quocirca

Business and IT Analysis

Global Print Security Landscape, 2019

A global market perspective on print security, 2019

February 2019

The far-reaching financial, legal and reputational implications of a data loss mean that information security is a business imperative. Safeguarding the ever-increasing volumes of valuable corporate data against unauthorised access has become integral to maintaining business operations and adhering to increasingly vigorous data privacy compliance requirements.

For many organisations, their cyber-attack surface area is increasing as connected Internet of Things (IoT) endpoints proliferate. These include both legacy and the new breed of smart printers and multifunction printers (MFPs). Consequently, businesses must take a proactive approach to print security as these print devices can provide an open door to corporate networks. By taking steps to analyse the potential vulnerabilities of print environments, businesses can mitigate risks without compromising productivity.

This report discusses the risks of unsecured printing and recommends best practices for integrating print into an overall information security strategy. It also highlights some of the key offerings by print manufacturers and independent software vendors (ISVs) in the market.

Louella Fernandes
Quocirca
Tel : +44 7786 331924
Email: Louella.Fernandes@Quocirca.com

Contents

quocirca

Executive summary

Data breaches are rarely out of the headlines and compliance pressure, such as the introduction of GDPR, means security remains high on the corporate agenda. Cyber threats and data breaches are no longer the sole domain of the IT department, they must be considered at board level as the repercussions are simply too big to ignore. Businesses of all sizes are potentially exposed to reputational, legal and financial losses as the result of cyber attacks. Due to the increasing sophistication of attacks and the emergence of insider threats, businesses face a battleground to balance business productivity with the need for privacy and security. One area of the IT environment which is often overlooked is the print infrastructure. The majority of organisations rely on print to support business-critical processes, meaning it can be the gateway to valuable, confidential and sensitive information.

Quocirca's Print Security 2019 report discusses how print security is becoming a greater concern to businesses with 59% reporting a print-related data loss in the past year. With only 27% classed as print security leaders, it is imperative that businesses become more print security conscious, particularly as they look to close the paper to digital gap in their business processes. This ultimately requires print security to move higher on the C-level agenda.

In response, print manufacturers are elevating awareness of print security risks. Today most offer a diverse range of product offerings encompassing built in hardware security, print security solutions and comprehensive security and risk assessments.

HP has cemented its lead as a visionary for print security, driving industry standards and offering one of the most comprehensive hardware, software and services portfolios. Nevertheless, most competitors are hot on their heels in developing their print security propositions. Leading players are moving to a secure-by-design approach, where security is built in from the ground up on new hardware.

What is setting the leaders apart in the market is their investment in security services such as assessments, monitoring and analytics. As the threat landscape becomes more sophisticated, machine intelligence will be key in being able to respond to or predict threats. This will enable an organisation to enhance their print security posture and mitigate potential risks.

Key findings:

- **Businesses remain reliant on printing.** Print will continue to play an on-going role in the business processes of most US and European organisations. 87% expect print to still be important in two years' time compared to 91% today.

- **The dependence on print creates risk.** Print is considered to be one of the top security risks to any organisation. 66% rank print in their top 5 risks, second only to cloud-based services at 69%.

- **Print security maturity varies.** Organisations vary in their capability to ensure the security of their print environment. In Quocirca's Print Security Matrix, 27% were classed as print security leaders, with 17% as laggards and the rest classed as followers. USA had the most leaders at 36%, UK the least at 18%.

- **Businesses are increasing their print security spend.** On average 11% of IT security spending goes on specific print security measures. 77% say print security spending is increasing.

- **Print related data breaches are frequent and costly.** 11% of all security incidents are print related, equating to an average of nine print-related incidents per year. 59% of these lead to data losses, costing an average of £313,000 per-annum to deal with. Other impacts include lost productivity and revenue.

- **The majority are concerned about malware attacks.** There is a perception gap where security risks are concerned. The top perceived security risk is malware, rated as the highest concern by 70%. However, when it comes to actual incidents, the most likely cause is the accidental actions of internal users, which are involved in 32% of incidents.

- **The use of a managed print service (MPS) leads to improved print security.** Overall 62% of organisations are using an MPS to gain access to print management and security skills which are often lacking in-house. This figure rises to 76% for print security leaders (as measured by Quocirca's index) compared with just 44% for the laggards.

- **Most organisations have conducted a print security assessment.** Overall, 70% have carried out an assessment, although only 18% have conducted these in-house. For the rest they are conducted by third parties such as MPS providers or managed security service providers (MSSP).

- **The use of print-specific security measures varies.** Overall, 51% have a formal print security policy, 48% apply regular firmware updates, 40% use pull printing, 37% use secure mobile printing and 36% third-party device testing.

quocirca

Scope and definitions

This paper examines the security challenges of operating an unmanaged and insecure print infrastructure. It draws on research carried out by Quocirca amongst 250 enterprises in the UK, France, Germany and the US in December 2018. Alongside the primary research, key vendors in the market participated to provide details of their security offerings.

The print security market is characterised broadly as follows:

- **Hardware vendors.** All the major vendors, including Canon, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, Sharp and Xerox offer comprehensive portfolios that include built-in hardware security features, access control software and third-party vendor agnostic pull-printing. Some vendors also offer security assessment services either independently or as part of their MPS offerings.
- **Third-party ISVs.** A range of ISVs offer secure print solutions including (but not limited to) Nuance, EveryonePrint, Papercut, Pharos, Print Audit, Ringdale and Y Soft.
- **Data loss prevention**. Although vendors in this space are not strictly operating in the print security market, Quocirca believes the capabilities they offer to printing documents based on content analysis offers a higher level of security.

The following vendors participated in this study:

- Hardware vendors: Brother, Canon, HP, Lexmark, Ricoh and Xerox.
- Third-party ISVs: EveryonePrint, Ringdale, Y Soft.

Each vendor was requested to complete a written submission detailing its strategy, capabilities and customer references to capture key facts and figures.

The following definitions are used through the course of this report:

- **MFP:** an MFP (multi-function printer, or sometimes product or peripheral), multifunctional, all-in-one (AIO), or multifunction device (MFD) combines print, copy, scan and fax functionality. MFPs offer advanced features such as scan-to-email, scan-to-network destinations and are often based on an embedded software platform. This allows software developers to build integrated solutions for MFP devices.
- **Pull Printing:** pull printing functionality allows a document to be released only upon user authentication using methods such as proximity/magnetic/smart cards or biometric recognition. Users submit jobs to designated pull-printing queues and jobs are moved from the pull-printing queue to the dedicated print queue. Requiring the user's presence at the printer in order to collect print jobs reduces print waste without imposing accounting limits.
- **Managed Print Service (MPS):** This is the outsourcing of the print infrastructure through a process of assessment, optimisation and ongoing management. MPS comes in many forms, from entry level packages that wrap hardware, service and supplies based on a cost-per-page contract to more sophisticated enterprise engagements that include document workflow, change and continuous management, based on stringent service level agreements.

The print security threat

The continuing digitisation of business processes may prompt expectations of the demise of paper and printing in the workplace. Such views are misplaced. Quocirca's research consistently shows that businesses remain dependent on print to support business activities. However, the way print is being used, managed and integrated into business processes is changing. Alongside this are growing concerns about the security threats that arise from continued reliance on printing. There are two broad areas of threats: those posed by the documents that print devices produce; and the vulnerability of the print infrastructure itself.

Paper output from printers often includes confidential documents, which can end up in the wrong hands at any point during their lifecycle, for example early on - if left in output trays, or later - if disposed of carelessly. Documents are also a privacy and compliance problem. Instances of documents being sent to the wrong recipient are all too common, especially in sectors like healthcare, where there is still plenty of paper correspondence. Documents destined for printing are also a risk before ink and paper ever meet, as most print devices contain local disk drives to store and queue output.

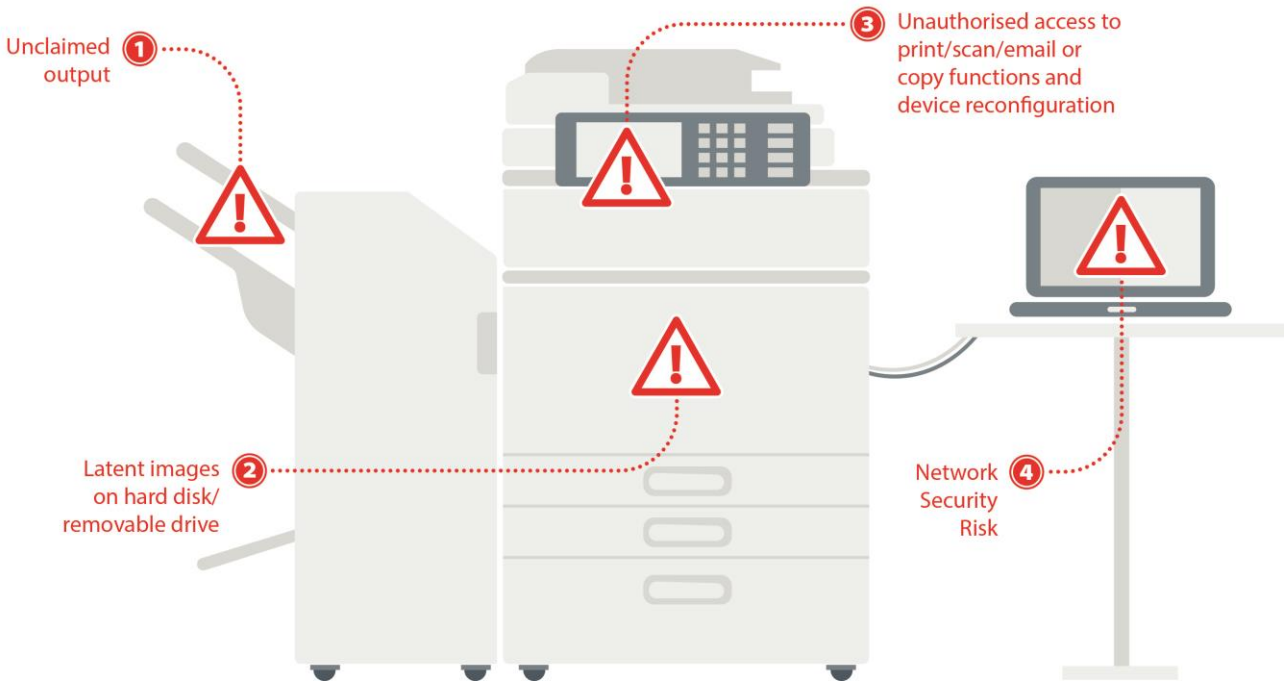
Although such stored output is one temptation for print infrastructure hackers, it is unlikely to be the primary target. The security threat from print devices is like that of any network-attached device, all of which are increasingly referred to as IoT (Internet of Things) devices. There are three main IoT related threats:

1. The device may be used as a network ingress point. In many cases printers may be poorly secured, firmware does not get updated and access credentials are easily compromised, for example because defaults are never changed or because access is shared between multiple administrators.
2. Second, sabotaging IoT devices may be an easy way to target and disrupt an organisation's business processes.
3. Thirdly, IoT devices, including printers, may be recruited to botnets which are then used to perpetrate distributed-denial-of-service (DDOS) and other attacks that can benefit from access to lots of *free* processing power.

Quocirca's Print Security 2019 market report reveals the key market trends impacting print security in today's ever-expanding threat landscape. It highlights the concerns and levels of confidence around print security and the ways these are being addressed. The report covers both European and US-based businesses ranging in size from 250 employees to many tens of thousands across a range of sectors (see appendix 1).

Print security vulnerabilities

Despite the move to digital communications, many businesses still rely on printing to support key business processes. MFPs are prevalent across businesses of all sizes and as such they are a critical network endpoint that must also be secured. Even behind a firewall, an MFP can be a front door to the network leading to the potential for compromising corporate or customer data.



MFP Security Vulnerabilities

The potential risks are illustrated in the diagram above. These include:

1. **Unclaimed output.** Confidential or sensitive information can be collected inadvertently or intentionally by an unauthorised recipient.
2. **Latent images on hard disk.** All documents whether they are printed, copied, scanned, faxed or stored are processed within the hard disk drive. This can present a risk not only if the device is hacked, but also at the end of life when potentially hard disk data could be recovered.
3. **Unauthorised access to MFP functions.** If MFP settings and controls are not secure, it is possible to alter and reroute print jobs, open saved copies of documents, or reset the printer to its factory defaults. Potential hackers could also attack print devices to either intercept or download copies of scanned-in documents, emails and user access credentials.
4. **Network security risk.** Jobs sent to the MFP for printing typically sit unprotected on the server queue. At this stage, the printing queue can be paused and files copied and the queue restarted. In the worst case, a user from the outside can obtain confidential information, or place malware on the device. Open network ports also present a security risk enabling the MFP to be hacked remotely via an internet connection. Printers can therefore be prime targets of denial-of-service (DoS) attacks. Further, if data transmitted to a printer is unencrypted, hackers are potentially able to access this data.

Print reliance provokes security concerns

Asked to consider the importance of print 91% of respondents indicated it is important today (2018). This only drops to 87% when asked to consider the position in two years' time (2020). There was some variation: 94% of public sector organisations believe print will still be important in 2020, whilst only 84% of industrial organisations say this will be the case; 93% of larger businesses agree, compared to 80% of smaller ones. In no country or sector did the figure drop below 80% either for today or in two years' time.

At one level businesses recognise the ongoing need for print, but at another they reveal concerns about the risks associated with this dependence on print. When asked to consider the risks that may lead to security problems and data breaches in general, the print infrastructure ranks second behind public cloud services (Figure 1), with 66% ranking it in their top five risks compared to 69% for the latter. In professional services, finance and retail, print is the top concern; this is also the case in France and the USA. Whatever the reality of the risks, the perception that print is a security problem has always needed to be addressed and this will remain the case. However, whilst most are aware of the risks associated with print infrastructure, there is plenty of scope for increasing the confidence that these risks can be mitigated.

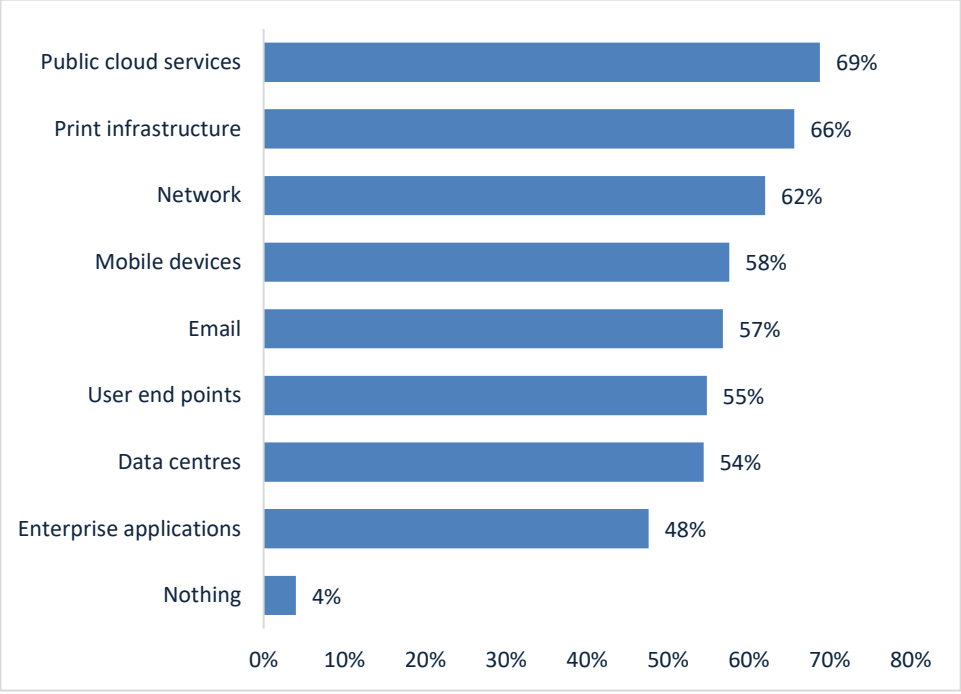


Figure 1: Rating of IT risks that may lead to security breaches (% ranking as a top 5 concern)

Print security – maturity, confidence, concern and spending

To assess the impact of effective print security, or a lack of it, it helps to have a measure of print security maturity. Quocirca has designed a print security maturity index for use in this report, the elements of which are defined in appendix 2. The index considers seven factors: the proportion of overall IT security spending that goes on print security; the use of print security assessments; the use of pull printing; having a formal print security policy; secure mobile printing; third party testing of printing devices and printer firmware updates.

Print security maturity index scores were classed as follows (all scores out of 10):

- **Print security leaders** – score of 8 or more – at the forefront of addressing print security issues, they are often big users of print and suffer the most print-related security incidents. Leaders recognise the threats and the need to mitigate them.
- **Print security followers** – score between 5 and 8 – may or may not be major print users, aware of the problems, but only partially addressing them.
- **Print security laggards** – score of 5 or less – in some cases low level users of print and consequently suffered fewer print-related incidents. However, many are just complacent, ignoring the threat from print and likely to suffer the consequences.

Print security maturity varies by country, sector and the size of an organisation (Figure 2). The US has the most leaders, France the most laggards. Retail, which relies on in-store printing and paper dispatch notes for online sales, has the most leaders, finance the least, perhaps because as a sector it has done more to move away from printed communications. Larger organisations lead over smaller ones in line with the expected ongoing importance of print.

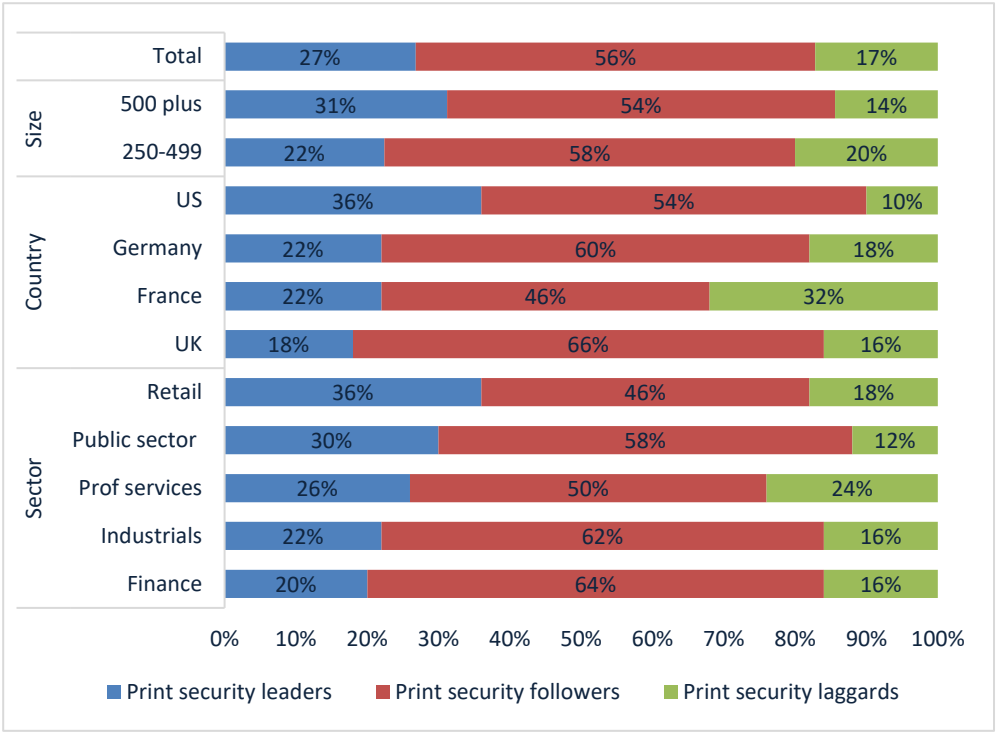


Figure 2: Quocirca's Print Security Maturity Index

Whether leaders or laggards, what print-related risks should organisations be protecting themselves against? Concern about the risk of security breaches and data leaks is high (Figure 3). 73% say they are concerned or very concerned. The figure drops to 46% in Germany and was highest in the US at 80%.

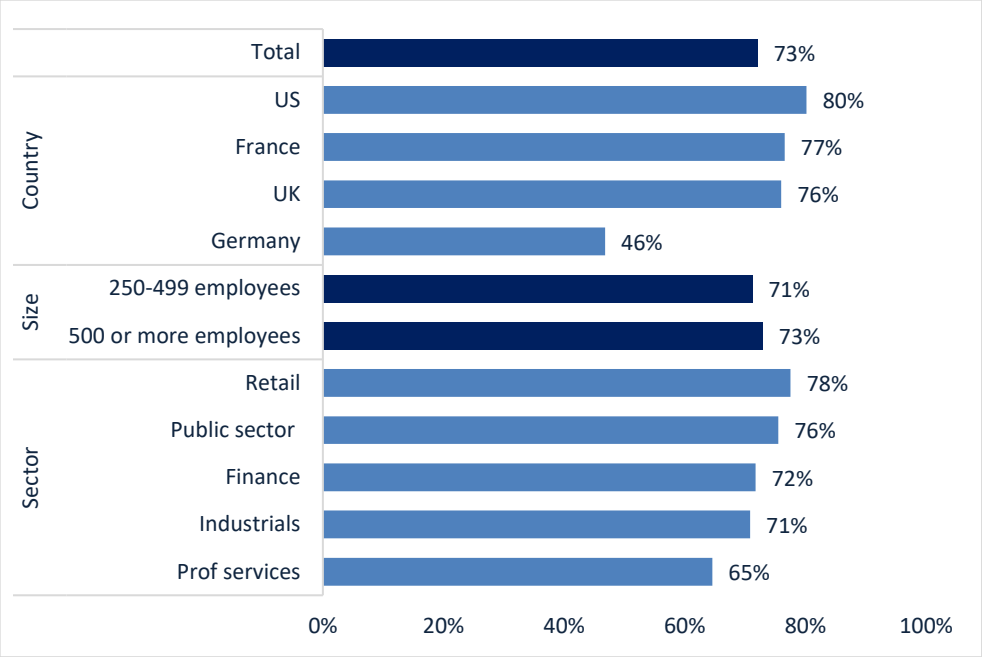


Figure 3: Concerns about the risk of print security-related data breaches (% concerned or very concerned)

Despite the concern, there is not much confidence that print infrastructure is protected against security breaches and data leaks. Overall just 24% feel highly confident whilst 33% have a low level of confidence (Figure 4). Confidence was highest in the US and lowest in Germany; highest in retail and lowest in professional services. That Germany was lowest with both confidence and concern, may just be indicative of conservative scoring by German respondents.

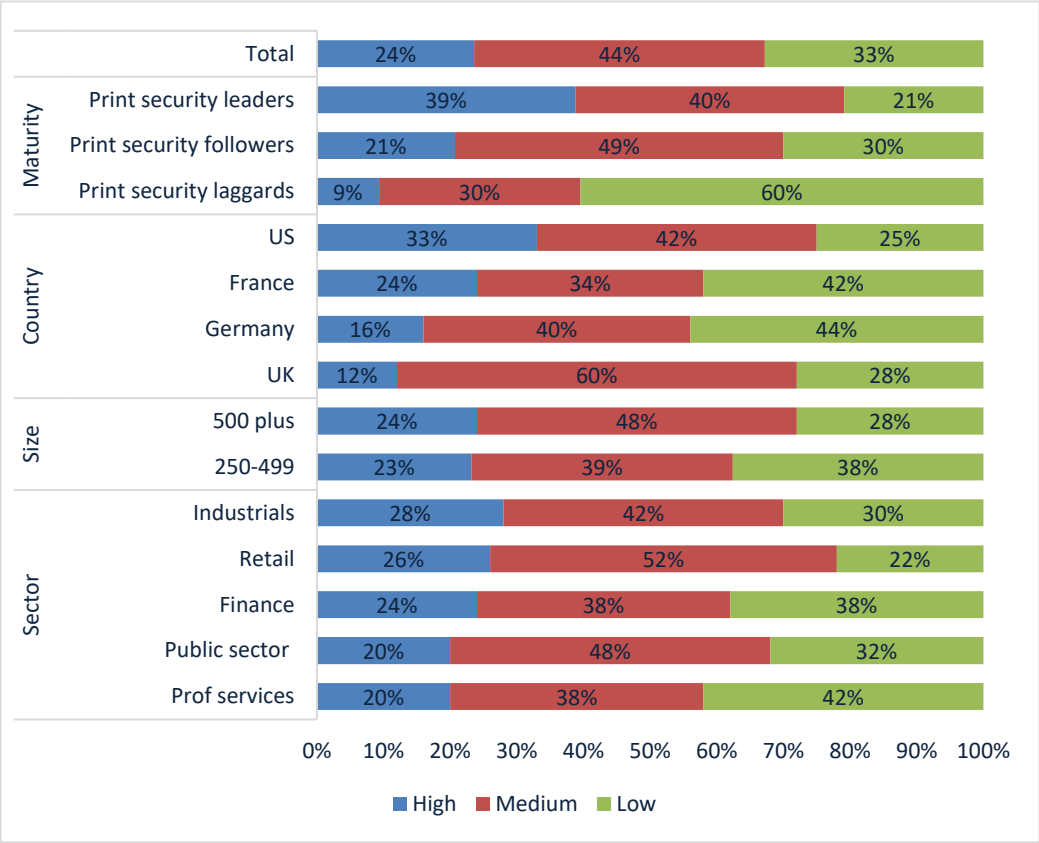


Figure 4: Print security confidence

One of the measures used to calculate the print security maturity index was the proportion of total IT security budget that was spent specifically on print security. The overall average is 11% (Figure 5). The figure is highest in the public sector (13%) and lowest in professional services (9%). Overall 77% say that absolute print security spend has increased in the last two years, the figure is consistent across most countries and sectors; only 6% say it has decreased (Figure 6).

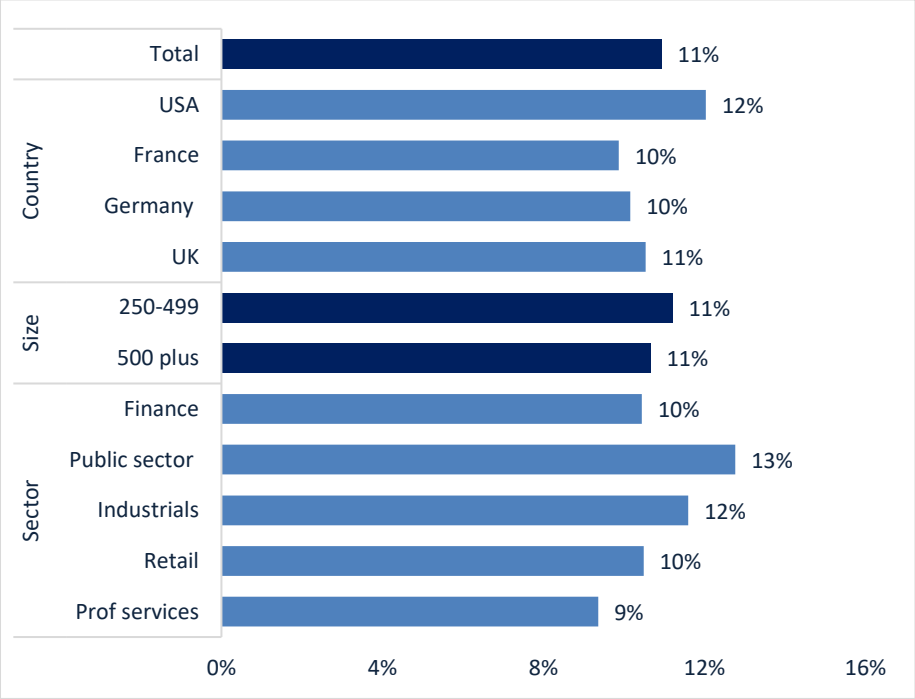


Figure 5: Annual print security spend as a % of IT security spending and print spending

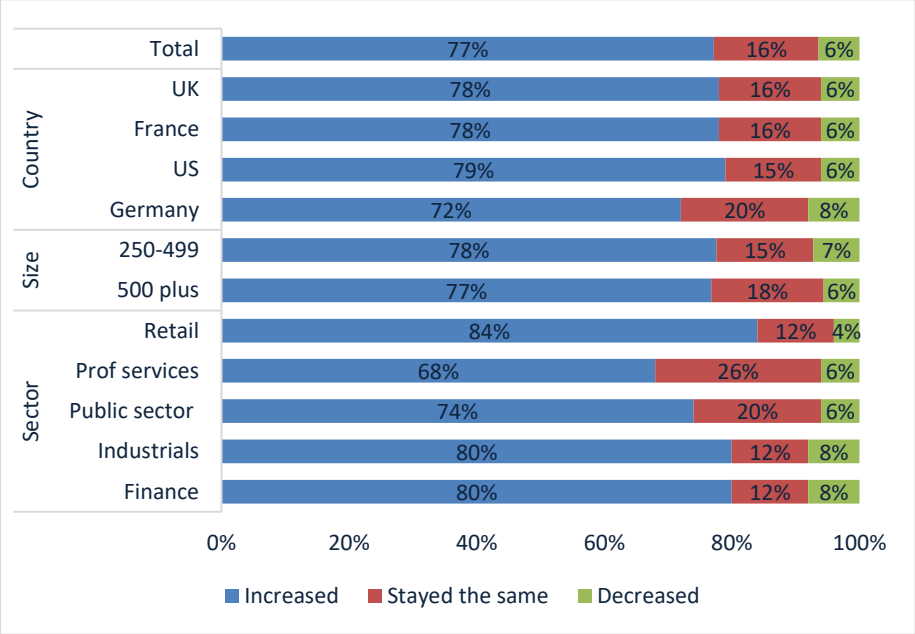


Figure 6: Change in print security spend over the last two years

Maturity, confidence, concern and spending are not just down to perception about the risks to print infrastructure, some of it is down to the incidents experienced and how well they have been dealt with.

Print-related security incidents, data losses and consequences

Print-related IT security incidents are frequent and costly. Overall respondents estimate that 11% of all IT security incidents in the last 12 months have been print-related. This might sound high, however many will have taken into consideration printed information falling into the wrong hands as well as attacks on printers themselves. For the average organisation this amounts to nine incidents during the previous year. Both figures are highest in the USA (14% and 11 incidents) and in finance (15% and 11.5 incidents). In finance, this may be related to the sector's magnetism for attackers viz. it suffers the most attacks overall and therefore the most on printers.

Print security maturity itself does not reduce the number of attacks on print (Figure 7). The most mature suffer the greatest number of incidents. So, print security maturity is more likely to be a response to the threat - an organisation more reliant on print takes security of the print environment more seriously. There are, of course, plenty of exceptions. Just because an organisation is more targeted and suffers more incidents, it does not mean it suffers more severe consequences, if it is mature enough to deal with them.

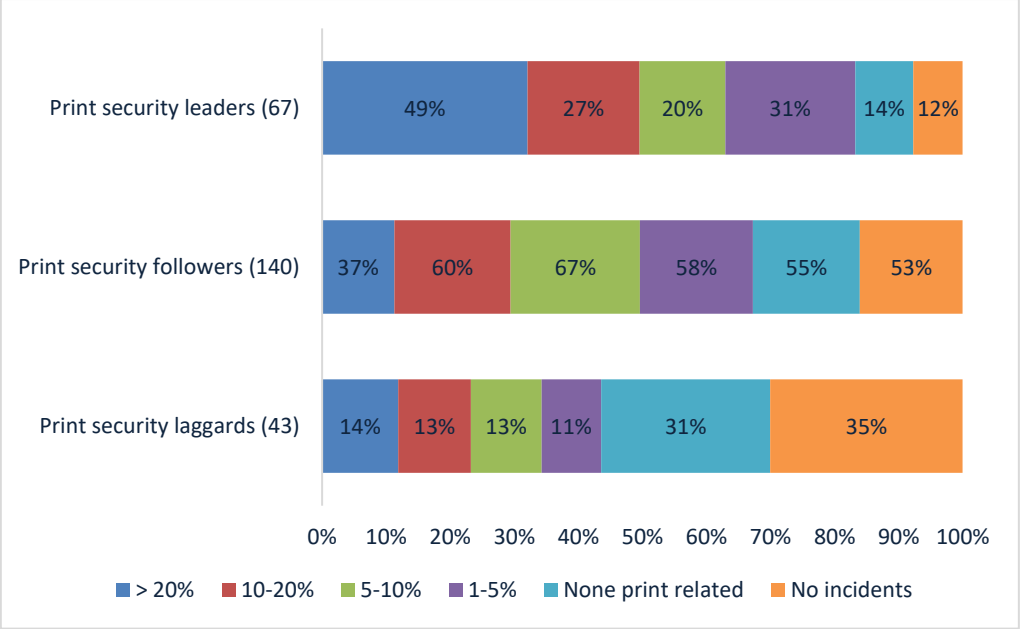


Figure 7: Print security incidents as a proportion of total security incidents by print security maturity

Overall, 59% say that in the past 12 months at least one print-related security incident has led to a data loss, rising to 70% in retail, 66% in finance and 64% in the USA (Figure 8).

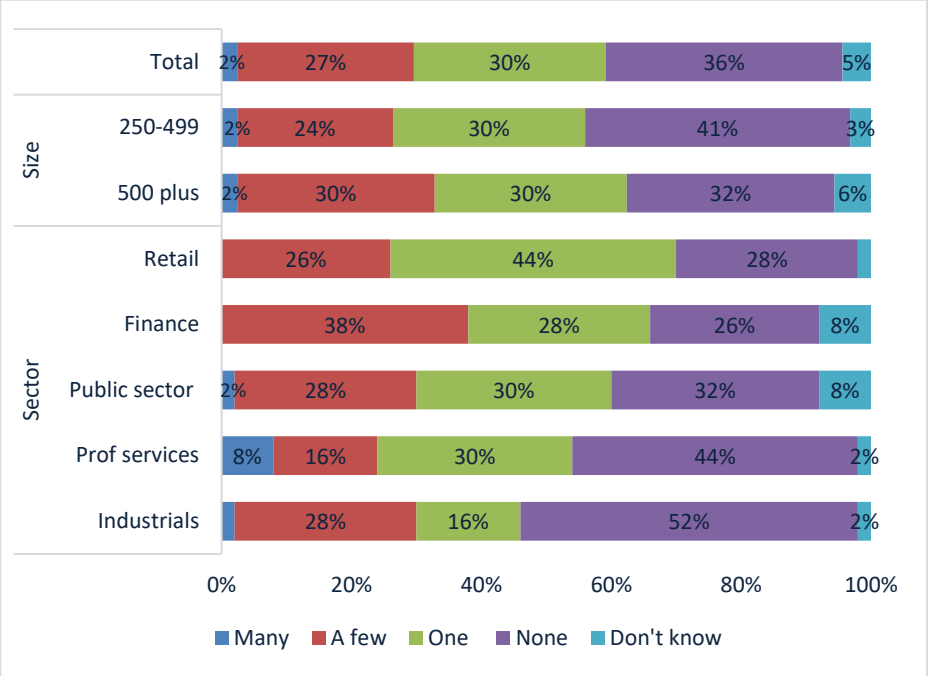


Figure 8: Print-related data loss incidents the past 12 months

Retail has had a lot of well-publicised breaches of customer data in recent years. Dealing with these data losses is estimated to cost an average £313,000 per annum (Figure 9). This is higher in more regulated Europe (£400,753) than in the USA (£199,805).

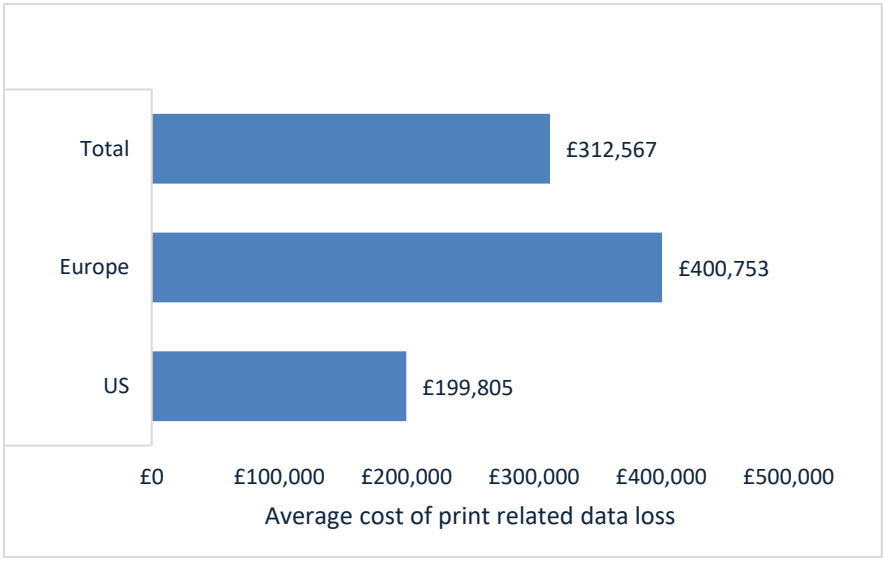


Figure 9: Average cost of a print related data loss (sample size = 148 organisations that suffered a data loss)

The consequences are not just financial, but also include lost productivity, lost business and revenue (Figure 10). Business-critical processes, such as loan applications and those still using paper documents which need signatures, all rely on printing and can be impacted by print security incidents. Processes may have to be temporarily stopped if a data breach has occurred or the process has been sabotaged. On average it is reported to take 4.4 days to recover from an incident, the figure is highest in finance (5.8) days, which has the most print-related data incidents and losses to deal with.

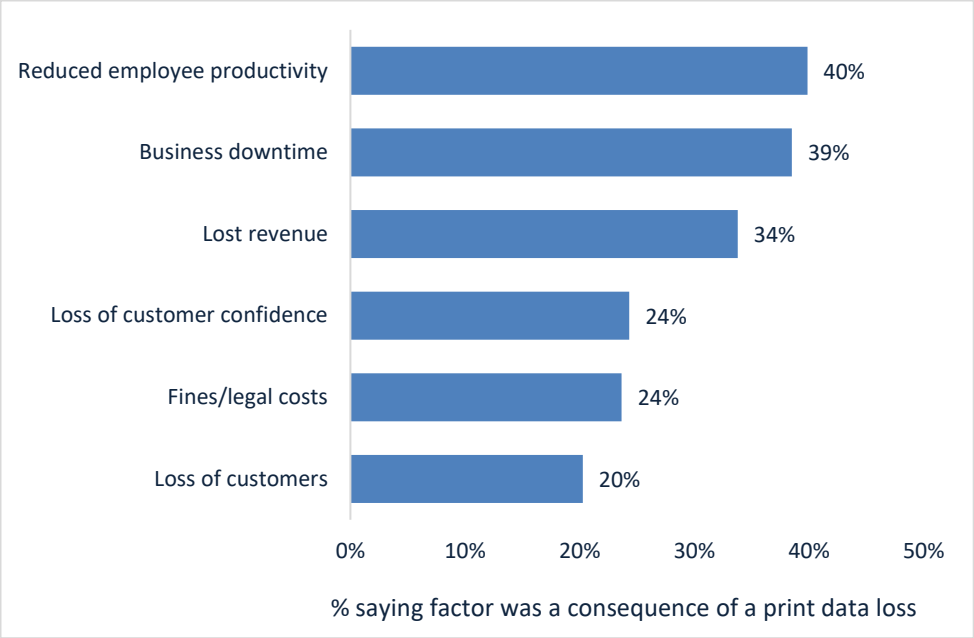


Figure 10: Consequences of print-related data losses

Overall 24% of respondents say there have been fines and legal costs associated with data leaks. Not all such incidents attract the attention of regulators, but there is concern that they could.

Across the board there is one regulation which is being taken into consideration more than any other – the EU General Data Protection Regulation (GDPR). 40% take GDPR into account when planning print investments. This is even higher than average in the USA (42%), where many multinationals rely on European trade. Additionally, many expect GDPR to be a harbinger for more stringent data protection regulations worldwide.

Only in France is another regulation, the Institute of Electrical and Electronics Engineers security regulation IEEE 2600, considered more often (by 30%) than GDPR (just 20%) when making print investments.

Print security concerns, action and budget constraints

Effective print security requires an understanding of where the risks lie and how best to mitigate them. Asked about the perception of risk 70% worry about malware being implanted on print devices, making it the top concern by some way (Figure 11). This is followed by the related issues of hacks via printers and the compromise of printer access credentials, both selected by 60%. Perceived risks are less about printed information itself and more about print devices.

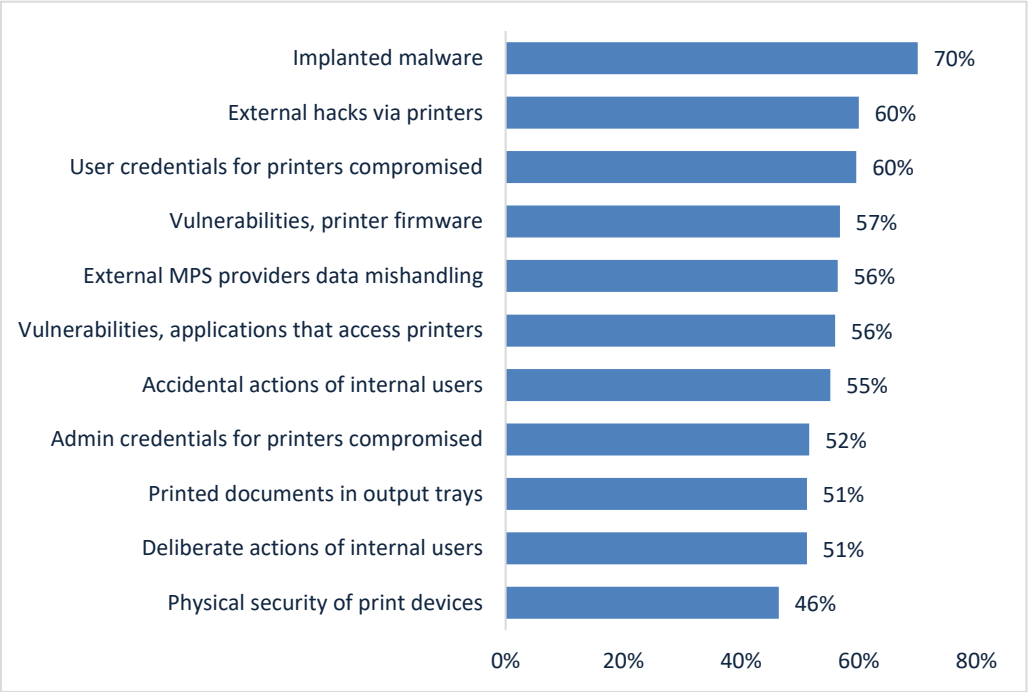


Figure 11: Concern with factors that may cause a print security incident (fairly or very concerned)

In the UK 70% worry about the accidental actions of internal users, just behind malware at 74%. When it comes to print, sending confidential output to printers in shared spaces or passing printed documents to the wrong recipients are the most likely errors.

UK respondents are right to worry; for those that have had incidents, when asked to state the actual factors involved, internal user accidents top the list by some margin (Figure 12), thought to be involved in 32% of incidents. The perceptions of risk and the reality do not align, potentially leading to too much focus on some risks and too little on others when it comes to taking protective measures.

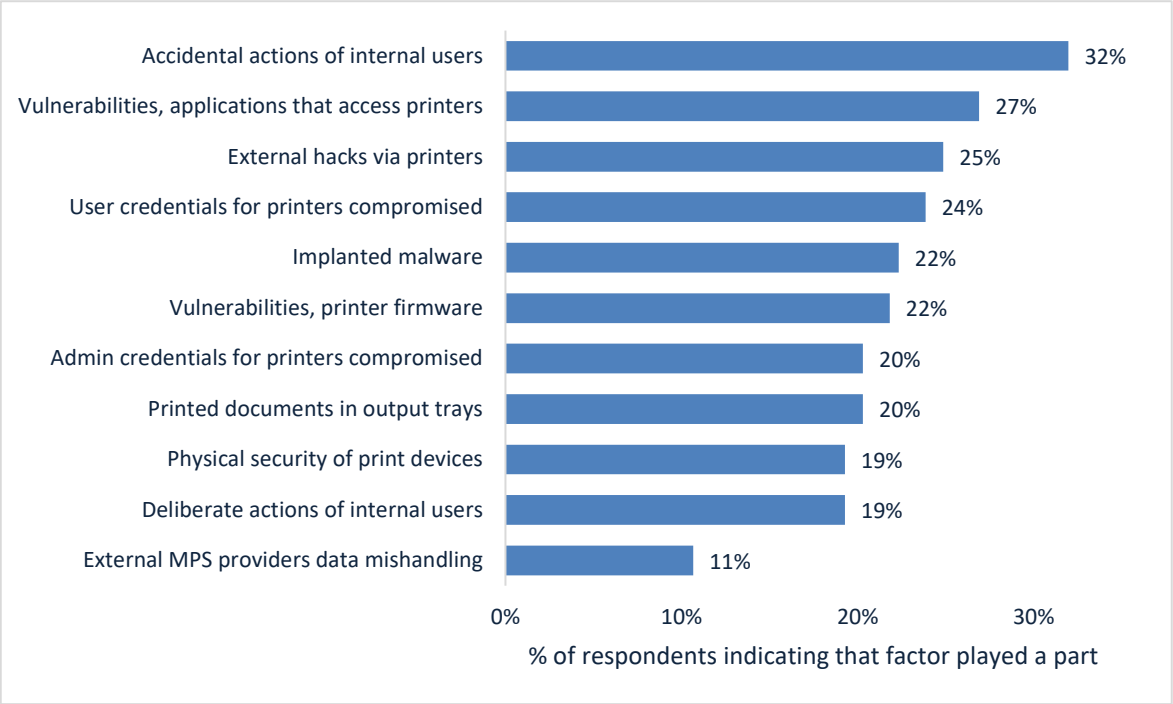


Figure 12. Factors that have played a part in actual security incidents

Whether it is perceived concerns, or the factors involved in actual incidents, the most cited factor inhibiting effective print security is budget constraints (Figure 13). However, whilst it tops the list, only 31% selected it and there are plenty of other reasons holding organisations back. These include poor integration of tools and a lack of internal skills. Internal skills might be further up the list, but for many it is less of a concern as they source such skills from third parties.

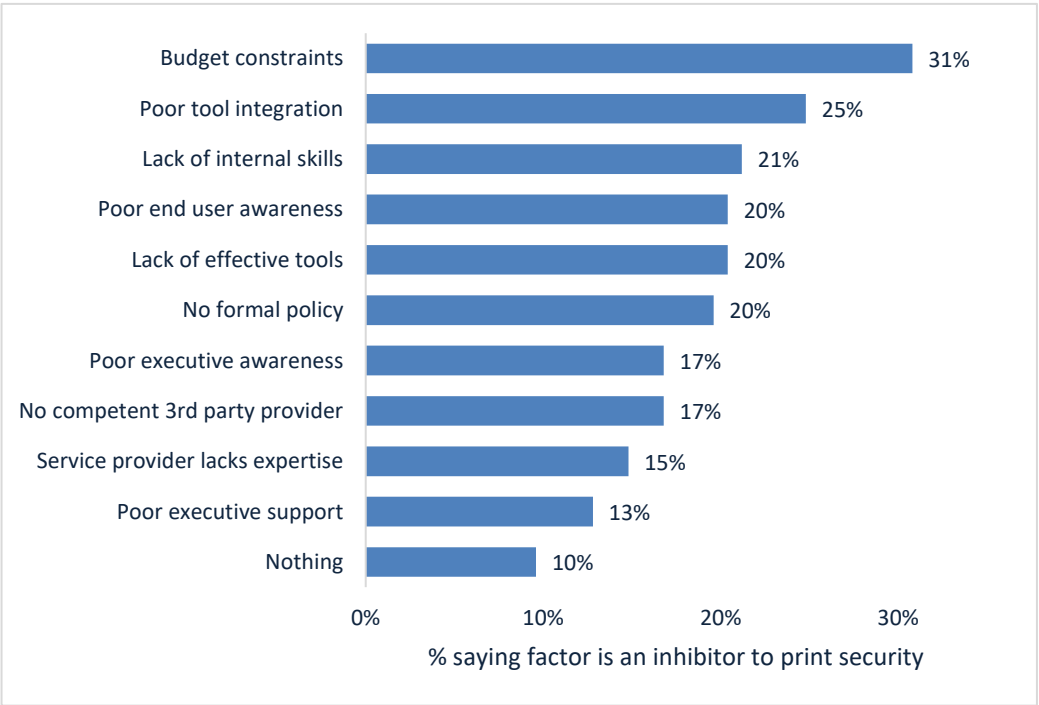


Figure 13. Inhibitors to effective print security

MPS, security assessments and other measures

62% of organisations are now working with managed print service (MPS) providers to manage print requirements in general (Figure 14). However, this figure rises to 76% for print security leaders, whilst it is just 44% for laggards. Whilst it is possible to work with an MPS provider simply to manage print costs and peripherals, increasingly they are also delivering value-added services such as print security.

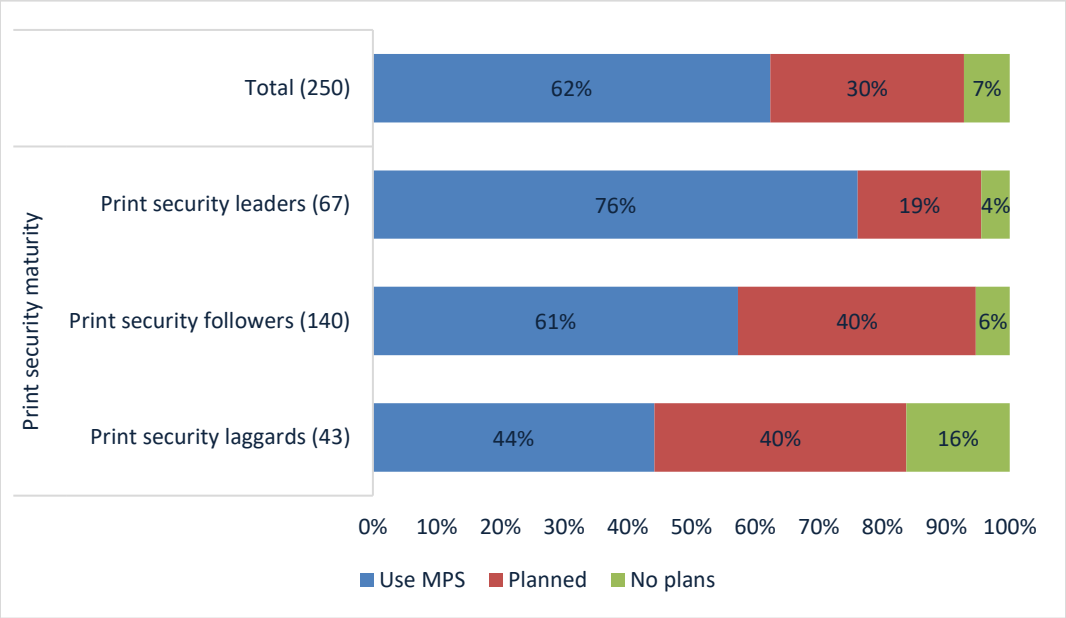


Figure 14: MPS adoption and print security maturity

That said, whilst the benefits of MPS seem widely accepted, 56% of MPS users worry about the security of the data collected by their providers. This is in line with general concerns about external service providers, so MPS providers should redouble efforts to communicate how safe their data handling is and turn security into a selling point. In reality, only 11% say an MPS provider mishandling data has been a factor in a real-world incident (see Figure 12), the least cited of any factor.

Print security assessments form the foundations of any print security plan and most MPS providers offer this service. The existence or absence of assessments is an element of Quocirca's print security maturity index. 70% of organisations currently carry out print security assessments, however, for more than half of these (38%) this is a recent activity started within the last 12 months (Figure 15).

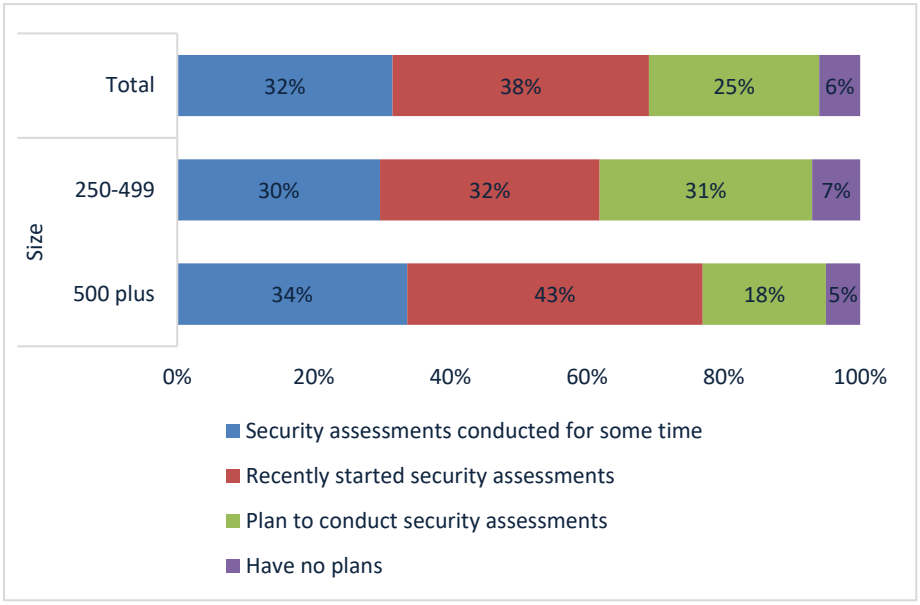


Figure 15: Print security assessment usage

These assessments work. Those who have been carrying them out for some time have a higher confidence in print security than others, those not doing them the lowest confidence (Figure 16). Most assessments are carried out by third parties, either as part of an MPS service or as a specific activity via another service provider or managed security service provider (MSSP). Only 18% say assessments are carried out in house, a figure which rises highest, to 28%, in the public sector. Protecting against security threats is the most widely cited reason for carrying out assessments, selected by 47%, next on the list is meeting print security standards at 35%, regulatory compliance comes in at fifth, selected by 28%.

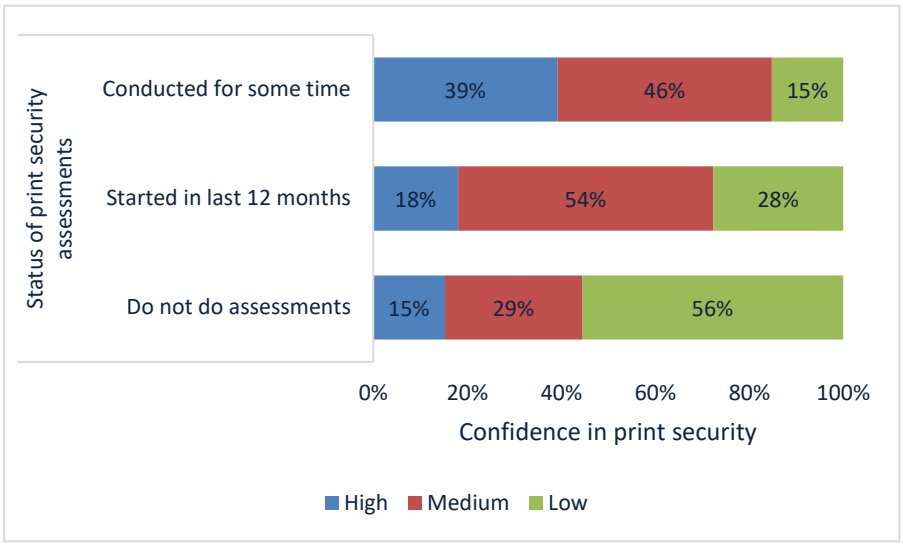


Figure 16: Print security assessment impact on print security confidence

Whoever carries out assessments, guidance should be forthcoming for improving print security. There are five print-specific measures that are recommended, and which could be used more widely (Figure 17). Having any one of these in place increases an organisation's score on Quocirca's print security maturity index. Most likely to be in place was a formal print security policy (51%), followed by 48% applying regular firmware updates to printers, 40% using pull printing (which avoids documents being left in output trays), 37% using secure mobile printing and 36% taking advantage of third-party printer device security testing.

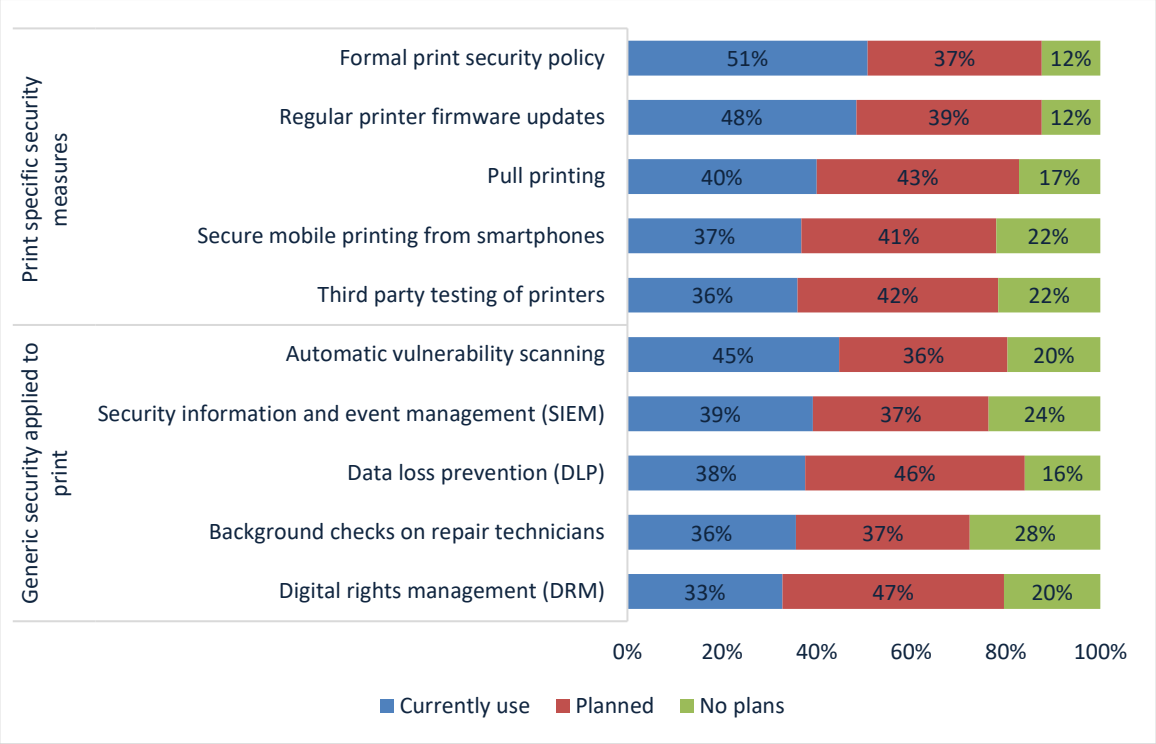


Figure 17: Adoption of print security measures

There are also several more generic security tools that can benefit the security of the print environment, such as security information and event management (SIEM), data loss prevention (DLP) and digital rights management (DRM), which are used by 39%, 38% and 33% of organisations respectively. For those using any of these measures, print specific or generic, the level of satisfaction is high, all scoring more than 4 out of 5.

Future outlook

Print security needs to be a strategic board-level issue, moving beyond the domain of the IT manager to the CISO and CIO. The continued high level of print-related data breaches demonstrates that businesses need to do more to protect their devices, network and data. An organisation's information security strategy can only be as strong as its weakest link. The expanding IoT security threat landscape means that the challenge of print security is moving beyond protecting the printed page. As IoT devices, smart MFPs are susceptible to the growing threat of DDoS attacks as well as providing an open gateway to the corporate network.

The threat to the print environment can be mitigated, but only a minority of organisations are currently succeeding. Those that are doing best, achieving the highest print security maturity scores, are some of the most prolific users of print. However, the threats exist for all organisations and print security laggards and followers can learn from the leaders.

Manufacturers must embed security into the architecture and interfaces of their products, in order to protect the lifecycle of devices, from inception to retirement. This means future proofing devices as they become more powerful, store more data and increase in functionality. MFPs should have the ability to run security updates automatically, validate new software and lock features where appropriate.

Devices should have the intelligence to identify a security event and communicate such events and remediate as appropriate. This means that print management functionality must be integrated in broader IT security management tools to provide remote warning notifications for errors or unusual activity.

Ultimately, print security demands a comprehensive approach that includes education, policy and technology. In today's compliance-driven environment, where the cost of a single data breach can run into millions, organisations must proactively embrace this challenge. By using the appropriate level of security for their business needs, an organisation can ensure that its most valuable asset – corporate and customer data – is protected. Managed Print Service providers are well positioned to provide the support and guidance needed. There is no room for complacency, given the far-reaching repercussions – legal, financial and reputational - of print related data losses.

Recommendations for IT decision makers

With businesses continuing to remain reliant on print for the foreseeable future, effective print security that forms an intrinsic part of an overall IT security plan enables the safe deployment of print infrastructure which addresses business objectives while protecting its assets. Print security needs to be firmly on the board agenda, with the risks understood by the CIO as well as the CISO.
Business leaders should consider the following when building a print security strategy:

1. A complete security ecosystem
Given networked MFPs and printers are as connected as any other IT endpoint, and not only process confidential and sensitive information but also generate this as output, print security must be treated as a fundamental element of the broader security strategy. There are multiple layers to print security – encompassing the device, network and the documents/information they produce. This demands a comprehensive risk assessment.

2. Conduct a comprehensive security assessment
The first step is to evaluate the existing fleet to discover potential security vulnerabilities, particularly when a mix of legacy and new devices have been deployed. Such insights provide organisations with visibility into their print environment and can set a foundation for ongoing monitoring of devices once the fleet is optimised and secured. Security assessments can vary widely from basic discovery to full assessments and are offered by most MPS providers.

3. Print security starts with procurement
Devices must be procured with security and remote management in mind. For the most effective control, devices should be based on common interfaces and standardised management tools. Evaluate devices that have built-in security such as intrusion detection, white-listing and syslog data collection with links to established SIEM tools.

4. Strengthen the processes for access credentials and vulnerability management
One key security challenge is the ability to easily upgrade firmware and patch devices as soon as vulnerability is publicised. Older devices that are not patchable are a particular security risk. Consider automating the deployment of firmware updates.

Access credentials are a weak point for print devices, for example default admin accounts are often left in place. Once installed, default passwords should be changed to unique, complex, strong passwords, as advised by the National Institute of Standards and Technology.

5. Protect sensitive or private jobs while in motion
End-to-end encryption of network traffic ensures secure transfer of print jobs to printers, however, as most printers cache content, locally stored data should also be encrypted. Many regulations require this, for example PCI DSS.

6. Continuously monitor the print environment and make use of analytics
Knowing the current status of devices provides a secure view of the entire print environment. Consider using network monitoring and alerting tools such as ICMP, SNP and Syslog to regularly track devices and fix issues. MFPs generate a wealth of data, for example on authentication and usage. This can be used to identify potential security events and enable fast responses to attacks. If using an MPS provider check if it offers regular compliance reports, which should include data breach monitoring and reporting.

7. User education and training
With many data loss incidents being caused unintentionally by internal users (32% of print security incidents involved the accidental actions of users in the current survey), it is vital that businesses have security training in place to educate employees on the importance of protecting sensitive information and raise awareness of relevant malicious threats. All organisations must better educate and train end users on the potential security risks associated with printing, many MPS providers will offer help with training needs.

Vendor profile: Brother

Quocirca opinion

In a climate where the threat landscape continues to evolve and become more diverse, Brother believes that security is the highest priority for organisations concerning their print environment. It strives to continuously strengthen its capabilities in this area, researching new enhancements to products and services, and dedicating engineering resource to develop appropriate responses to evolving security threats.

Security considerations are integral to Brother's product, MPS and solutions offering. It also considers a wider security approach and recommends customers' security strategies should include elements such as NAC (Network Access Control) technology for controlling access to the network by devices and users. While Brother does not offer its own NAC solution, it does work with NAC vendors to ensure clients' network environments are secure. Brother ensures European GDPR considerations are at the centre of its Cloud Computing and MPS strategy. Each MPS agreement can be tailored to fit the needs of the customer, and Brother Partners can offer additional services to be included in order to create a unique proposition.

Brother supports industry-standard communications protocols and encryption. TLS/SSL (Transport Layer Security/Secure Socket Layer) encryption, the same encryption used in e-commerce to protect bank and credit card details, is in-built into its hardware, enabling documents to be encrypted at up to 256-bit during transmission over the network. Moreover, Brother devices can connect directly to internal or external secure environments using built-in IPsec support; communicate with network resources using SMB v3 (Server Message Block); can be managed via encrypted SNMP v3 (Simple Network Management Protocol) even during remote set-up and routine maintenance; and conform to the high security standards determined by IEEE 802.1x, whether hardwired with a cable or via an organisation's wireless infrastructure.

Other security features include the ability to enable or disable individual communication protocols at a granular level, which reduces the potential attack surface while still allowing users to perform fundamental tasks. Administrator passwords are encrypted and the configuration interface times-out after a period of inactivity.

Considering that, to all intents and purposes, printers and scanners are IoT devices even though they run standard TCP/IP services, Brother also has features which help to securely protect data communications, including IP Filtering which prevents access to the device over the network, and Protocol Control, a feature that allows administrators to enable or disable individual communication protocols at a granular level, which reduces the potential attack surface while still allowing users to perform fundamental tasks. Brother also routinely implements a more secure version of an existing standard protocol; for example, the SMB protocol is often used as a way of disseminating ransomware attacks, yet the most recent version of SMB (v3) is not vulnerable in this way, and therefore has been implemented in its devices.

Brother printers include several features to securely protect devices by taking automated action. This includes automatic intrusion detection, where a device automatically reboots if it senses threats, ensuring the integrity of the device and the wider print environment. Temporary print data is protected and encrypted in the device using a proprietary algorithm. Device firmware is also digitally signed and checked before update to prevent malicious code being uploaded to the device.

Dependent on the model, other hardware-centric security functions include Setting Lock, which restricts access to the device's settings through its control panel and Secure Function Lock, which prevents access to both the device's settings and certain functions. This allows administrators to decide who can do what with each machine, for instance controlling which users are able to fax and scan, or imposing monthly limits, through unique PIN numbers, NFC access cards or Active Directory/LDAP integration. Solutions are also available to secure the paper input tray, ideal for use in environments where access to pre-printed security paper, such as checks and prescriptions, must be strictly controlled to prevent theft or unauthorised use.

Due to the risk associated with internal persistent storage, Brother doesn't offer hard disks as an option for its SMB range of printers, and upon power-off, printers do not retain any document data in memory.

Product overview

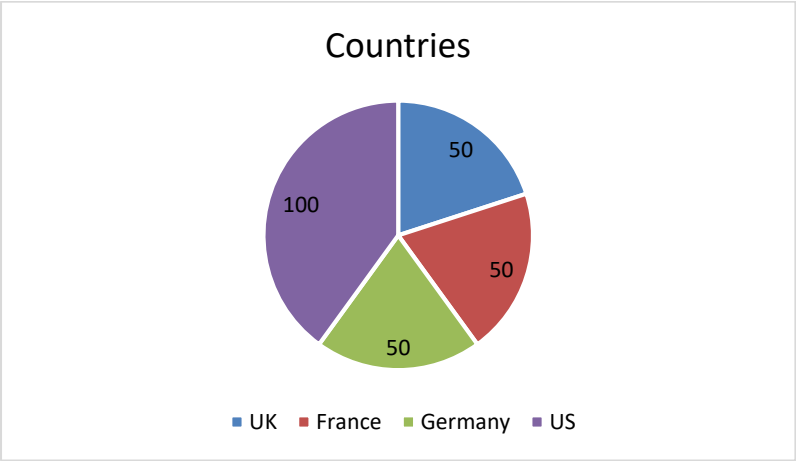
Brother offers a range of proprietary tools and utilities that can monitor usage and audit printing practices, and supports third-party solutions including Nuance, Papercut, Ringdale and One Q among others, to enable customers to protect data and create a secure print environment.

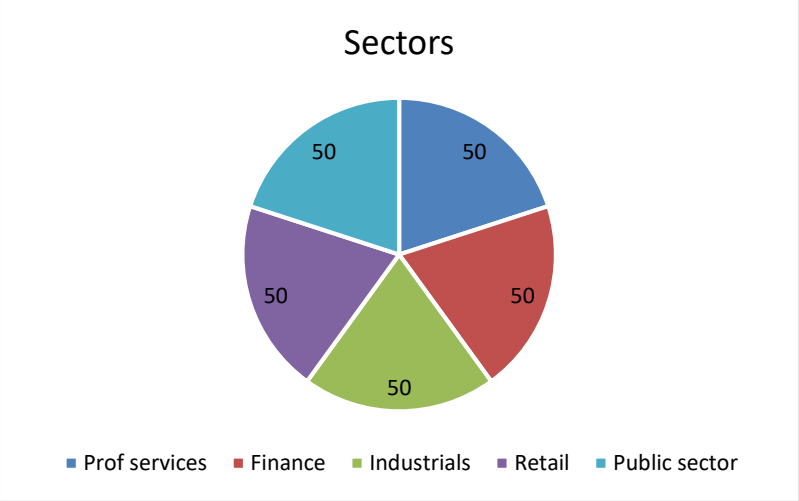
Key features include:

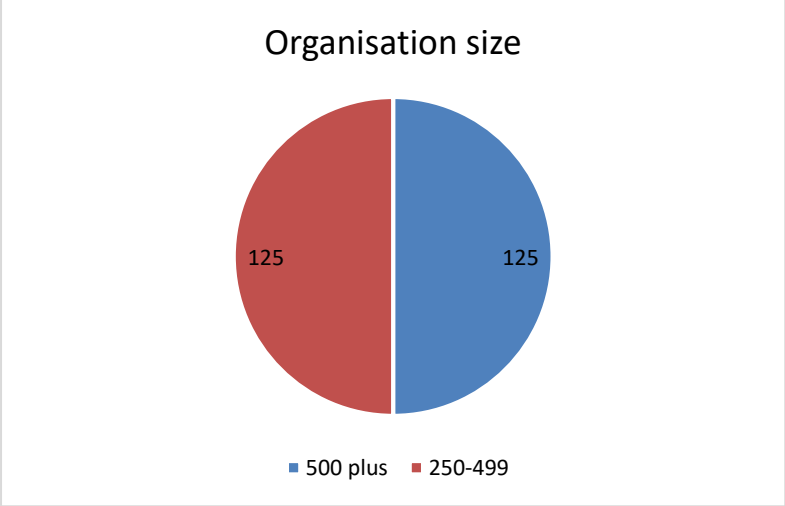
- **PrintSmart Secure Pro.** Users can collect documents from any printer that is connected to the PrintSmart Secure Pro server using a PIN or, where supported, NFC Card authentication.
- **Mass Deployment Tool.** Provides a configuration interface to enable a variety of device settings to be managed. It allows users to install and manage multiple local or network connected devices quickly and easily, without having to install additional software.
- **Meter Read Tool.** Communicates with Brother USB or network-connected devices and reports on device status. It collects usage information and can notify of any machine errors or if consumables are running low.
- **BRAdmin Professional.** Allows system administrators to view and control the status of Brother network-connected products (as well as most other SNMP-compliant network printing devices) from a Windows computer on the same network.
- **Secure Print.** Allows users to delay printing until they are physically in front of the printer, by configuring an optional PIN for that user. When printing a confidential document, the user simply assigns the PIN number to that job in the print driver, which is then required to unlock the device for printing.
- **Secure Print+.** Works much in the same way as Secure Print except an optional NFC access card is configured, users then assign the NFC access card to a job in the print driver which unlocks the printer.
- **Secure PDF.** Brother's single and multifunction scanners enable scanned documents to be turned into a four-digit PIN-protected secure PDF.
- **Scan to Secure File Transfer Protocol (SFTP).** This establishes a private and safe data stream, and by controlling access to SFTP servers, organisations can help keep their whole network secure.
- **Watermark print.** Watermarked documents ensure that the origin of every page of a printed document is carried through any copies subsequently made.
- **Print identification**. The date and time, login user name or other personal identification may be added to the header or footer of each printed page independently from the document being printed.

Appendix 1 – Demographics

Breakdown of sample showing actual respondent numbers







Appendix 2 – Print security maturity index

The print security maturity index has a maximum value of 35, but this is recast as a score out of 10 in the report. The index indicates how advanced a given organisation is with its print security planning and deployment. The index is based on seven factors, each given a weighting in the index as indicated below.

Annual print security spending as a proportion of overall security spending (weight = 25%)

- More than 20% = 5
- 15-20% = 5
- 10-15% = 4
- 6-10% = 3
- 4-6% = 2
- 2-4% = 1
- 1-2% = 1
- 0% - none = 0
- Don’t know = 0

Whether print security assessments are carried out (weight = 25%)

- We have carried out assessments for more than 12 months = 5
- We have started to carry assessments within the last 12 months = 4
- We plan to start assessments in the next 12 months = 3
- We plan to start assessments, but not within the next 12 months = 2
- We should do assessments, but have no plans = 1
- We do not carry out assessments and see no value in them = 0
- Don't know = 0

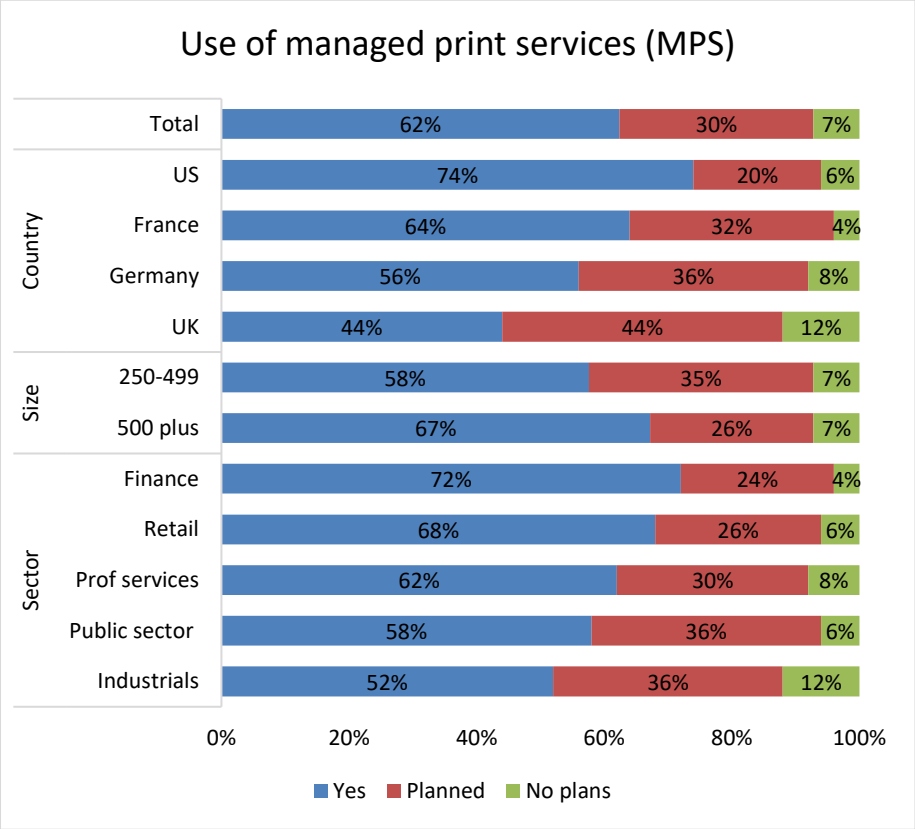
Whether five print security-specific capabilities are in place

- Pull printing (weight = 10%)
- A formal print security policy stating how print security should be ensured and the policy enforced (weight = 10%)
- Secure mobile printing from smartphones (weight = 10%)
- Third party testing for printing devices (weight = 10%)
- Firmware updates (weight = 10%)

For each print security capability

- Currently use = 5
- Plan to use in next 12 months = 3
- Plan to use beyond 12 months = 2
- No plans to use = 0
- Don’t know = 0

Appendix 3 – Use of Managed Print Services



About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With worldwide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

For more information, visit www.quocirca.com.

quocirca

Disclaimer:

This report has been written independently by Quocirca. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data and advice.