through implementing security measures across four crucial stages: Control, Preservation, Destruction and Support.

1 CONTROL

Protect data integrity, ensuring data cannot be tampered with in transit or at rest. Secure data input and capture devices, as well as how data is transported across networks and stored.

- Copy protection
- User authentication and authorisation
- Restricted access / locked print
- Device malware protection

2 PRESERVATION

Enable secure access to data. Ensure security protocols don't hinder business innovation, functionality or productivity.

- Data encryption
- Authorisation infrastructure
- Trusted platform module (TPM)
- Quick, secure access regardless of user location or device

FOUR CRUCIAL STAGES

3 DESTRUCTION

Minimise risk of data loss or theft, ensuring regulatory compliance through effective data disposal.

- Data Overwrite Security System (DOSS)
- End-of-life device cleansing
- Hard disk disposal
- Memory flushing

4 SUPPORT

Provide businesses with end-to-end security support.

- Infrastructure security assessment
- Print security optimisation
- Security Incident Response Team (SIRT)
- Supporting documentation including compliance

The modern digital workplace must be as dynamic as the cyber threats it faces and as flexible as the working practices within it. That's why we believe that cyber security should operate seamlessly across the technology our customers choose to enable their workplace. With our commitment to ISO 27001 throughout our organisation, and IEEE 2600 certification across our products, you can rest assured that with Ricoh you'll have best-of-breed security controls in place – no matter how you choose to structure and grow your business.

Want to get technical? For further details of Ricoh's security capabilities, download the full report: **Ricoh Security Solutions**

To discover how Ricoh can help you secure and empower your business, visit us at ricoh.ie or contact your local Ricoh representative.

Ricoh Ireland
First Floor Unit 160 –
Airside Business Park
Swords, Dublin

00353 18 953930

ricoh.ie

RICOH
imagine. change.