The Print Security Landscape, 2022

Securing the remote and hybrid workforce

Report Excerpt: HP Inc.

January 2022

QUOCIRCA

Executive summary

Quocirca's Global Print Security Landscape 2022 report reveals that many organisations are struggling to keep up with print security demands in today's hybrid work environment. Home printing is creating new security concerns, exacerbated by shadow purchasing of devices. SMBs and mid-size organisations are finding it harder to keep up with print security challenges leading to a higher incidence of print-related data loss. This is leading to a lower confidence, particularly among SMBs, in the security of their print infrastructure. However, in Quocirca's Print Security Maturity Index, those organisations classed as leaders that have implemented a range of technology and policy measures are seeing lower levels of data loss and have higher confidence in the security of their print infrastructure. Print manufacturers and channel partners must strengthen their security propositions for organisations of all sizes to help customers mitigate risk in the new era of hybrid work.

The study is based on the views of 531 IT Decision Makers (ITDMs) in the US and Europe. 23% of the respondents were from SMBs (250 to 499 employees), 29% from mid-size organisations (500 to 999 employees) and 47% from large enterprises (1,000+ employees).

The following vendors participated in this study:

Manufacturers: Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, Xerox
ISVs: EveryonePrint, Kofax, MPS Monitor, MyQ, PaperCut, Ringdale

Key findings

- **Remote working is here to stay and is creating an expanded threat landscape.** Pre-pandemic approaches to securing the print environment focused around a primarily static, office-based workforce now need to move to supporting workers who spend some time in the office, and some in the home environment. On average, 44% of employees are expected to work remotely as offices fully reopen. Hybrid work creates significant security challenges for IT teams to manage as the exploitable attack surface increases. The proliferation of shadow IT and unsecured home networks means that organisations need to rethink their security posture around the print environment.
- **IT security remains the top investment priority over the next 12 months.** 53% of respondents say it is one of their highest three priorities. MPS (managed print services) are second in importance (41%) followed by managed IT services (38%) and cloud services (35%). 70% of organisations expect to increase their print security spend over the next 12 months, with only 11% expecting a decrease.
- **A reliance on printing creates a need for effective print security.** Despite rapid digitisation over the course of the pandemic, many organisations remain reliant on printing. Printing will remain critical or very important for 64% of organisations in the next 12 months. 44% anticipate that office print volumes will increase, and 41% that home print volumes will do likewise. Printers and networked MFPs pose a security risk not only in terms of printed documents being accessed by unauthorised users, but also as an ingress point to the network if left unprotected.
- **Just a quarter (26%) feel completely confident that their print infrastructure will be secure when offices fully reopen.** Organisations are struggling to keep up with print security demands: more than half (53%) say it has become considerably or somewhat harder to do so. 67% of respondents are concerned about the security risks of home printing, compared to 57% who are concerned about office print security.
- **Print security is lower on the security agenda than other elements of the IT infrastructure.** Top security risks are considered to be cloud or hybrid application platforms, email, public networks and traditional endpoints. Employee-owned home printers come in as the 5th top security risk (24%) ahead of the office print environment (21%). This suggests both a lack of awareness and complacency in not

fully appreciating the security vulnerabilities around printing, which remains an integral endpoint in the IT environment.

- **There are marked differences between MPS users and non-MPS users.** Organisations that use an MPS provider foresee much greater growth in print volumes and are most confident in the security of their print environment – despite having a higher awareness of the risks. They are also twice as likely to state that keeping up with print security challenges has become somewhat or a lot easier. The visibility and control provided by an MPS appears to ease the security burden for users, increase assurance that they can ramp up print volumes if needed, and reduce complacency, therefore lowering the likelihood of being blindsided by a security incident.

- **In the past 12 months, over two thirds (68%) of organisations have experienced data losses due to unsecure printing practices.** This has led to a mean cost per data breach of £631,915. Such quantified financial losses are bad enough for organisations to manage, but they also state many other negative impacts, such as a loss of business continuity and ongoing business disruption after the breach. Customer loss is reported to be the biggest impact for SMBs. Large organisations are less likely to have suffered a print-related data loss, with 36% reporting no breaches compared to 24% of SMBs. The public sector is the most affected vertical. Vulnerabilities around home printers were cited as the top reasons for data loss – such as home workers not disposing of confidential information securely, and interception of documents stored in the home printer environment.

- **Quocirca's Print Security Maturity Index reveals that only 18% of the organisations can be classed as Print Security Leaders**, meaning they have implemented six or more security measures. The number of leaders rises to 22% in the US and falls to 12% in France, which also has the highest number of laggards (37%). Print Security Leaders are likely to spend a higher amount on print security, experience fewer data losses, and report higher levels of confidence in the security of their print environment. When compared by vertical, finance has the largest percentage of leaders (23%).

- **Less than a third (28%) of ITDMs are very satisfied with their print supplier's security capabilities.** This drops to 20% in the public sector. US organisations are most satisfied, with those in Germany least happy. ITDMs who use an MPS have far higher satisfaction levels (42% are very satisfied) than those who don't (20%).

- **Most ITDMs turn to managed security service providers (MSSPs) for print security advice.** MSSPs are the primary source of security guidance for 35% of organisations overall, rising to 40% in the US. Just 18% of ITDMs overall would turn to an MPS provider for print security guidance, while 21% would consult a print manufacturer. This points to an opportunity for MPS providers and channel partners to collaborate more closely with MSSPs.

- **CIOs and CISOs differ in their views on the future of print, and their handling of security challenges relating to the hybrid print environment.** CISOs are more bullish, with 53% and 58% respectively expecting a rise in office and home print volumes, compared to 42% and 40% of CIOs. Notably, CIOs (32%) and CISOs (33%) show the most concern around home printing compared to other IT respondents, ranking it as their second top security risk. CIOs also seem to be finding it harder than CISOs to keep up with print security challenges – 61% stated that they were finding it considerably or somewhat harder, compared to only 44% of CISOs, where 29% also stated that they were finding it somewhat or a lot easier.

Table of Contents

Work environment and technology trends

Any hopes that the pandemic would just go away, and that everything would return to how it was, have been dashed. Pre-pandemic approaches focused around a primarily static, office-based workforce now need to move to supporting workers who spend some time in the office, and some time in the home environment. Security is high on the list of most organisations' priorities when managing this hybrid working environment.

Remote working is here to stay

Pre-COVID, 32% of an average organisation's workforce was working predominantly remotely (Figure 1). Once offices fully reopen, this is expected to grow to 44%. Geographically, the biggest increase is expected in the UK (29% to 45%), with the public sector being the vertical experiencing the biggest growth (26% to 45%). Smaller organisations (250-499 employees) are expecting to see a higher rise than those of other sizes (from 29% to 42%).

This demonstrates the scale of the problem organisations have to deal with: a largely office-based workforce, where sales and field staff once formed the majority of the remote working population, will now become a far more disparate environment with closer to half of the workforce working remotely – at least part of the time.

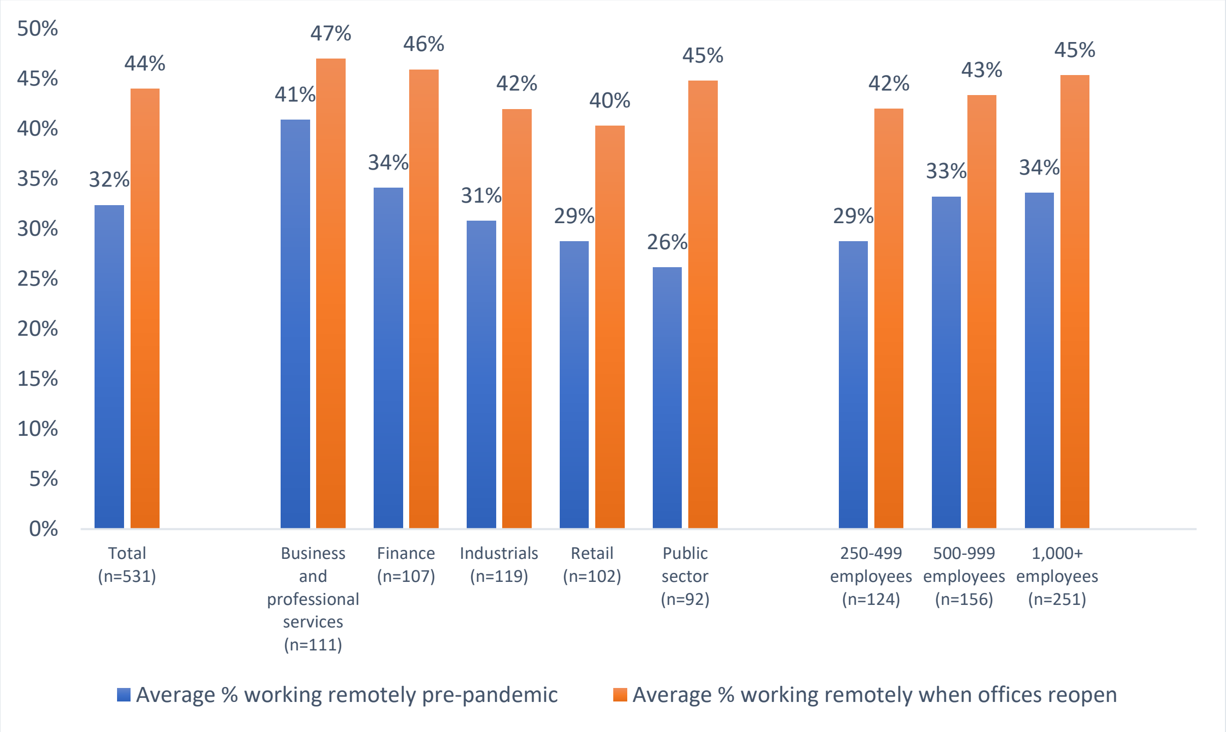

Figure 1. Average percentage of workforce working fully or predominantly from home

Most workers will not be based at home full time. This means the organisation must apply security measures that cover the whole gamut of work practices: those 100% in the office, those 100% remote, and those somewhere along the spectrum between the two.

Cloud adoption is set to accelerate

The cloud has been the foundation of digital transformation over the course of the pandemic, enabling the rapid shift to homeworking and supporting virtual collaboration for dispersed workforces. Cloud adoption is set to increase with 21% of organisations expecting to be fully in the cloud in two years' time, compared to 2% now (Figure 2). The proportion that expects to be fully in the cloud in the next two years rises to 28% in the US and 26% in retail.

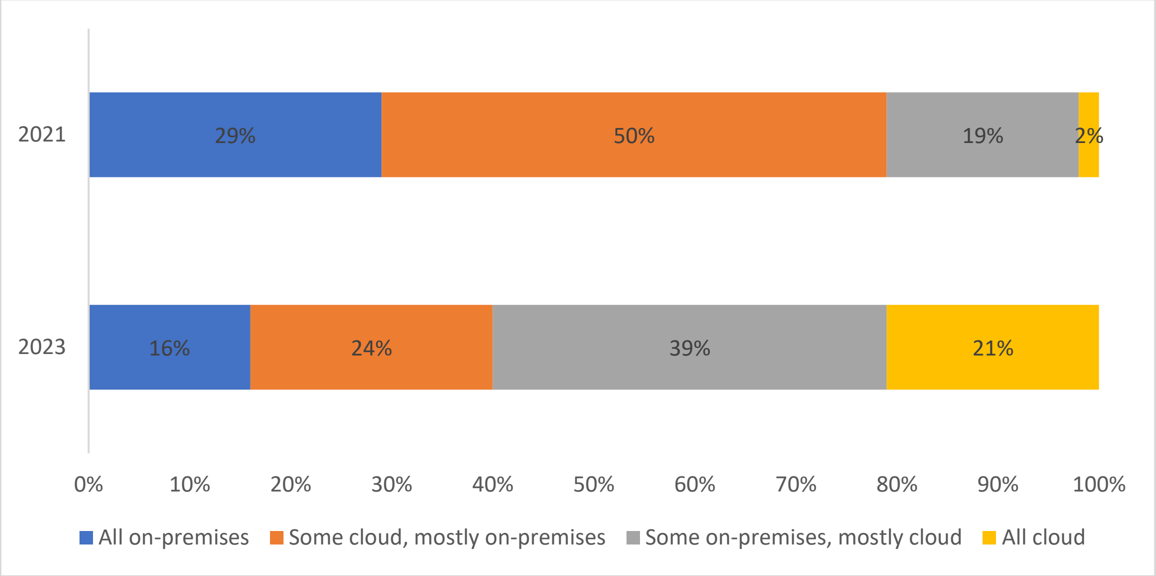

Figure 2. Which statement best reflects your organisation's total IT environment (infrastructure, applications, data, etc, excluding client devices)?

When it comes to printing, overall 44% reported that they were currently using a cloud-based print service, with a further 43% planning to do so. In fact, 52% believe using a cloud print service is more secure than managing printing on-premise, with a further 35% saying it is somewhat more secure.

Increased use of the cloud across all business sizes creates the need for robust security measures to protect users and keep data and business operations safe from cyberattacks. It is unsurprising therefore that security is a top technology investment priority for the next 12 months.

Security leads technology investment priorities

IT security remains a key priority for the majority of organisations, with 53% of respondents placing this among their top three key areas for investment (Figure 3).

63% of French respondents stated security as one of their top three priorities, compared to 50% in the US and the UK. 56% of UK respondents state that cloud services will be a key area for investment, against an overall average of 35%. Only 41% of public sector respondents see security as one of their highest priorities, against 62% in business and professional services.

Overall, 41% expect that MPS will be an investment priority over the next 12 months, rising to 59% in the UK, 52% in the retail sector and 46% in large organisations. A move to operating offices at lower overall capacities will accelerate the need to evaluate and change current printer fleet deployments. This will create new opportunities for MPS providers to deliver secure and agile print solutions that support the hybrid working model.

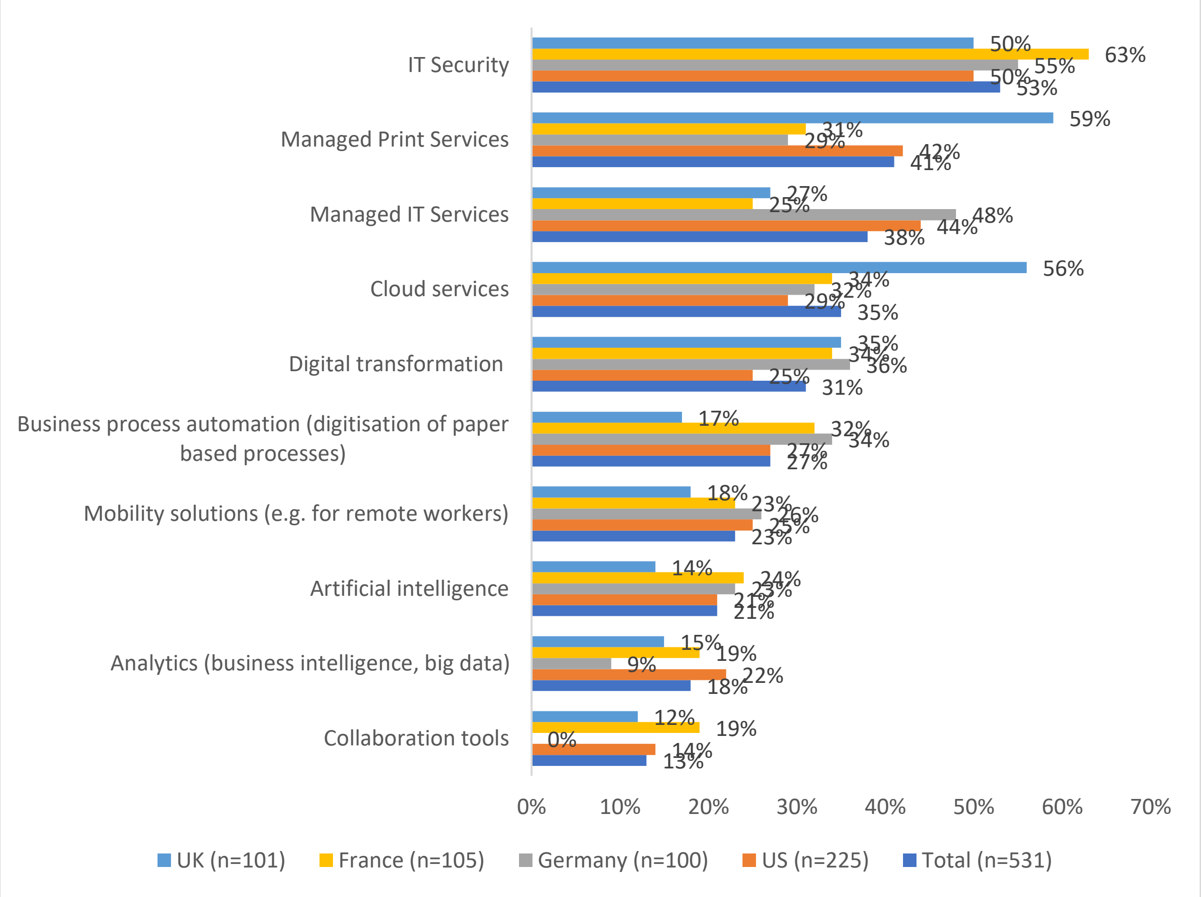

Figure 3. Top technology investments for the next 12 months (Top 3 selected)

A continued reliance on printing requires effective print security

Overall, 64% indicate printing will remain critical or very important in the next 12 months, down from 71% now (Figure 4).

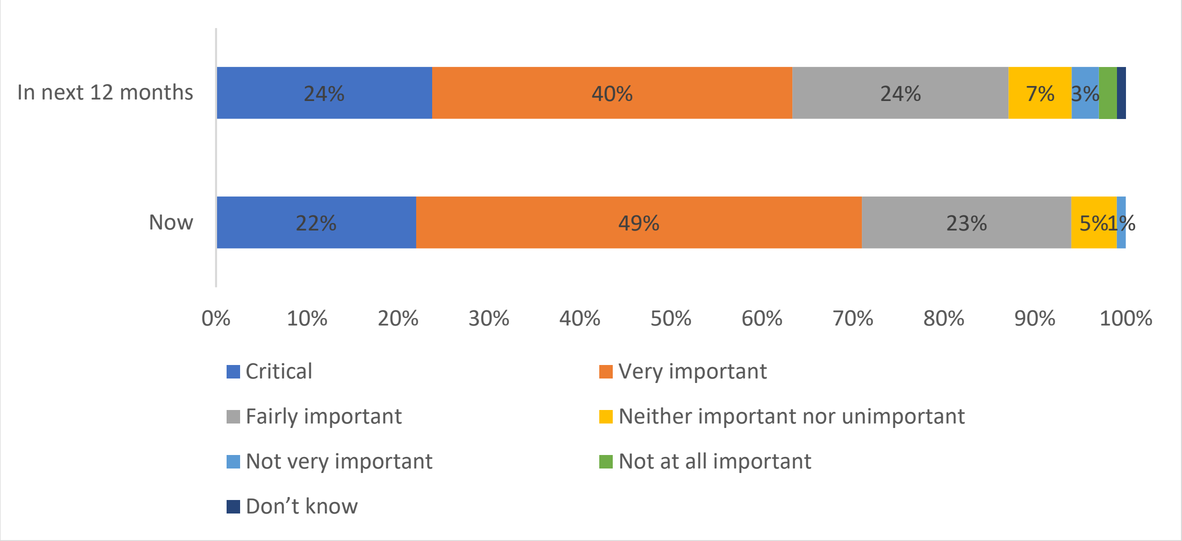

Figure 4. How important is printing to your business?

Notably it is smaller organisations that expect the importance of printing to decline faster – 59% believe it will be critical or very important in the next year down from 72% now. In comparison, 65% of larger enterprises believe it will be critical or very important compared to 73% now. This ongoing dependence on printing, particularly in large organisations that are managing a hybrid workforce, will demand more effective and integrated print security measures that protect and manage devices, documents and the network.

Although office closures have severely impacted office print volumes over the past year, 44% expect office print volumes to increase over the next 12 months (Figure 5). However regional variations prevail, with just 28% of German respondents expecting an increase compared to 59% in the US. Overall, 41% expect home print volumes to increase. Notably, CISOs are more bullish with 53% and 58% respectively expecting a rise in office and home print volumes, compared to 42% and 40% of CIOs.

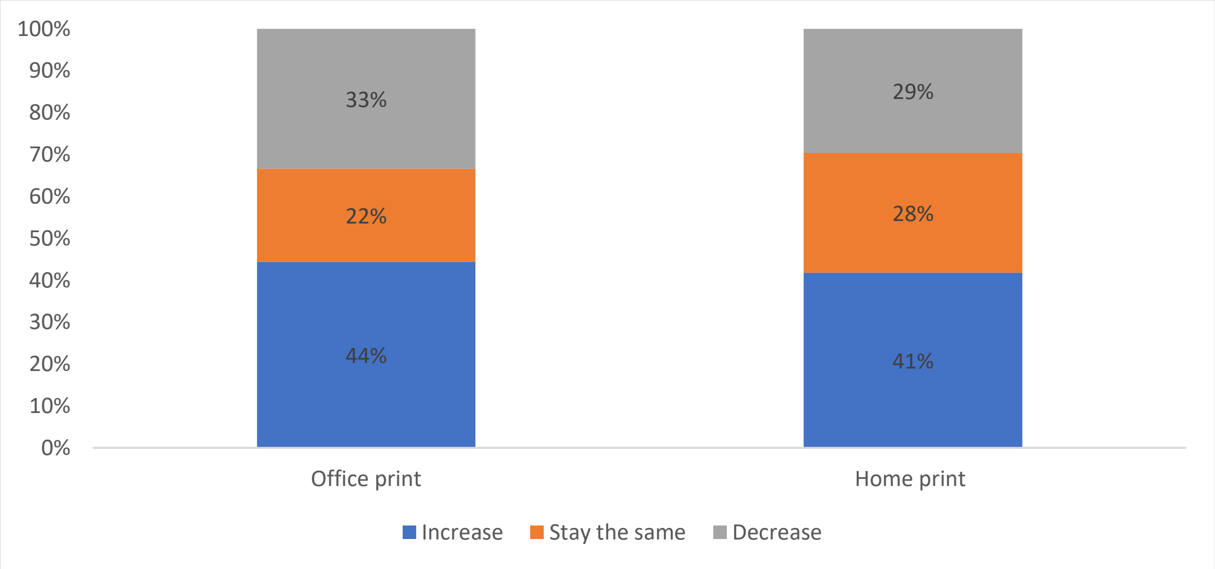

Figure 5. Over the next 12 months, how do you expect your organisation's print volumes to change?

There is an even bigger gap in expectations between those organisations that use an MPS provider and those who do not (Figure 6).

Those not using an MPS provider expect to see office and home print volumes to stay the same or fall slightly over the next 12 months. Those using an MPS provider foresee much greater print volume growth. Being able to measure volumes accurately using MPS tools and reporting systems, alongside having more control over how and where printing takes place, will make many MPS users more open to increasing print volumes as needed.

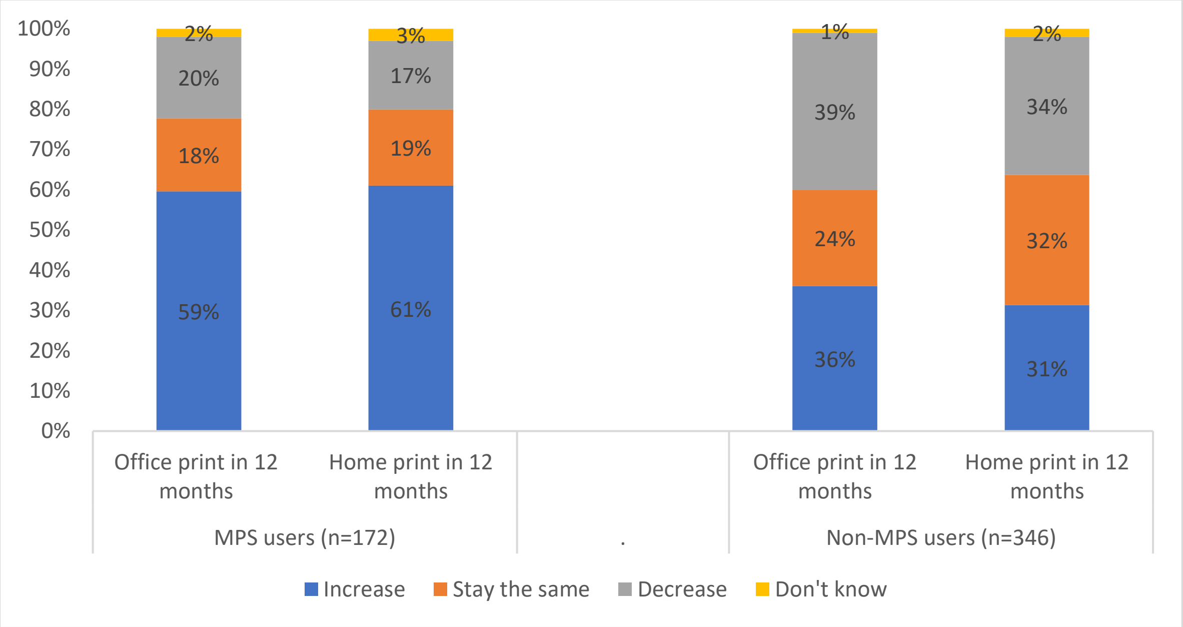

Figure 6: How do you expect print volumes to change over the next 12 months? (By MPS usage)

When looking at the level of confidence that print levels will return to pre-pandemic levels, the US has the greatest certainty, with 86% either very (46%) or somewhat (40%) confident (Figure 7). Germany has the lowest level of overall confidence (61%).

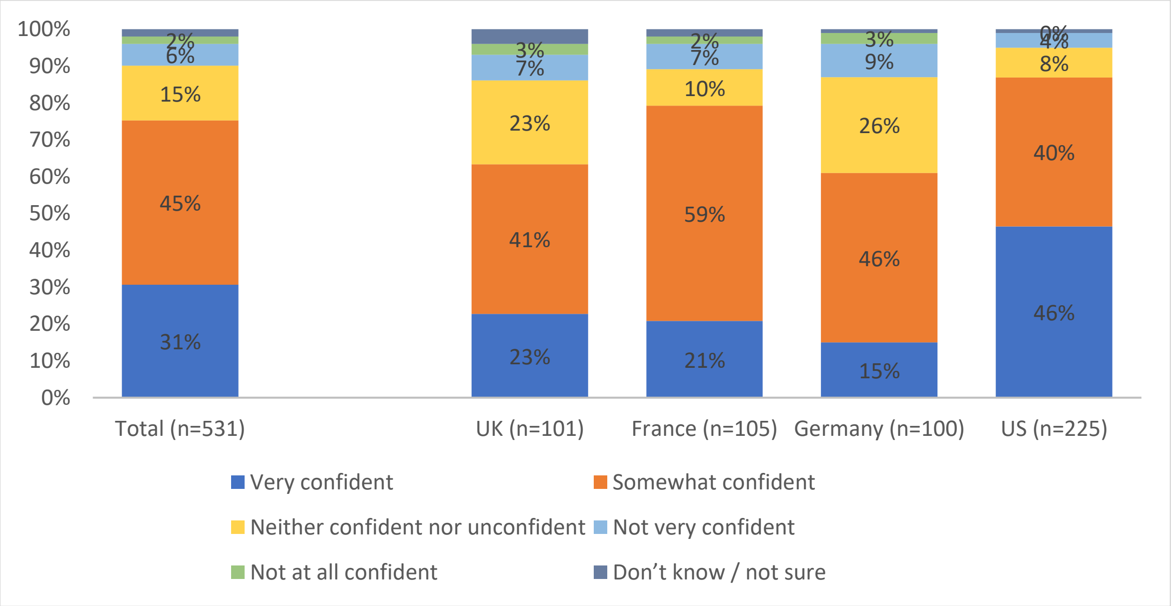

Figure 7: How confident are you that office print volumes will return to pre-pandemic levels over the next 12 months?

The expanded threat landscape

The move to hybrid working means that more devices are being used – many of them not provided, managed or controlled by the organisation. Bring Your Own Device (BYOD) has expanded to become Bring Your Own Office (BYOO), with desktop/laptop computers being used alongside tablets, mobile phones, printers and other devices, mainly bought and set up by the user themselves. This has major impacts on the overall threat landscape that an organisation has to monitor and manage: not only via direct endpoint management, but also when protecting the security of data and information when devices connect across public networks.

Employee-owned home printers are viewed as a high security risk

Despite the continued prevalence of printing across both the home and office environments, print security continues to be lower on the security agenda than other elements of the IT infrastructure (Figure 8). Overall, 24% view employee-owned home printers as a top security risk with 21% citing the office print infrastructure poses a top risk. This compares to 33% that cite cloud or hybrid platforms, email (28%), public networks (28%) and traditional endpoints (24%).

There are distinct variations in the perceived risks around printing depending on whether the organisation is using an MPS. In most cases – apart from email and traditional user endpoints – MPS users are far more wary of the threats posed by each area. They are also far more likely to have visibility of their print environment and should be implementing measures to mitigate risks around both home and office printing.

Notably, CIOs (32%) and CISOs (33%) show the most concern around home printing compared to other IT respondents, ranking it as their second top security risk. This awareness of the security vulnerabilities of remote working and shadow IT around home printing amongst C level respondents is encouraging. However, it also points at the security challenges they face in managing and securing home printing, particularly as remote working is set to persist.

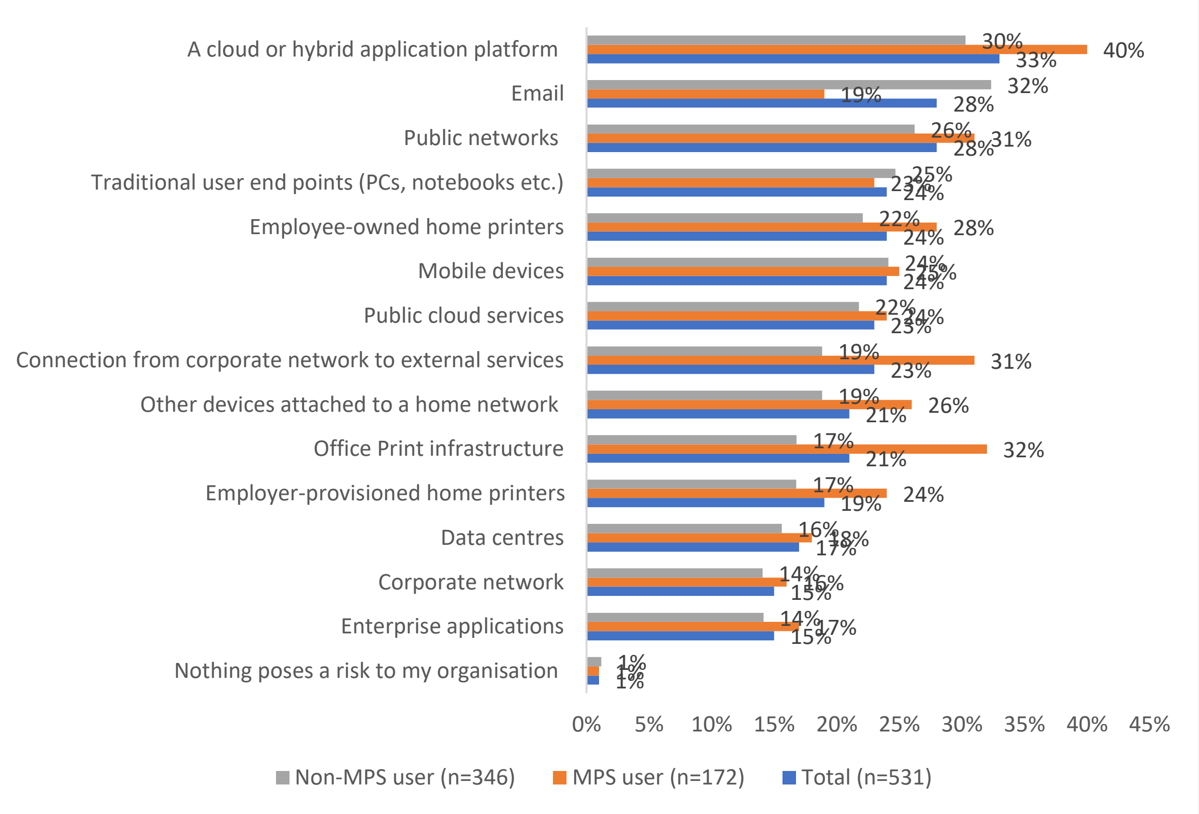

Figure 8: Which areas are considered to pose the greatest security breach risk? (Select up to five)

Print security challenges are harder to keep up with

The shift to remote working has made it more difficult for many organisations to keep up with print security challenges (Figure 9), with more than half (53%) overall stating that it was either considerably or somewhat harder. This rises to 55% amongst SMBs. This was highest in the UK (63%) and lowest in the US (47%). Although MPS and non-MPS users were not far apart in their perceptions of how much harder it had become, MPS users were twice as likely to state that it had become somewhat or a lot easier (31%) than non-MPS users (15%).

CIOs also seem to be finding it harder to keep up with challenges – 61% stated that they were finding it considerably or somewhat harder, compared to only 44% of CISOs, where 29% also stated that they were finding it somewhat or a lot easier.

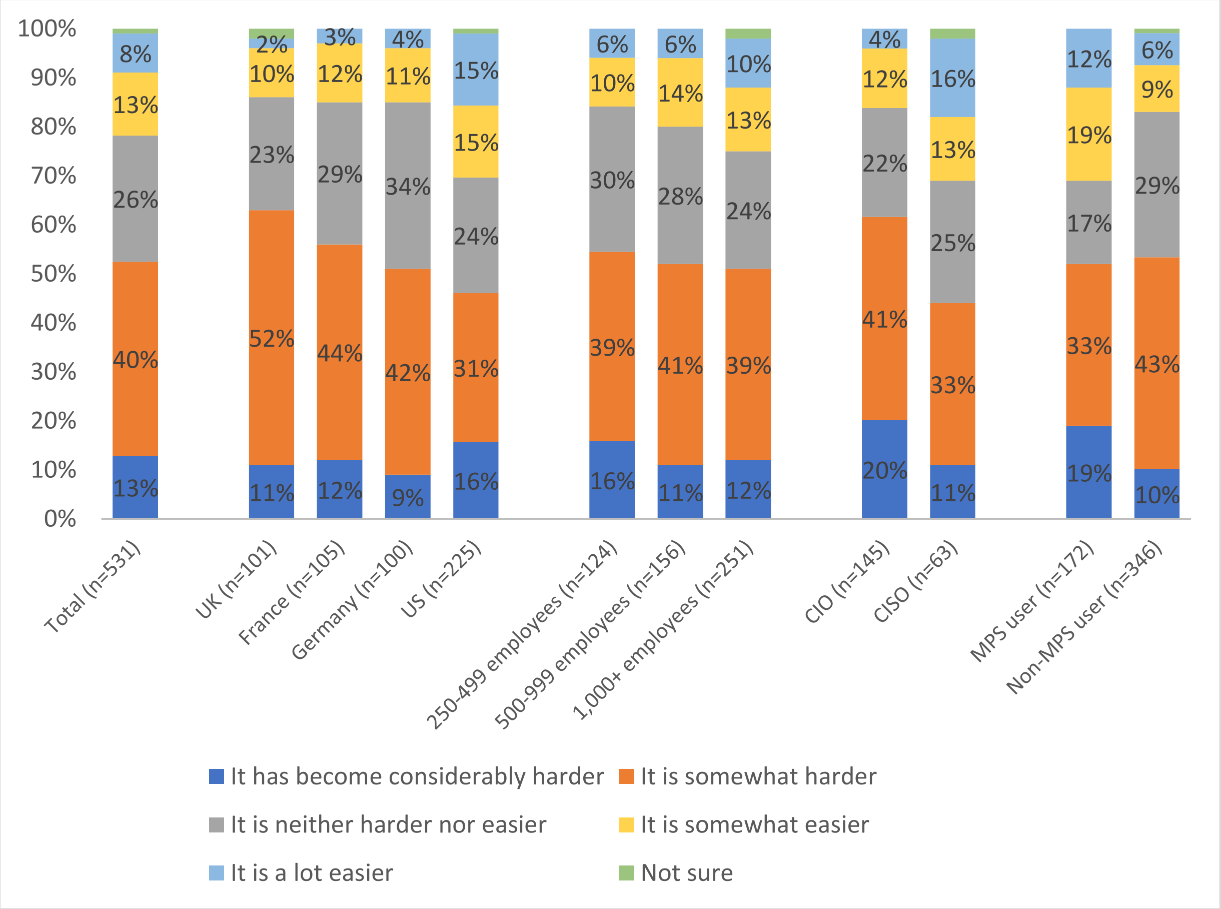

Figure 9: How do you feel about keeping up with print security challenges and demands?

Organisations using MPS are most confident in their print security

Overall, 26% of respondents say they are completely confident and a further 34% are mostly confident in the security of their print infrastructure once offices reopen (Figure 10). US respondents are the most confident, with 37% reporting they are completely confident compared to just 16% in the UK, 17% in Germany and 22% in France. Industrials is the most confident sector (31% say they are completely confident), dropping to 21% in the finance sector. Mid-size organisations report the highest confidence (33%) compared to 20% of smaller organisations.

Notably, organisations using an MPS have the most confidence in their print security. 84% of MPS users are completely (37%) or mostly confident (47%) in their security compared to only 49% of non-MPS users (22% and 27% respectively).

This positive finding demonstrates how MPS can help organisations mitigate risk and instil confidence in their security posture. MPS can deliver proactive security measures such as remote monitoring and remediation and in-depth security assessments are fundamental in understanding security vulnerabilities across the hybrid work environment.

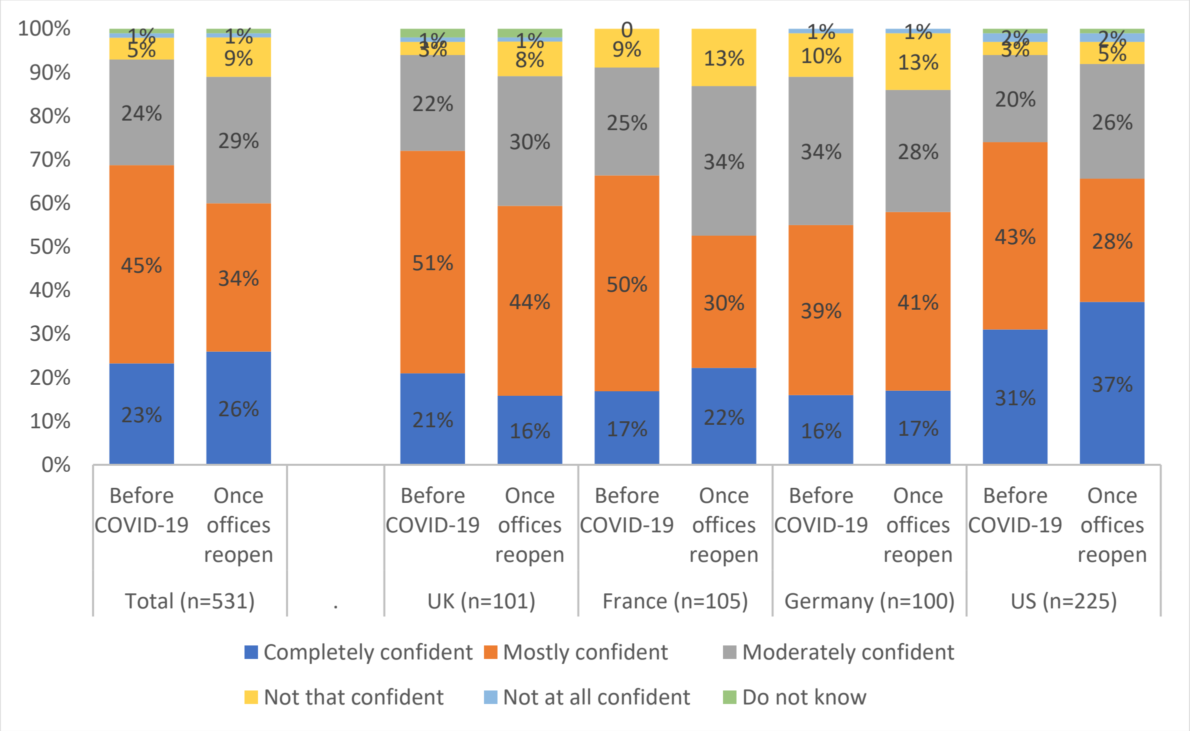

Figure 10: How confident are you that your organisation's print infrastructure (office and remote workplace) was/is protected from security breaches and data loss?

Print related data loss, cost and impact

The majority report print-related data losses, particularly in smaller organisations

68% of organisations have reported at least one print related data loss over the past 12 months (Figure 11), rising to 72% in the US and 77% in organisations with 500-999 employees and dropping to 59% amongst large organisations. Public sector organisations were most likely to have experienced a data loss during the period (77%), while industrials reported the lowest volume of data breaches (62%).

With mid-sized organisations stating the highest confidence levels in the security of their print platforms, yet also disclosing the highest number of data breaches, there is an obvious disconnect between perception and reality here. The channel should step up to help in providing solid security audits backed up with advice that will enable an organisation to better understand its security risks. The organisation can then make better decisions on what it implements as adequate security measures – aided by the channel partner.

Notably, 73% of those operating a mixed fleet of printers reported data breaches – while only 58% of those with a standardised fleet did. For MPS providers this opens up major opportunities to move customers to a managed, single vendor fleet in order to better control data security – focusing on the message that data breaches result in material business and reputational costs to an organisation.

MPS and non-MPS users reported pretty much the same levels of data breaches, although those using an MPS service did report a greater level of "many data losses" (20%) than non-MPS users (10%). Although this may look bad, it is likely that the MPS service itself uncovered the data breaches, whereas those not using an MPS service may well have had more breaches that they were unaware of.

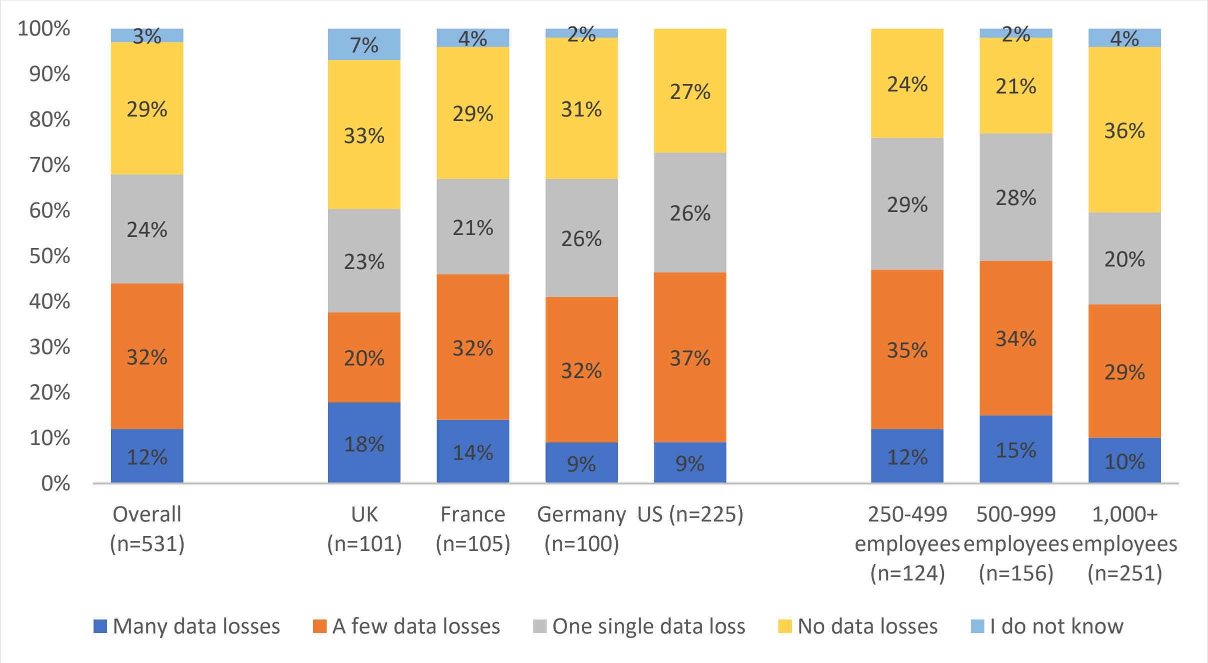

Figure 11: Level of data losses through printers/MFPs due to insecure printing practices (in past 12 months)

When asked to consider the reasons behind the print related data losses they had suffered, 28% cited vulnerabilities around home printers such as homeworkers not disposing of confidential information securely. 27% indicated the printer was used as an access point into the corporate network and 26% stated user credentials for an office printer were compromised.

The cost of a print related data loss

These data losses are costing organisations an estimated average of over £630,000 per breach, rising to over £806,000 in the UK and dropping to under £545,000 in the US (Figure 12).

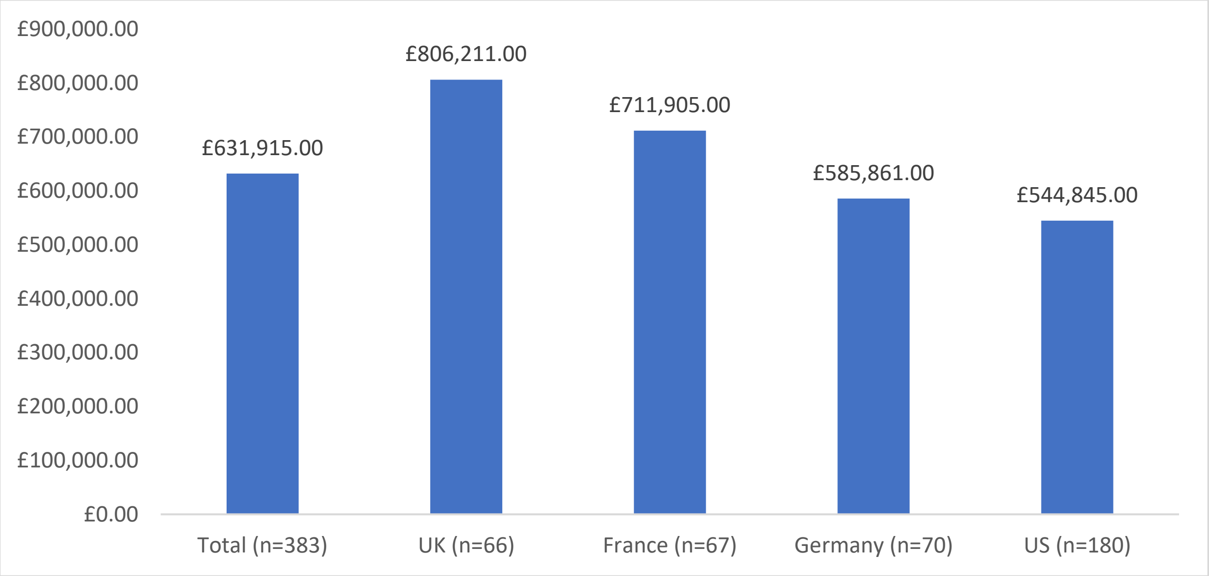

Figure 12: Estimated average cost of a data loss

Unsurprisingly, large organisations report higher costs (£1,109,394 per breach) compared to mid-sized organisations (£989,259) and SMBs (£131,875). However, 36% of the largest organisations reported no data losses, compared to only 21% of the mid-sized organisations and 24% of the SMBs. In all cases, though, such costs are considerable and could have major impacts on the survivability of the organisation concerned.

The broad consequences of a data loss threaten SMBs

Beyond the simple direct costs of a data breach, organisations also report a range of other impacts (Figure 13). The highest impact overall is on the amount of time it takes the IT team to respond to and manage the issue (33%).

Although SMBs find this less of a problem, with only 23% stating it as a major impact, 30% report that the data loss had led to lost customers. This compares to just 18% of mid-size businesses. The impact of lost customers on any SMB cannot be underestimated. Smaller companies need to understand the consequences of a data breach in order to assess risk. Many often mistakenly believe that they are too small to be a target or underestimate the vulnerabilities around their print environment – creating weaknesses for cyber attackers to exploit.

Given that just 20% are confident in their print security this is an opportunity for the channel to deliver security services and solutions to this market segment.

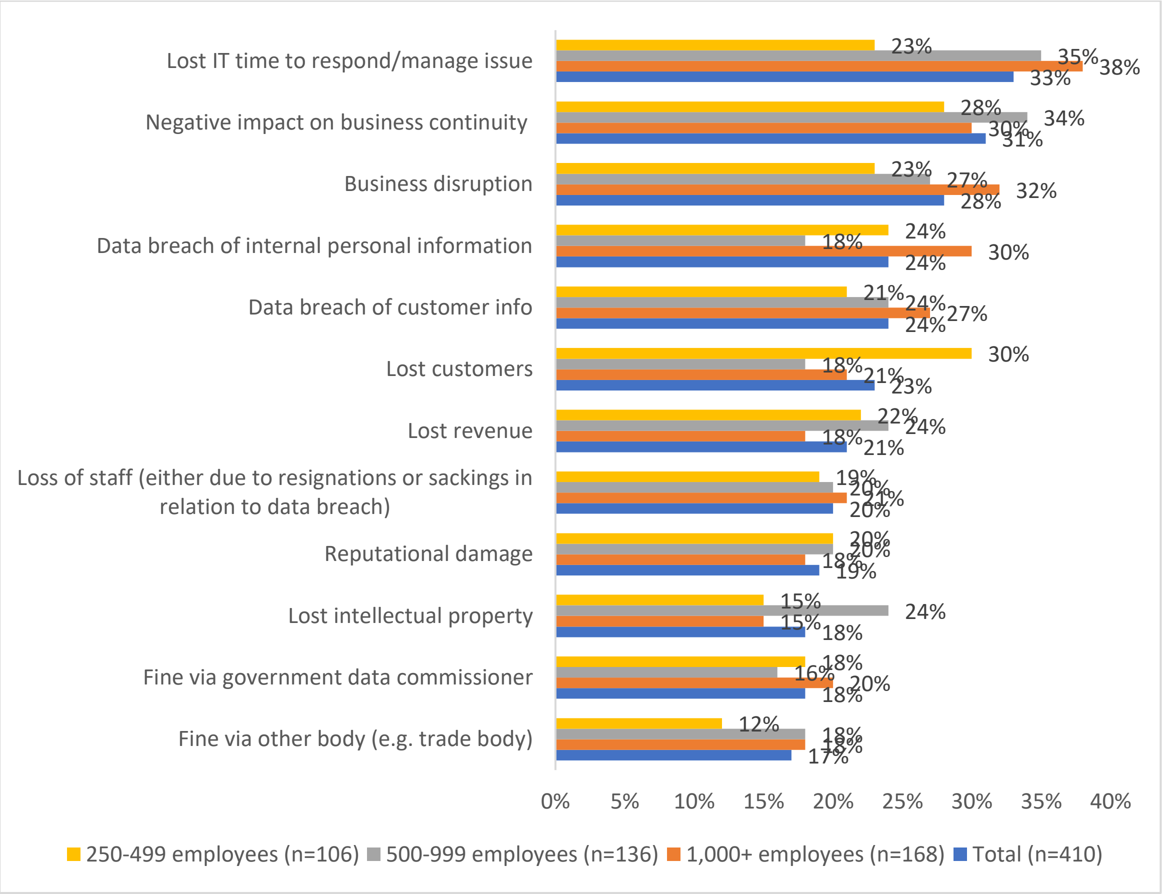

Figure 13: What were the major impacts of these data losses? Select all that apply

Awareness and effect of PrintNightmare

In June 2021, Microsoft was made aware of a pair of critical errors in its print spooler. The two related issues enabled remote code execution and privilege escalation – both of which can present catastrophic security issues to organisations. Microsoft issued out-of-band patches to attempt to resolve the errors – but this led to some printers no longer working and the need for administrators to manually install print drivers for users in some cases. The organisation that first discovered the issues, Sangfor, accidentally published a proof of concept (PoC) means of leveraging the errors to gain access to an organisation's environment. Although rapidly deleted, the PoC was copied and distributed widely. PrintNightmare was covered extensively in the technical press, and Microsoft pushed hard for its patches to be installed as a matter of urgency.

Quocirca's research shows that 27% of respondents are unaware of PrintNightmare (Figure 14), rising to 41% in the UK. Overall, 19% say it had impacted their business, rising to 25% in the US and 26% in smaller businesses. Somewhat surprisingly, those in the largest organisations are the least aware, with 33% stating that they have not heard of PrintNightmare.

For those using a well-provisioned and run MPS service, there is less need to know too much about such threats: the MPS provider should be monitoring for them, and patching and managing the environment to minimise them.

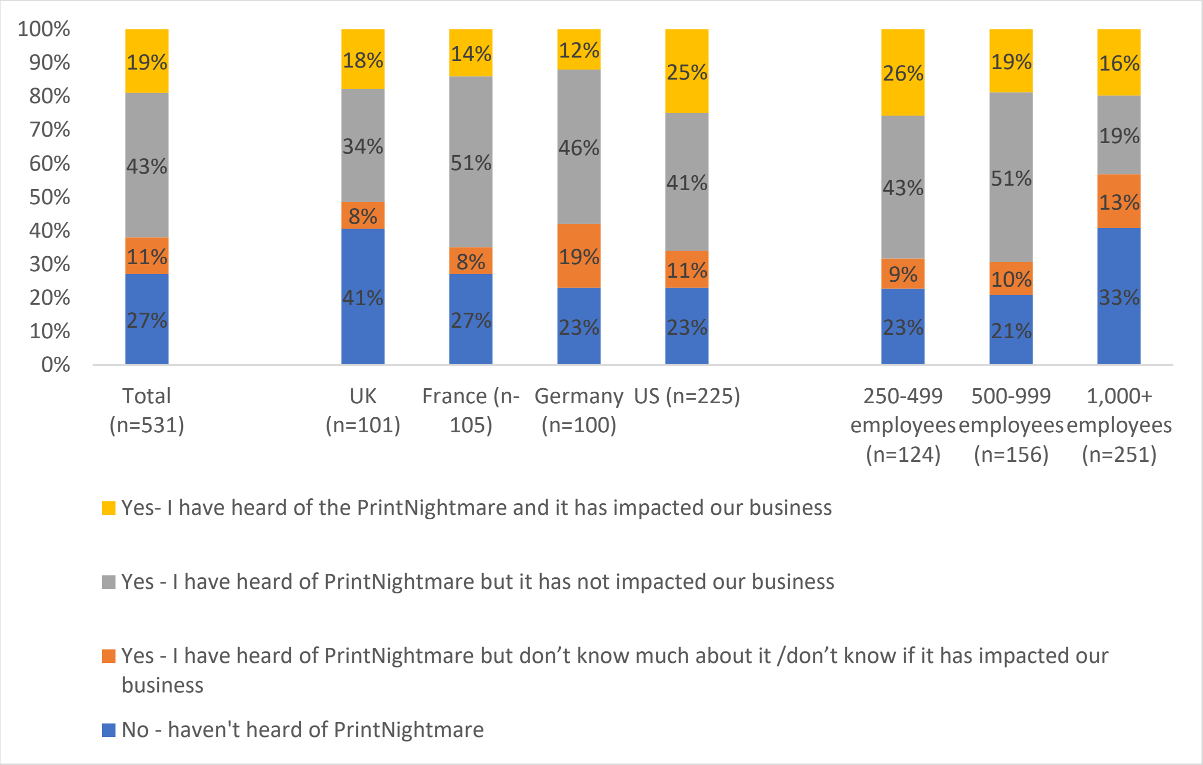

Figure 14: Are you aware of the Microsoft PrintNightmare printer spooler flaw/vulnerability, and has it had any impact on your business?

Taking measures to address print security

With such marked differences between respondents' confidence in the security of their print environments, and the problems they have encountered due to a lack of adequate print security, organisations must now take the steps required to create a long-term strategic approach to information security, moving to embrace the change to hybrid working and the use of a more disparate printer fleet.

Print security spend set to increase over next 12 months

Overall, 70% of organisations expect their print security spend to increase over the next 12 months (Figure 15), with only 11% expecting a decrease. This rises to 77% in France and drops to 59% in the UK. Overall, 13% are expecting an increase in print security spend of greater than 26%.

The largest organisations (1,000+ employees) report the highest expectation of an increase (72%), with industrials being the vertical with the greatest expectations (76%). 77% of MPS users expect to see an increase in print security spend, compared to 66% of non-MPS users.

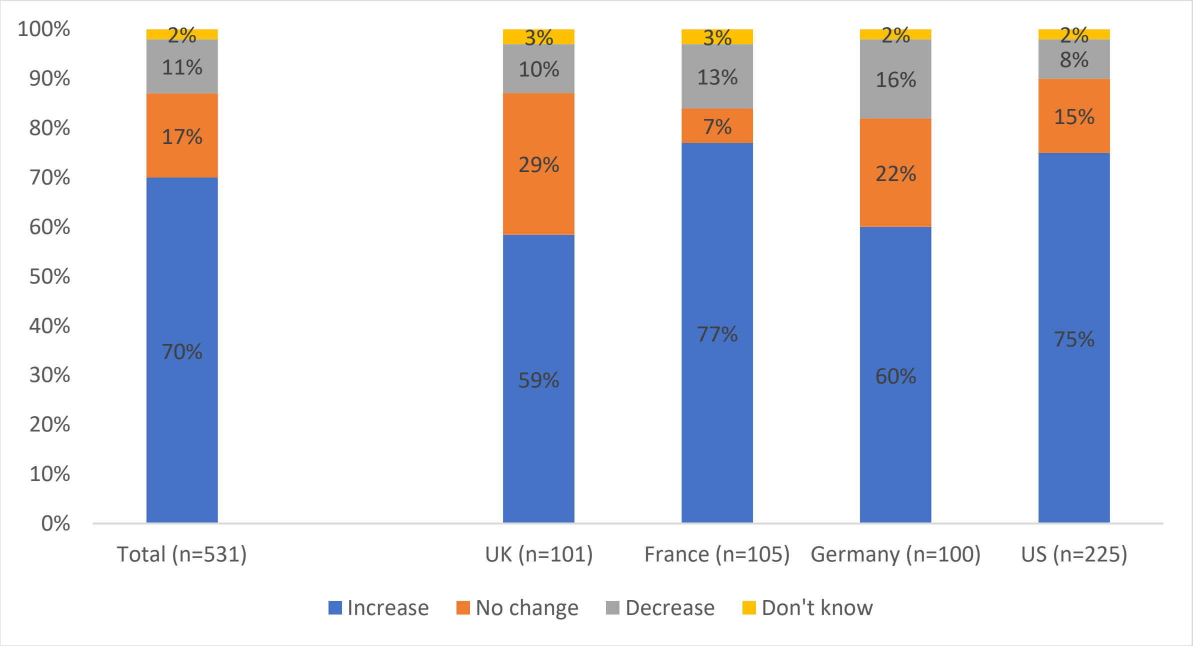

Figure 15: How do you expect your organisation's print security spend to change over the next 12 months?

Formal print security assessments and reporting are the top measures implemented

A variety of print security technologies and processes are being adopted (Figure 16).

The use of reporting and analytics (38%) along with formal assessments (38%) is the most widely implemented approach. This rises to 41% and 45% respectively in large organisations, which are also far more likely to implement many of the other measures. SMBs show lower adoption in areas such as implementing formal print security and risk assessments (30%) and revising security/BYOD policies to cover home printers (23%). 32% of organisations have adopted a zero trust security model.

The US is ahead in terms of having already implemented each area – by some degree. For example, 45% of US respondents state they have implemented reporting and analytics, against only 32/33% in other regions. Likewise, 44% of US respondents have adopted formal processes to respond to print security issues, against only 30% in France. 44% of US respondents also say they have adopted a zero trust approach to security – compared with only 21% in the UK, 22% in France and 30% in Germany.

42% of respondents in retail state they have adopted reporting and analytics as a means to secure print, dropping to 32% in business and professional services, which scores higher on the presence of formal processes to respond to print security incidents (41%). Formal assessments and security audits of cloud and MPS providers are high on the finance sector's list (45%), along with the use of content security solutions such as DLP (44%). Pull printing scores poorly, with only 31% of respondents saying they use it, rising to 38% in finance.

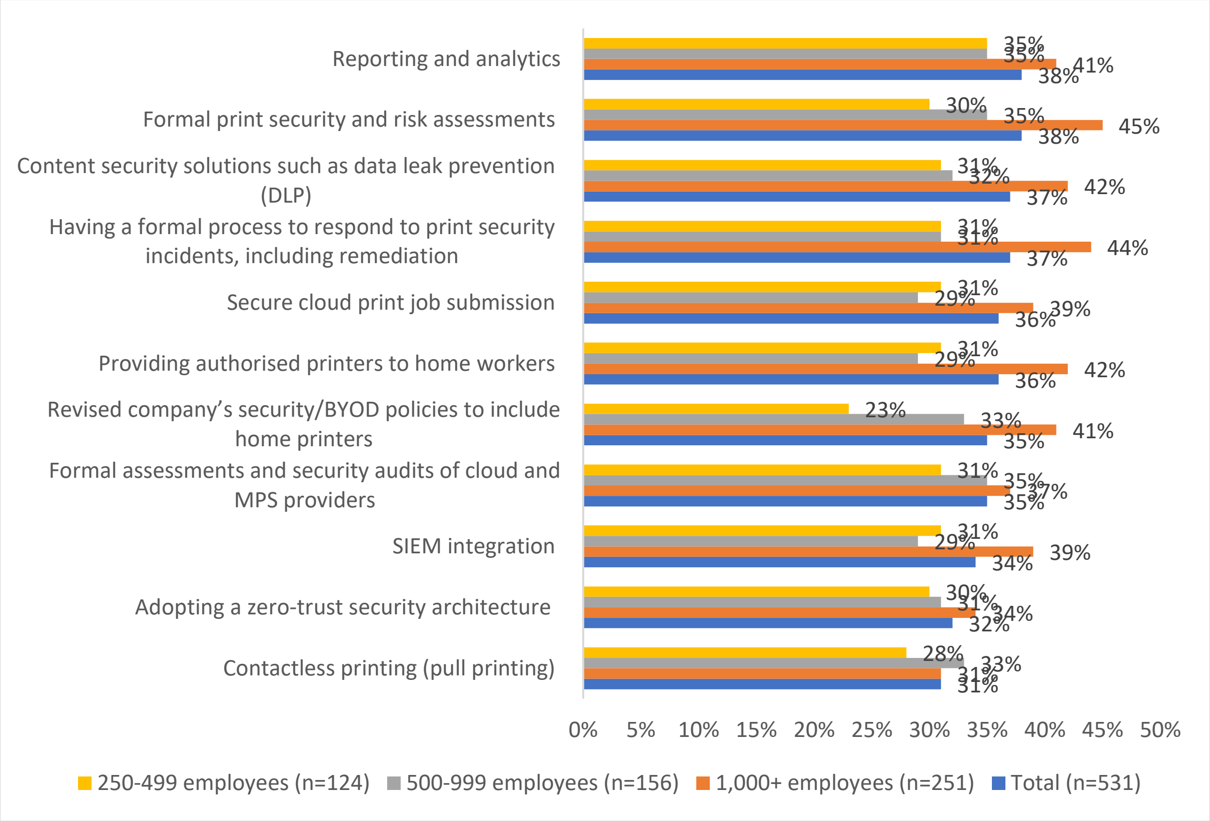

Figure 16: Has your organisation implemented any of the following print security measures?

The Quocirca Print Security Maturity Index

To understand and compare the extent to which organisations are adopting these measures, Quocirca has created a Print Security Maturity Index based on the number of measures implemented by our research sample, dividing them into leaders, followers and laggards.

- **Leaders** have implemented six or more of the measures (i.e. more than 50% of the measures indicated in Figure 16).
- **Followers** have implemented between two and five measures.
- **Laggards** have implemented one or none of the measures.

Overall, just 18% are classed as print security leaders, rising to 22% in the US (Figure 17). France has the largest proportion of laggards (37%).

When compared by vertical, finance has the largest percentage of leaders (23%), with all the others on 17% or 16%. Although there is not much of a spread, business and professional services has the highest proportion of laggards at 27%. Large organisations are the most mature, with 23% being leaders, with mid-sized organisations on 14% and SMBs on 12%. (Figure 18).

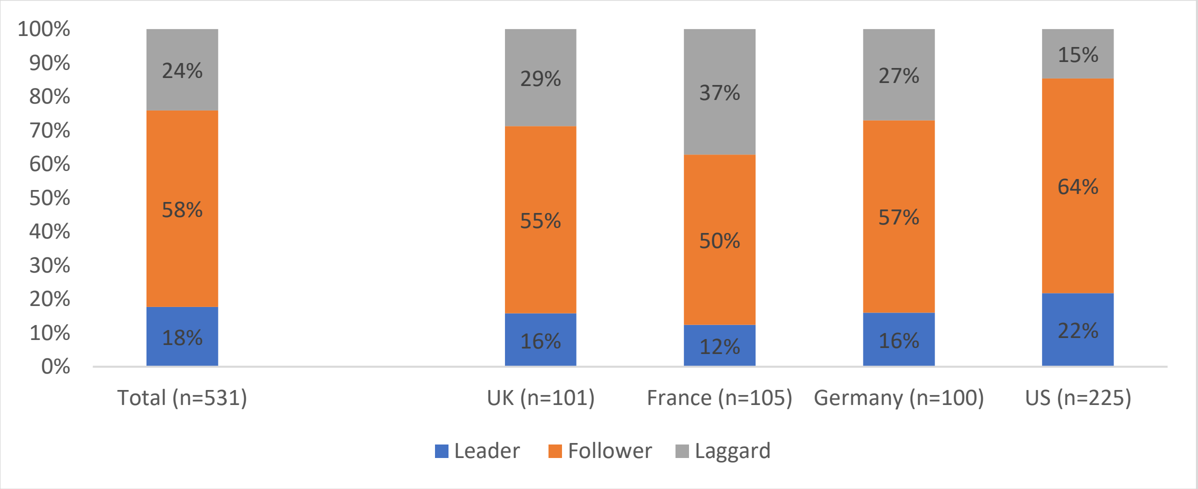

Figure 17: Quocirca's Print Security Maturity Index by country

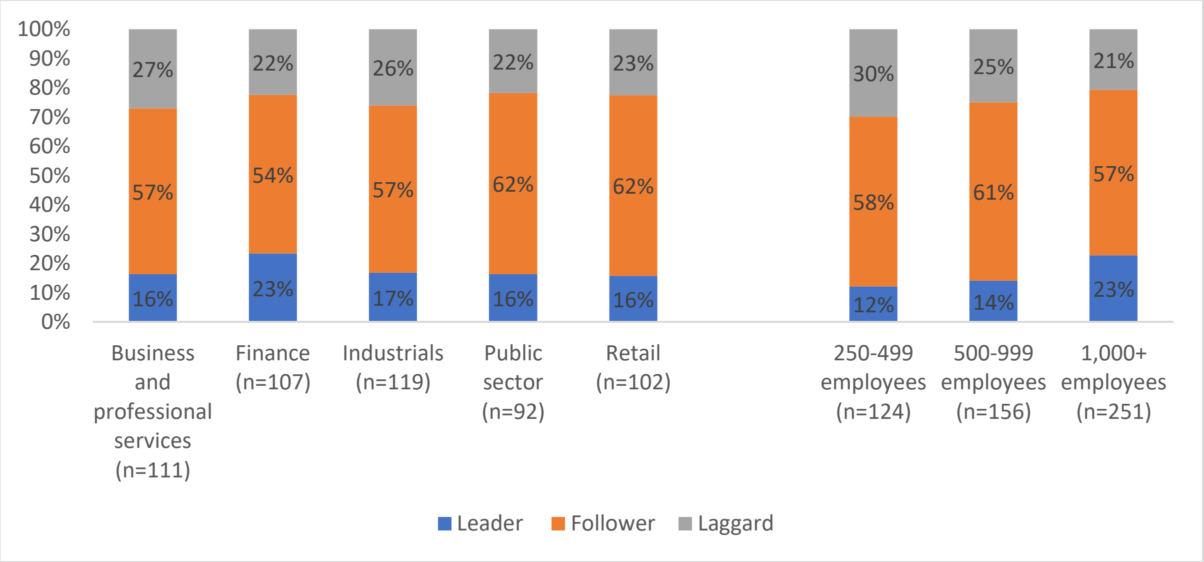

Figure 18: Quocirca's Print Security Maturity Index by vertical and size

How organisations are positioned among these segments has a major impact on other aspects of how well they are performing. For example:

- 72% of those in the leader segment use MPS, compared with only 30% of those in the follower segment and 9% of laggards.
- 80% of leaders expect their print security spend to increase over the next 12 months, compared to 70% of followers and 60% of laggards.
- 74% of leaders worry about the security of the home print environment, compared to 70% of followers and only 52% of laggards. This is probably down to greater awareness of what is happening on the platform. However, 81% of leaders are completely or mostly confident that their print infrastructure is secure against data breaches as offices reopen, compared to 64% of followers and only 38% of laggards.
- 36% of those in the leader segment report no data losses in the last 12 months, whereas only 28% of followers and 27% of laggards state no losses (Figure 19).

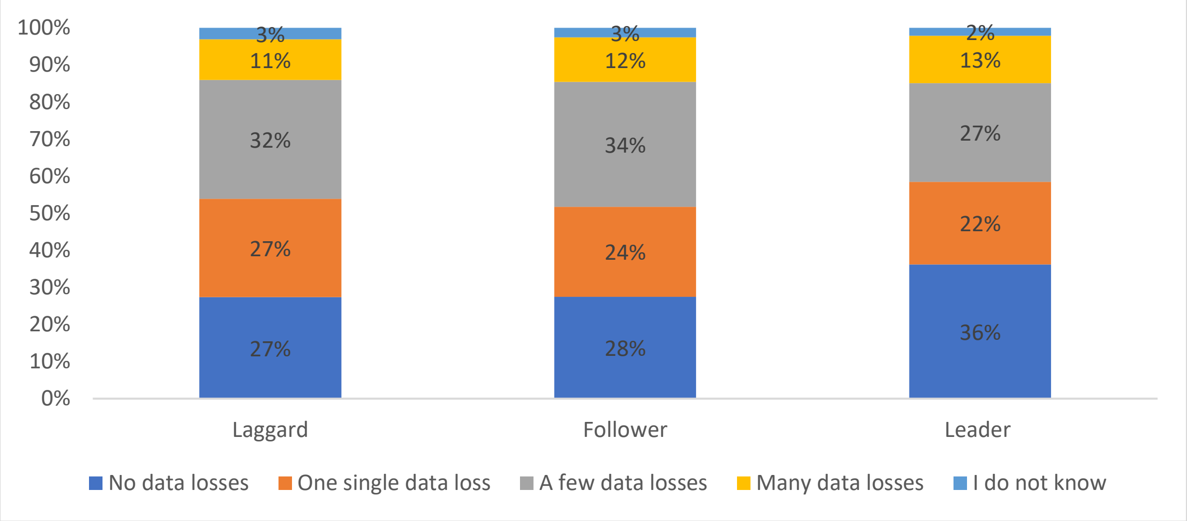

Figure 19: Reported data losses by Print Security Maturity Index

Organisations using MPS are most satisfied with print security

US organisations are most satisfied with their print suppliers' print security capabilities (Figure 20), with German respondents least satisfied. Notably, German respondents also tend to be least confident in their print security. Just 20% of public sector organisations are very satisfied, compared to 32% of retail organisations. There is an opportunity here for suppliers to drive up satisfaction rates by extending their security offerings and working with customers to increase confidence in print security.

Those using an MPS have far higher satisfaction levels (42% being very satisfied) than those without an MPS (20%). This is a strong point: it is obvious that the services which fall under an MPS offering lead to better relationships with customers.

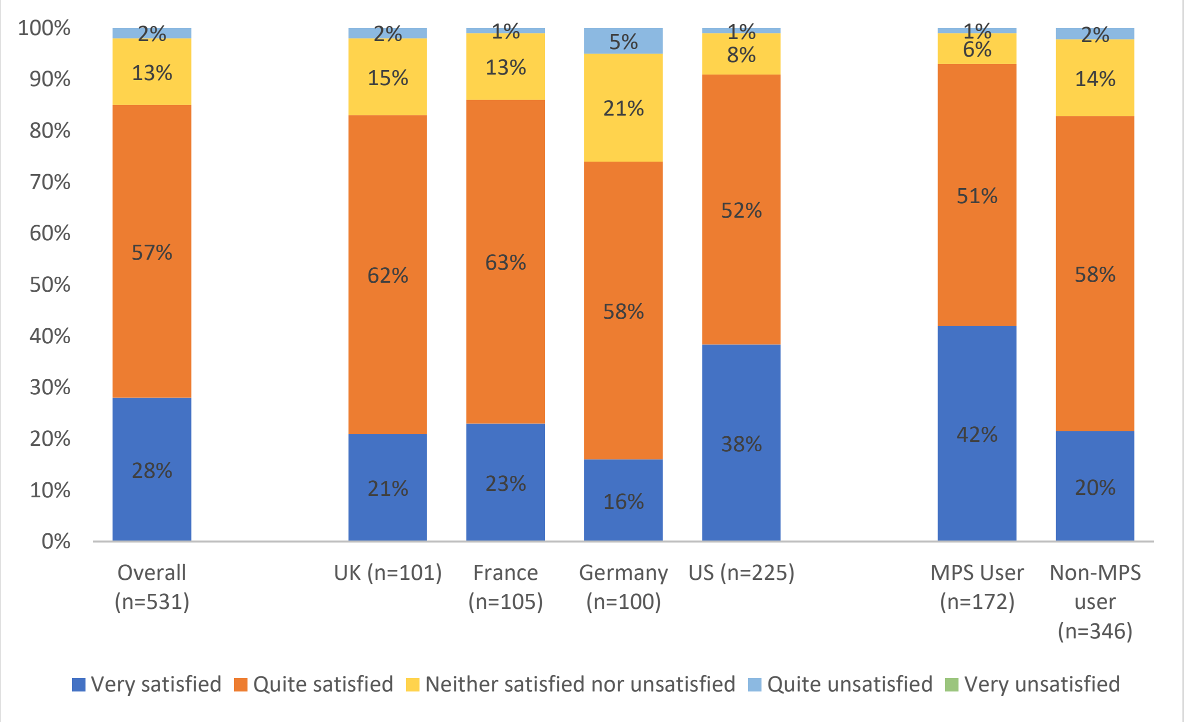

Figure 20: How satisfied are you with your print supplier's capabilities when it comes to securing your print infrastructure?

Most are turning to advice from MSSPs

Managed security service providers (MSSPs) are a popular choice for print security advice (Figure 21); overall, 35% of respondents say they would turn to an MSSP. 21% would turn to either an ISV or a print manufacturer. Whereas mid-sized and larger organisations are more likely to turn to an MSSP (40% and 36% respectively), smaller organisations favour ISVs – although there is more diversity in who they would turn to overall. 18% of respondents would consult an MPS provider for print security advice.

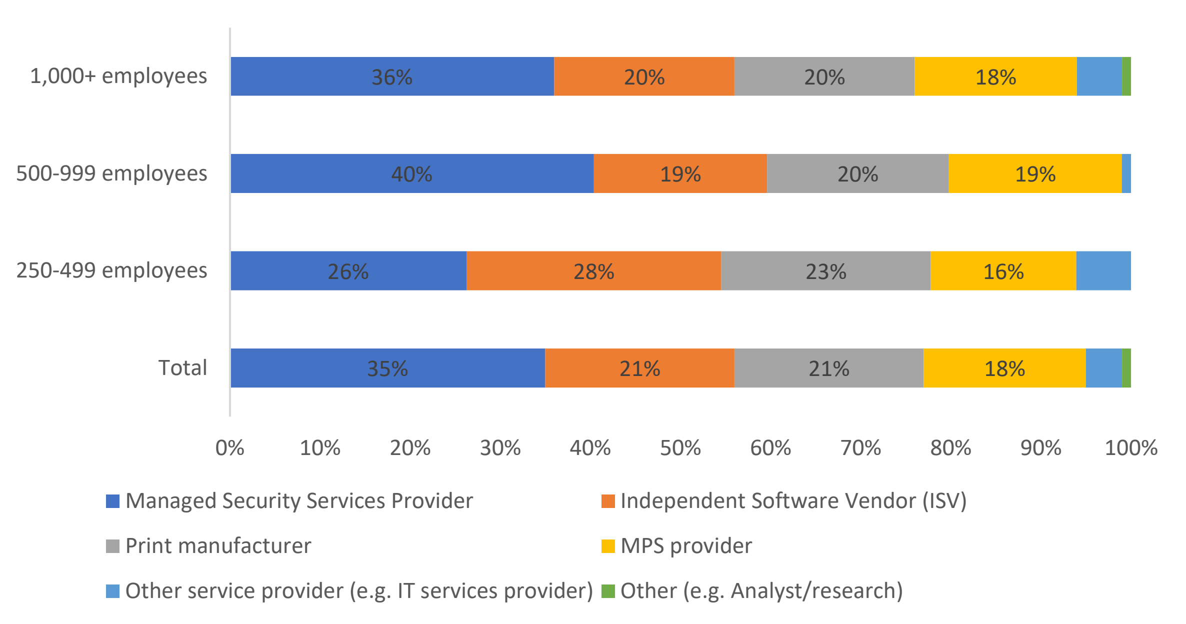

Figure 21: Where would your organisation go first for more information about improving print security?

Interestingly, those organisations using an MPS provider are still more likely to turn to an MSSP (40%) than to their existing MPS provider (23%). Those not using an MPS provider are likely to turn to a MSSP (33%) or a print manufacturer (24%). For those offering MPS, bolstering security offerings in order to fight off competition from dedicated MSSPs makes sense – maybe even through partnering with an MSSP to provide such services under the MSSP's banner.

Supplier recommendations

With 70% of organisations expecting to increase print security spend over the next 12 months, this is an area of opportunity for print manufacturers, service providers and channel partners – in particular those offering MPS. They have a vital role to play in encouraging customers to treat print security with the same urgency as other areas of IT, and helping them to implement solutions that will protect the print environment from a device, document and network perspective.

More than half of organisations are already struggling to meet the demands of securing today's fragmented print environment. Suppliers can become the 'hero' here; taking on some of the day-to-day responsibility for protecting critical data while enabling both office- and home-based employees to work in an optimised way.

- **Offer targeted maturity assessments of the security of customers' home and office print environments.** These should encompass the identification of security vulnerabilities, and the recommendation of layered measures to address their specific security requirements. Introducing services that continuously monitor print infrastructure for threats and data breaches will foster recurring revenue.
- **Demonstrate and promote competencies across IT and print security.** Endpoint security in particular has risen in importance given the expanded threat surface created by remote and home working.
- **Help clients to become Print Security Leaders.** According to Quocirca's Print Security Maturity Index, just 18% of organisations are considered leaders, which means they have implemented six or more print security measures. Providing expert guidance around reinforcing security will be worth the effort: Print Security Leaders are more likely to increase their print security spend than other organisations.
- **Seek strategic collaborations with MSSPs.** More than a third of ITDMs turn to MSSPs for print security advice, with just 18% saying they would consult MPS providers. There's an opportunity for MPS providers and channel partners to collaborate strategically with MSSPs.
- **Highlight the benefits of using an MPS to help sway non-users.** MPS usage brings organisations greater control, consistency and confidence around printing, providing visibility over the security of the entire environment while easing the burden of monitoring and managing the risks.
- **Bolster MPS security offerings to strengthen client relationships.** Less than a third (28%) of ITDMs are very satisfied with their print suppliers' security capabilities. ITDMs who use an MPS are far happier: with 42% saying they are very satisfied, compared with 20% of those who don't.
- **Aim to move customers to a managed, single vendor fleet.** Far fewer organisations that operate a standardised fleet experienced a data loss in the last 12 months than those with a mixed fleet. Standardisation will enable better control over data security, minimising the financial and reputational costs associated with a data breach.

Buyer recommendations

Print devices continue to become more sophisticated, with greater intelligence being built into even low-end consumer printers. Such intelligence can be used by those with malicious intent to access a print environment, and if that then provides direct access back into the corporate environment, chaos could ensue. Organisations must therefore pay far closer attention to protecting the print environment, particularly when looking to the continuation of hybrid working.

Organisations need to look at investing in the following areas to ensure that the print environment is secured to the same levels expected across any other area of the IT platform.

- **Conduct in-depth print security and risk assessments.** Most organisations have these in place for the overall IT environment, but the print platform often seems to be left out. Given the increasing threat landscape associated with hybrid work, organisations must ensure that the print infrastructure is fit for purpose across device, document and network security. This can be carried out internally, or by third parties such as managed security service providers (MSSPs) or managed print service (MPS) providers. New assessments must fit in with the broader IT security and risk assessments.
- **Implement a zero trust architecture.** Zero trust operates on the basis of 'never trust, always verify', assuming that an environment will be compromised and no device should ever be fully trusted. Organisations have started to implement zero trust environments, but mainly within the constraints of their owned and managed IT environment. This now needs to be extended to the wider hybrid environment, embracing home workers and all the devices that are being used for work purposes across that environment – including print devices.
- **Provide defined and authorised printers for home workers.** Individuals still require access to printed output when working from home. However, basic consumer printers do not come with the capabilities they may require, such as print speed and quality, and will not generally adhere to the needs of the organisation – such as security and manageability. Organisations should move to defining classes of printer that individuals can use, depending on need. These should then be supplied and provisioned by the organisation, along with the means of managing and controlling what business content the individual prints on the device.
- **Revise BYOD policies to include employee printers.** For many organisations, supplying and provisioning printers to all employees working from home may not be practical. Existing bring-your-own-device (BYOD) policies must now be updated to cover the home environment – moving to a BYOO (bring your own office) approach, with policies covering desktop/laptop PCs, tablets, mobile devices, desk phones and print devices. An effective BYOD/BYOO policy will help ensure that each individual's environment adheres to an organisation's basic security needs.
- **Evaluate content security solutions.** Content management systems based around document metadata, where documents are classified based on their sensitivity – along the lines of 'Public', 'Commercially sensitive', and 'Internal use only' for example – allow specific policies to be set, such as '*this document cannot be printed*' or '*this document can only be printed on an approved printer*'. This enables home-based employees to use their own printers for routine jobs without the risk of restricted documents ending up in their wastebins.
- **Implement pull printing.** Requiring a PIN or a Bluetooth or NFC token to release a job at a printer means that the print job owner has to be present before the job is printed out. Pull printing is most useful in shared access environments, as is the case for many office printers. However, it could also be applied to allow home users to submit print jobs securely via the cloud to office printers, or even their own printer – enabling them to be tracked at a central level. Jobs that the owner forgets about are held, and can be securely deleted if not printed out after a defined period of time.
- **Continuously monitor through reporting and analytics.** Risk assessments, tuning content security and configuring SIEM (security information and event management) systems all require insight provided by gathering reports from across an organisation's network, including its extension into employees'

homes. SIEM systems themselves can often provide this information, as can other log management tools.

- **Formalise processes to respond to print security incidents.** Accept that leaks are likely to happen – and plan how to deal with the repercussions. Most of the respondents to Quocirca's research had at least some security measures in place, and a reasonable belief that their print environment was secure, but 68% still experienced at least one print-related data loss in the past 18 months. Organisations must put appropriate processes in place to respond to data breaches by dealing with the possible legal and reputational damage caused, while building back business capabilities in the shortest possible time.
- **Use cloud routing for certain print jobs.** While a lot of printing is informal and needs to be near to the user to be effective – for example, printing a report in order to review it – other print jobs are part of larger business processes, and the user who submits the job may never see the output. For example, letters to be mailed to customers, marketing output, and forms that make up part of a broader process may be better printed at a more suitable printer. Employees can securely submit such jobs from home to a cloud print service, which can check the veracity of the submission, and seek secondary authorisation before allocating the job to the most suitable print resources available. Even within the office environment, such routing can help in minimising print wastage by making sure that certain print jobs go to the most suitable printer.

Vendor landscape

Quocirca has created a snapshot of the positioning of vendors in the Global Print Security market (Figure 22). Please note due to varying service offerings for each vendor, and regional differences this is intended for guidance only.

The graphic represents Quocirca's view of the competitive landscape for vendors based on the following categories:

1. **Leaders:** Vendors with strong strategic vision and a comprehensive print security product and service offering. Leaders have made significant investments in their hardware, solutions and service portfolio and infrastructure and also demonstrate a strong vision for future strategy.
2. **Major players:** Vendors that have established and proven offerings and are continuing to develop their solutions service portfolio. These vendors are most likely to be strongly focused on the SMB market with a hardware-centric approach.

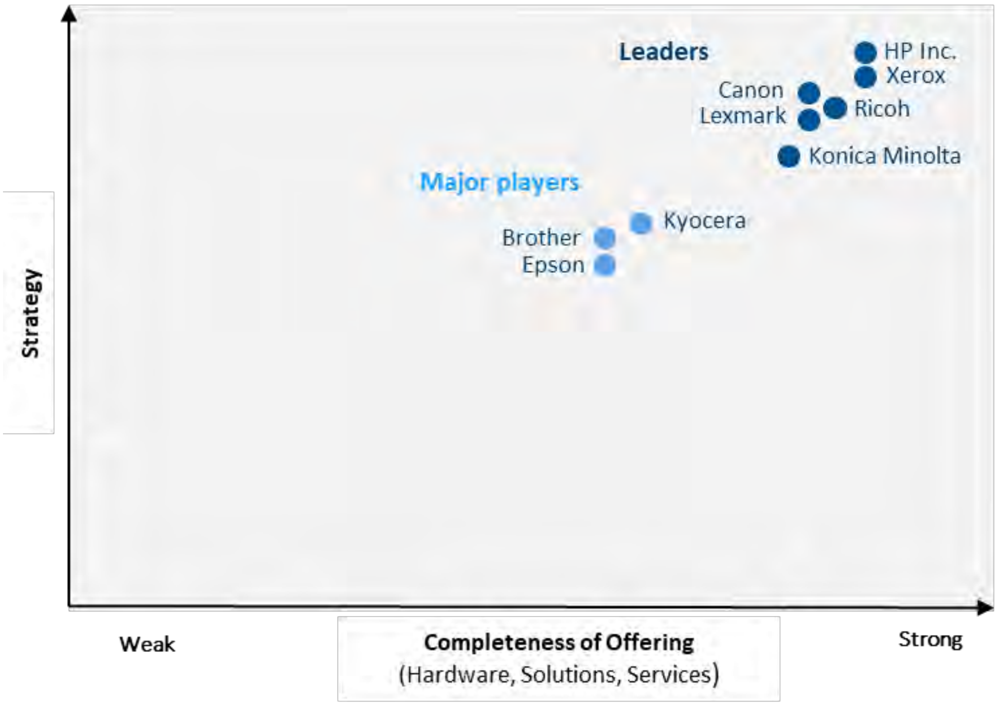

Figure 22. Quocirca Print Security Vendor Landscape, 2022

Vendor Profile: HP Inc.

Quocirca opinion

HP has reinforced its leadership in the print security market by drawing on its strong technology heritage and ongoing commitment to security innovation to address today's growing threat landscape. Security is fundamental across all HP's offerings that cover consumer, SMB, enterprise and graphics/specialty (Large/Wide Format, Indigo, Scitex, and 3D products as well as its personal systems and collaboration portfolio). Over the past year, the company has invested heavily in elevating its proposition with HP Wolf Security. Today, HP Wolf Security provides the most comprehensive suite of hardware, software and services in the market, across both PC and printing. All this is backed by one of the strongest print security-focused direct and channel programmes in the market, one that enables HP and channel partners to build security practices and deliver secure print environments for their customers.

Key to its approach are three main focus areas - building a secure foundation with hardware-enabled protection; delivering proactive support against cyber threats; and providing advanced solutions to build resiliency to stay ahead of security threats in the era of hybrid work. Leveraging security innovation from HP Labs, HP is continually monitoring the threat landscape and building a multi-layered technology portfolio to address the risks of the growing attack surface. Notably, HP has incorporated zero trust principles into its HP Wolf Security proposition which provides integration with the broader security stack and combines hardware security features with endpoint security services. This demonstrates HP's comprehensive understanding of the distributed, complex and heterogenous nature of today's corporate infrastructure environment.

HP excels in the depth and scale of its security services and solutions which support multivendor environments. This enables businesses of all sizes and all industries to build cyber resilience with the use of secure hardware, remote monitoring tools and solutions that protect document security.

HP continues to outperform its competitors in brand awareness in Quocirca's research, with 43% of IT Decision makers viewing HP as having the strongest print security offerings in the market. This is testament to the company's longevity in the market and its maturity of offerings. HP's successful Wolf campaign has been key to driving broader industry awareness of print security vulnerabilities and risks, and HP continues to educate the market beyond traditional IT and security professionals, targeting messaging at individuals in roles such as procurement and general office workers.

Key security highlights

Innovation and technology led security expertise
HP continues to innovate across its security portfolio, displaying a strong commitment to deepening its cybersecurity expertise and resources. Notable hardware features include self-healing firmware and in-memory breach detection along with built-in BIOS protection. This is further enhanced by unique initiatives such as HP's Bug Bounty programme, and cloud-based data intelligence to support ongoing cyber resilience. HP's commitment to staying ahead of the threat landscape is evidenced by the HP Security Advisory Board (SAB) which leverages access to security experts and ethical hackers.

HP fully leverages its research arm, HP Labs. Its Malware Lab in Bristol studies the behaviour and methods of malware. The Bristol Lab originated Network Behavioural Anomaly detection – which was found by examining malware and identifying what it typically does once it attacks a device. For instance, HP printers' closed system structure will see a spike in DNS packets as the malware tries to phone home. HP's devices will reboot themselves to a known good condition and flush memory of the attack.

Multi-layered endpoint protection with HP Wolf Security
Built on over 20 years of security research and innovation, along with strategic acquisitions, HP Wolf Security unifies all of HP's endpoint security innovations under one banner, spanning Print, PC, consumer, commercial and future ventures.

Rooted in Zero Trust principles, the breadth and scale of the HP Wolf Security programme for hardware, services and solutions is currently unmatched in the industry. Its hardware-enforced security covers device hardware and supplies as well as document and data protection.

HP Wolf Security solutions can self-monitor and self-heal from the ground up while providing remote management capabilities to enable total visibility. This enables Cybersecurity teams to proactively mitigate the impact of threats below, in, and above the OS, while remaining transparent to the user. HP uses secure coding, development, testing and certification best practices including Common Criteria Certification, NIST, OWASP (Open Web Application Security Project) profiles and SSDL (Secure Software Development Lifecycle) practices for firmware, software, and cloud.

Utilising best practices in supply chain security was validated recently in an announcement of 3rd party certification that HP is compliant with ISO 20243. This certification validates that product security and integrity is maintained at each point during the product lifecycle, including design, sourcing, building, testing, manufacturing and distributing of HP printers and cartridges. Validation was received that all the stages of a product's lifecycle adhered to security best practices – this is important as one weak link in the product lifecycle chain can compromise security.

Advanced security assessment services

HP offers advanced security assessment services, delivered by credentialed print security advisors and trained print specialists through MPS engagements. HP Secure MPS includes advanced secure professional services, software solutions and expanded core delivery capabilities for customers' multi-vendor print fleets. Its commitment to enabling deeper security assessments through a suite of advanced security assessment services is a strong differentiator in the market.

Security assessment services include:

- **Print Security Advisory Service:** HP Print Security Advisory Service can help customers develop a cohesive printing security strategy to protect their business. In-house certified security specialists work directly with customers and channel partners (in addition to certified channel partner team members where appropriate) to deliver the industry's comprehensive print security assessments, security service plans and recommendations for remediation of risky practices and vulnerable devices.
- **Print Security Implementation Services:** The implementation of risk mitigation recommendations from the Print Security Advisory Service: Enables users to deploy security settings, add security enhancements like device certificates and integrate printers into SIEM tools.
- **HP's Security Advisory Retainer Service:** This provides ongoing security expertise, periodic risk profile updates and support.
- **HP Print Security Governance and Compliance Service:** Trained experts to monitor and manage print security compliance in addition to alignment with global security and regulatory frameworks.

Channel-led security offerings

Through the HP Amplify Program, HP has one of the broadest ranges of channel training programmes for security. With the channel critical to its success, HP heavily invests in its channel with educational programmes, certifications, social media, communications, and resources. HP reports that to date, the number of trained partners is over 5100, and this is expected to double in the next year. HP offers 10 courses across most of its major markets, with dealer education programmes that span both its computing and print business. Beyond its Security Certification Training, which includes a free online security assessment tool for certified partners, HP offers Security Sales Action Plan – a sales enablement guide that simplifies security for channel partners and provides a blueprint to develop and evolve their security practice. HP's Essential Security Policy Assessment Tool which covers 15 security configurations, is free as a MS SCCM plug-in, Smart Device Services software, HP Action Center, and HP Security Manager.

The Channel Partner Security Assessment Tools & Services Sales Action Plan are key differentiators for HP. They have simplified and scaled the ability for channel partners to provide their own branded security assessment services. Once Security Certified (Technical and Sales tracks) by HP, channel partners can use free print security assessment tools and Security Sales Action Plan resources to engage with customers.

Enhanced hybrid workplace security

Remote working enforced by the global pandemic saw HP respond to demand with extension of the security perimeter to the home office. The HP Flexworker Service enables companies to deliver printers with embedded device security to be shipped directly to remote workers and securely connect to the cloud for monitoring, data collection and automatic supplies replenishment. HP has expanded Security Advisory Services to include recommended security settings for remote and home workers as well as security training and guides. HP recently launched the industry's first device-to-cloud security compliance monitoring and remediation service for consumer printers.

Document security

HP offers several options for authentication, job accounting, and pull-print solutions. This includes HP Secure Print, a flexible solution that supports all network types, whether a traditional corporate network behind a firewall or a zero-server print infrastructure environment. HP Secure Print includes HP Insights, a comprehensive print analytics solution that allows you to track and gather print user data, analyse the results, and create reports to continually optimise your print environment and improve efficiency.

Cloud print security underpinned by zero trust

HP Managed Print Cloud Services allows customers to leverage HP's security innovation while maintaining control and flexibility around how the service is shaped. The offering addresses both trusted and zero-trust cloud environments and is delivered through a well-defined, modular approach with flexible services and software stacks to meet the needs of customers wherever they are in their cloud journey.

Industry-leading bug bounty programme

HP launched the industry's first print security bug bounty programme in 2018 and has engaged in several programmes to complement and extend its own rigorous penetration and vulnerability testing over the years. It has now expanded this initiative to focus specifically on office-class print cartridge security vulnerabilities. HP's position is that security features need to go beyond the hardware and include the cartridge for an end-to-end secure system that protects both the network and information. This latest move underscores its commitment to mitigating risk across all aspects of printing - including supply chain, cartridge chip and packaging, firmware, and printer hardware.

Security products and services portfolio

Hardware

HP Wolf Security is segmented into HP Wolf Essential Security (Consumer market), HP Wolf Pro Security (SMB & Mid-Market) and HP Wolf Enterprise Security (Enterprise). Depending on the model, HP printers include a range of security features. HP Managed and Enterprise models can self-heal from an embedded "golden copy" of the BIOS with unique security features including run-time intrusion detection (Common Criteria Certified), HP Sure Start BIOS protection (NIST 800-193 Compliant), whitelisting (Common Criteria Certified), HP Connection Inspector and HP validated cartridge security.

Key features include:

- **HP Sure Start.** In reboot, HP Sure Start detects and prevents the execution of malicious code and self-heals the BIOS. If a compromised version is discovered, the device restarts using a safe "golden copy" of its BIOS.
- **Run-time intrusion detection.** Memory activity is monitored in real time to continually detect and stop attacks. It is Common Criteria Certified to check for anomalies during complex firmware and memory operations, automatically stop intrusions, and reboot to heal itself.
- **HP Connection Inspector.** Evaluates outgoing network connections to determine what's normal, stops suspicious requests and automatically triggers a self-healing reboot.

- **Whitelisting.** Helps ensure only authentic HP code is loaded into memory and notifies IT if compromised. Firmware is automatically checked during startup, and if an anomaly is detected, the device reboots to a secure, offline state and notifies IT.
- **Secure cartridges.** Security is built-in with tamper-resistant chips, firmware and packaging.
- **HP Roam for Business.** Replaces traditional, printer-specific drivers with an intuitive mobile print experience that is simple to use, scalable and provides a secure printing experience consistent across desktop and mobile devices. Customer and company data are protected by advanced security features such as encryption, authentication, and integration with identity providers including Azure Active Directory.
- **HP Advance.** A highly scalable print management software suite that enhances security through user authentication, secured mobile printing and streamlined output management and digital processes. Increases workflow efficiencies and reduces costs; multivendor capabilities.
- **HP Security Manager.** Helps streamline security by establishing a single policy and quickly applying it across the entire HP printing and imaging fleet, discovering and securing newly added devices to the customer network via Instant On technology. Automates certificate deployment and provides compliance reporting. HP Security Manager includes firmware vulnerability assessment. Also works for select Zebra (automated certificate management coming soon) and Samsung devices.
- **HP Access Control secure pull print.** This server-based pull print software solution can be set to require all users to authenticate before retrieving a print job.
- **HP Secure Print.** Designed to keep data, devices, and workflows secure using the latest security standards:
  - Data is encrypted at rest using AES-256 and in transit with TLSv1.2 using SHA-256
  - Printer network traffic is encrypted using IPPS
  - Print jobs remain inside the customer network with the on-premises job storage option
  - Printers can be secured by IP address or network name
  - User identity information (card number, user PIN) is hashed as a one-way, non-reversible value
  - Cloud-native architecture allows quick deployment of new features and updates
- **SIEM integration.** McAfee, SIEMonster, ArcSight, Splunk or IBM QRadar.
- **Authentication.** HP Universal Print Driver and HP Access Control (for PC network printing), and HP JetAdvantage Connect and HP Access Control (for mobile users) require users to enter a password or PIN, scan their badge, or fingerprint. Mobile phone authentication for enterprise-class printers.
- **HP Workpath apps.** Supports existing authentication methods, such as a proximity card, on any device in the fleet while user IDs/passwords are not stored.
- **Universal print driver.** Includes a secure encrypted printing feature for sensitive documents. It allows users to send a print job to be held until they release the job via a PIN at the device.
- **Proximity card reader.** Users can quickly authenticate and print securely at a printer or MFP via an existing ID badge.
- **Security action plan and assessment tools.** Security Sales Action Plan, SMB Assessment Questionnaire, FW Vulnerability Assessment, Quick Assess and HP Hack Demo Videos. Significant support will be provided for channel partners with these tools, and associated channel partner security certification programmes.
- **Security services.** HP Print Security Advisory Service, HP Print Security Implementation Service, HP Print Security Governance and Compliance Service, HP Print Security Advisory Retainer Service. Custom consulting services are also available.
- **HP Secure Document Management and Monitoring.** Supports both Data Loss Detection and Data Loss Prevention use cases by mitigating threats inside or outside of a customer's organisation, such as the intentional or unintentional release of sensitive documents or information. Allows the customer to see every document that is printed, copied, scanned or faxed and allows for discovery alerts to notify authorised users when keywords or phrases are found.
- **HP Managed Print Cloud Services (MPCS).** MPCS is designed to be an HP-managed service that includes cloud infrastructure management with cloud providers AWS or Azure, software management of select applications, and a standard set of services. MPCS provides a global, always-on print environment with layered security designed for each client's unique business needs. With minimal need from IT

personnel, customers can shift their focus to what they do best and lower their overall print spend with a solution that expands or contracts as the business evolves.

- **Microsoft Universal Print.** HP's strategic relationship with Microsoft advances its ability to enable a better, more intuitive, and secure print experience for users, natively integrated with Microsoft 365, while helping IT reduce time and effort. As an industry leader and innovator in the technology standards that Universal Print is built on (IPP), HP is working with Microsoft to build a cloud-to-cloud integration with Universal Print and the HP Managed Print Cloud Services platform. Through this collaboration, organisations will be able to increase security of documents and data, streamline the management of their devices, and limit print jobs to authorised users.
- **HP and Troy MICR printers.** Fraud and counterfeit deterrent solutions. Unique relationship spanning 26 years leverages HP and Troy technologies and services to enable secure cheque, prescription and other sensitive document printing.
- **Bug bounty programme.** Industry-first printer bug bounty programme now extended to uncover print cartridge security vulnerabilities and a broader range of devices.

About Quocirca

Quocirca is a global market insight and research firm specialising in analysing the convergence of print and digital technologies in the future workplace.

Since 2006, Quocirca has played an influential role in advising clients on major shifts in the market. Our consulting and research is at the forefront of the rapidly evolving print services and solutions market, trusted by clients who are seeking new strategies to address disruptive technologies.

Quocirca has pioneered research in many emerging market areas. More than 10 years ago we were the first to analyse the competitive global market landscape for managed print services (MPS), followed by the first global competitive review of the print security market. More recently Quocirca reinforced its leading and unique approach in the market, publishing the first study looking at the smart, connected future of print in the digital workplace. The Global Print 2025 study provides unparalleled insight into the impact of digital disruption, from both an industry executive and end-user perspective.

For more information, visit www.quocirca.com.

Disclaimer:
This report has been written independently by Quocirca. During the preparation of this report, Quocirca has spoken to a number of suppliers involved in the areas covered. We are grateful for their time and insights.

Quocirca has obtained information from multiple sources in putting together this analysis. These sources include, but are not limited to, the vendors themselves. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in any information supplied.

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.

All brand and product names are trademarks or service marks of their respective holders.