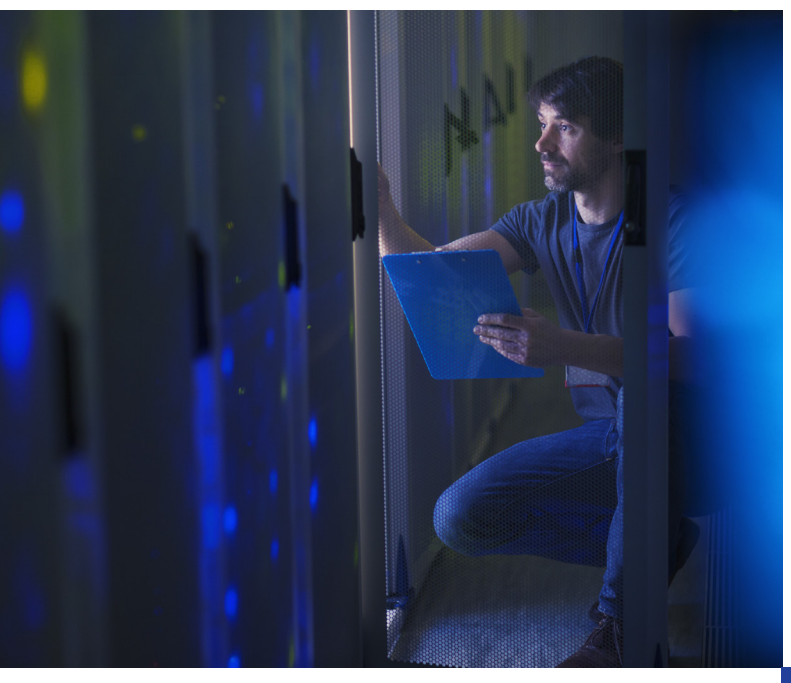

SECURING THE CONNECTED OFFICE

The rapid expansion of Internet of Things (IoT) is causing significant security challenges for organisations.

Technology has made sharing information easier than ever with cloud computing, mobile working and managed print services becoming more prevalent.

More than half of decision makers in EMEA now **share documents** outside company systems.

But as innovation growth continues, **data security remains important...**

32% of companies were victims of **cybercrime** in 2016[1]

The average total cost of a **data breach** was **€3.07million** in 2017[2]

Especially as the **basics** often get **overlooked**

Security blind spot

Traditional enterprise devices can be weak spots too:

42% of documents contain sensitive information, yet **50% of managers** are concerned about **people leaving confidential documents** on a printer or copier

47% of managers are already aware of employees **losing documents inside** their organisation, with **46%** aware of this happening **outside their organisation**

and the **General Data Protection Regulation** is putting even more **pressure on businesses...**

80% of **senior managers** looking to **upgrade** their **document security** in the next **1-2 years**

Information security doesn't need to be difficult to master...

But it means considering the information journey and all connected devices in the office...

77% cited that **systems** that **convert paper documents into digital**, editable documents are **critical** or **important**

While **multi-function printers** (MFP) bridge the digital and physical information boundaries:

Print Copy Send Scan

Each action provides a security touchpoint that needs to be considered.

Four steps to securing the connected office

There are steps organisations can take so that they **enjoy the benefits of IoT**, without the security headache.

Step one

Audit and assess - Map out your current physical and digital vulnerabilities and prioritise

Step two

Protect the environment - Perform a network health check to identify any additional security gaps

Step three

Be smart with devices and print systems - Choose devices that align with your security policies and procedures

Step four

Adopt a policy for protection - Review and continuously update security policies and educate your workforce on the importance of data security

Download the 'IoT Security: 4 steps to a safer connected office' report here

1. http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
2. https://www.ibm.com/security/data-breach