

Maintaining a secure printing ecosystem

As part of the Brother
Digital Transformation series



Barriers to investment in printing security

With the rising threat of high-profile confidentiality breaches and hacks, most small and medium sized businesses (SMBs) are very aware of the need to protect their IT systems.

Managing the security of the IT estate is a challenge which needs to be tackled wholesale. Printers, scanners and copiers need to be just as secure as other IT equipment. If overlooked, these devices risk offering hackers an easy backdoor into the organisation. SMBs are becoming increasingly aware of the importance of this issue, with **72%** of businesses saying that it is critical that their printers, scanners and copiers are secure. This is even more acute amongst those organisations handling sensitive data in industries such as Professional Services (**82%**) and Healthcare (**81%**).

However, this still leaves close to a third of organisations not recognising its importance. And concurrently, almost half do not feel that their organisation has sufficiently invested in printer hardware security.

If businesses understand the need to invest in printer security, why are they not currently doing so?

Our research highlights two clear reasons:



Insufficient accountability for printer security



Lack of understanding and knowledge around security threats and standards

This report is designed to help SMB decision-makers understand the importance of printing security, as well as how to implement secure printing solutions. It is part of a wider series that aims to inform decision-makers on how to best utilise digital technologies within SMBs. The reports are based on a robust programme of research undertaken amongst SMB decision-makers in the EMEA region. The series is split up into four reports, each tackling one of the following themes:

- Digital workflows
- Implementing the right solution for your business
- Security
- Sustainability



Who is responsible for printer security?

All too commonly there is a lack of clarity and accountability around individual responsibility for printer security. Almost half of SMBs across Western Europe **(44%)** report that it is unclear who is responsible for printer security in their organisation. Where accountability falls short, it is consequently likely that decision making and implementation of printer security will suffer, leaving businesses vulnerable.

Responsibility for printer security is likely to be largely unassigned since the printing setup has not traditionally been recognised as a 'weak point' in the same way as other devices such as laptops. Whilst our research shows that decision-makers are beginning to realise that printing security is vital, SMB job roles don't seem to reflect this as yet.

SMBs are particularly vulnerable to a lack of accountability as there is often a very small number of employees looking after the entire organisation's suite of hardware and software. If IT professionals are not aware of the risks of printing security, it can become a low priority.

However, all employees within an organisation have some level of responsibility for ensuring that sensitive information is kept secure.



Whilst IT and technology specialists are responsible for the security of devices themselves, employees have a responsibility for ensuring that data itself is kept secure. Data security is perhaps the greatest risk area for commercially sensitive business information.

Data security includes a wide range of threats, including:

-  unauthorised access to print outs
-  forgetting to log out after printing confidential documents
-  lack of traceability for who has accessed which documents on the printer

Almost 9 in 10 businesses have experienced a printer-related security incident...



... and seven in ten (**72%**) claim that data security is a bigger threat than device security. However, currently, less than one in three businesses say that they are very confident that their printing infrastructure includes sufficient security measures. This is compared to the **53%** of businesses who feel they do have the right hardware security in place.

The majority of SMBs (**64%**) also say that ensuring their data is secure is a top priority. This is seen as a key challenge and can be a real hinderance to efficient performance.

Currently, almost half of SMBs (**48%**) say they have few or no processes in place enabling them to account for who prints or collects printer jobs. It comes as no surprise that almost nine in ten businesses (**86%**) report having had a printing-related security incident.

These security incidents are most commonly linked to confidential documents being left unattended on the printer, printouts not being collected, or employees picking up confidential documents that aren't theirs.

As a result, the majority of SMBs (**64%**) are starting to put measures in place to tackle printing-related security issues, by restricting access to certain printers or introducing ID cards / PIN codes to release print jobs to the right people.

This is a step in the right direction. In the coming years, it will be important for all businesses to introduce more secure processes and for those already on the journey to maintain and improve their accountability and auditing trails.

There are three main objectives for true information security, which comprise the acronym CIA.

These cover both device and data security:

Confidentiality

Protecting confidential business data to ensure it is only shared with the intended recipient. Key to this is authentication and authorisation measures which require users to verify their identity and that they are permitted to do what they are attempting to do, before any printing is released.

Integrity

Ensuring the device firmware is secure and resilient to hacking and other external threats.

Availability

Ensuring the device is up and running and accessible to authorised users to perform crucial work tasks.

Lack of knowledge fosters poor security practices

Less than a third (**32%**) of key IT decision-makers working within SMBs say they have advanced knowledge of technology security and potential threats. If IT decision-makers do not have sufficient threat knowledge, then businesses will continue to struggle to put the appropriate measures in place to protect themselves. In SMBs, the IT decision-maker typically has a role which covers lots of different technology bases. It is understandable that they are not experts in printer-specific security.

Often jargon is the culprit. Over half (**51%**) of SMBs say there is too much jargon being used around printer security, and this is particularly the case in France and Italy.

And almost 60% of SMBs say they have a good understanding of relevant security standards.

Related to this, decision-makers are also unlikely to have an authoritative knowledge of the printing technology providers that could be most relevant to their security needs. As a result, it's not surprising that businesses are looking to brands they 'know' to provide secure printers, without truly understanding what security measures they do or do not currently have in place.

Printer partners need to do more to help you decode the relevant security standards, and to ensure you choose the best solution for your business.



Brother Insights

Given the complex nature of the print security landscape, Brother has seven crucial insights and recommendations to help SMBs protect themselves from the far-reaching financial, legal and reputational implications of a data loss.



Get the Board onboard

The scale of devastation caused by cyberattacks and data breaches, combined with the requirements of General Data Protection Regulation (GDPR) legislation, mean print security needs to move beyond the domain of the IT department. It must be strategically considered at board level with Chief Information Officer (CIO) and Chief Information Security Officer (CISO) involvement.



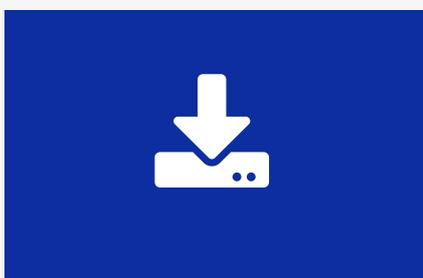
Conduct a thorough audit

It is crucial for businesses to uncover any potential print security vulnerabilities by ensuring their print environment is included in regular security audits. This is particularly important if your business has a mix of new and legacy devices. With regards to managed print services (MPS), not only do most providers offer full assessments, an evaluation will structure the ongoing monitoring of devices once the fleet is optimised and secured.



Change pre-set admin passwords

Default or pre-set admin passwords are a weak point for print devices – the good news is this is easily fixed. Once the device is installed, simply change passwords, opting for something strong and secure.



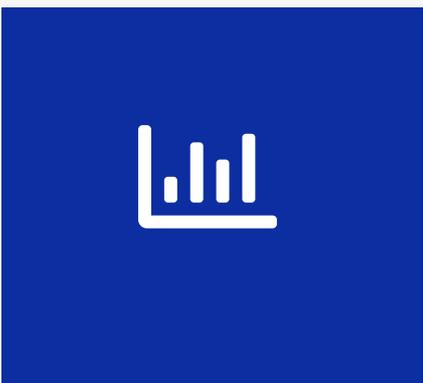
Update your firmware and patch

Potential security vulnerabilities for print devices can be significantly reduced by updating firmware and configuring the device for automatic updates. If you have any questions around this, contact your print device manufacturer for advice.



Protect print jobs

It's not only printing devices that need protecting, but the documents you are sending to print. End-to-end encryption of network traffic ensures secure transfer of print jobs to printers. As most printers temporarily store print jobs, ensure data is encrypted.



Monitor devices

Knowing the current status of your printing devices provides a holistic view of your entire print environment. Businesses should consider using software tools to monitor devices and allow issues to be fixed as soon as they happen. Devices generate a wealth of data and this can often be used to identify potential security events and enable fast responses to attacks. MPS users can also obtain regular compliance reports, which should include data breach monitoring and reporting.



Train employees

With many data loss incidents being caused unintentionally, it is vital that businesses educate employees on the importance of protecting sensitive information and raising awareness of malicious threats. Often, MPS providers will offer help with training needs.



Final thoughts

Printing systems may have been an overlooked aspect of organisational security in the past, but SMBs are increasingly realising their importance. Nevertheless, significant challenges remain for implementing printing security.

SMBs will have to clearly define responsibility around printer security, to ensure that devices are properly protected and keep up with threats. As well as device security, data security breaches are also a vital consideration, and the cooperation of internal employees will be necessary in order to minimise risks.

Even if there are clear definitions of responsibilities within SMBs, having sufficient knowledge to effectively manage printing security is still a major challenge. Printing technology is increasingly complex and a world full of jargon. Businesses should look to rely on trusted suppliers to make sound decisions.

An effective printing setup needs to be more than just secure. The other reports in this Digital Transformation series have more information on implementing digital workflows, maximising productivity, and ensuring that your setup is sustainable.

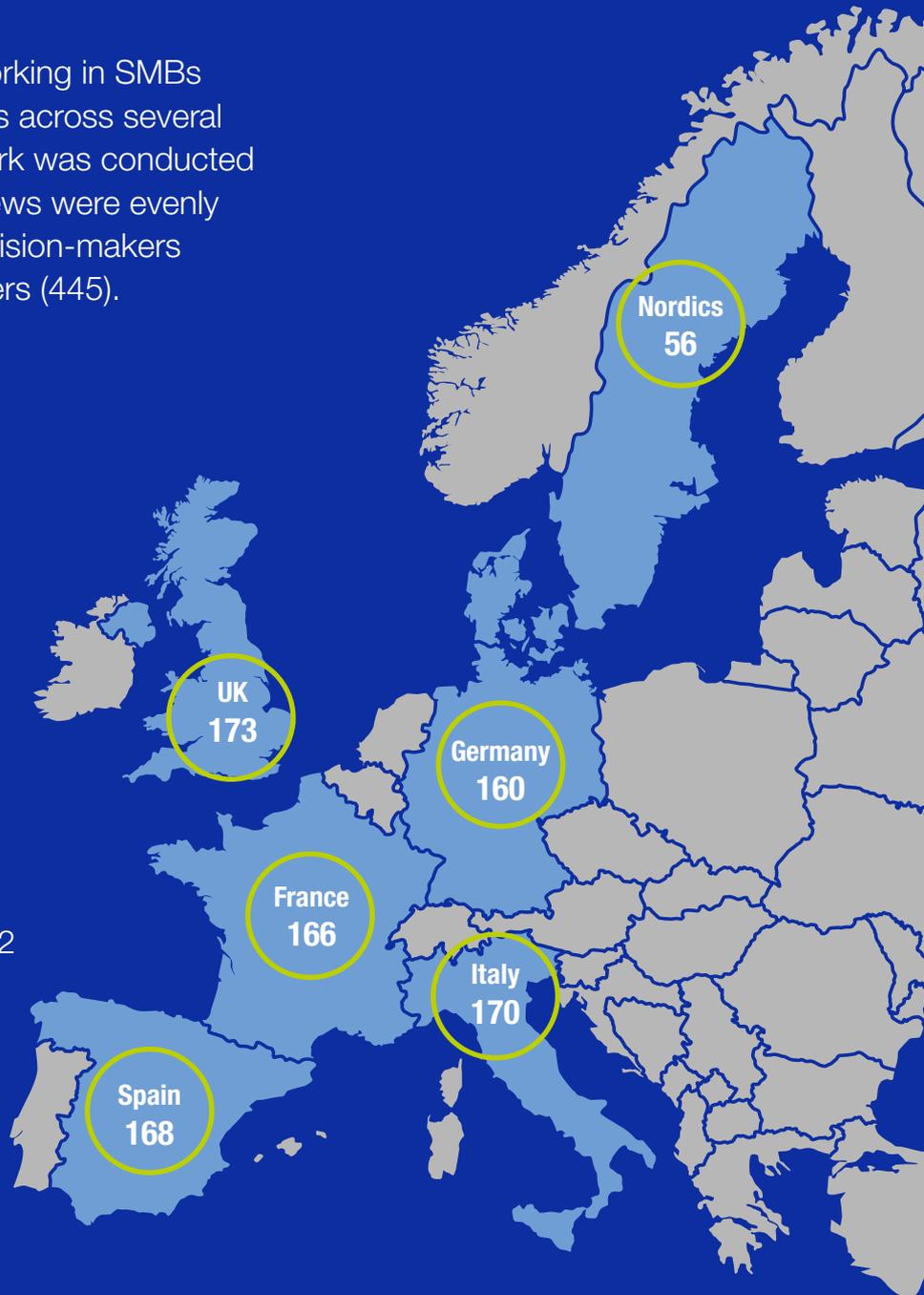
Our methodology

This report is based on 893 online surveys with IT and business decision-makers.

IT and business decision-makers working in SMBs with between 10 and 499 employees across several Western European markets. Fieldwork was conducted across 2019 and early 2020. Interviews were evenly split between strategic business decision-makers (448) and business IT decision-makers (445).

Key industries interviewed:

-  Healthcare - 152
-  Retail - 117
-  Logistics - 113
-  Hospitality - 81
-  Transportation and storage - 62
-  Professional services - 65
-  Manufacturing - 54
-  Financial services - 53
-  Education - 51
-  Construction - 39



Additional interviews were from other industries, including energy, pharmaceuticals, agriculture, defence, property & real estate, sports and entertainment.

The research was conducted by market research agency, Savanta.

Arriving soon

brother
at your side

www.brother.eu

Brother International Europe Ltd
Brother House, 1 Tame Street, Audenshaw,
Manchester M34 5JE
Tel: +44(0)161 330 6531
Fax: +44(0)161 330 5520

All specifications correct at the time of printing and are subject to change. Brother is a registered trademark of Brother Industries Ltd.
Brand product names are registered trademarks or trademarks of their respective companies.