

The Print Security Landscape, 2020



Executive Summary

As cyberattacks continue to increase, capitalising on the new vulnerabilities of remote working, securing the print infrastructure – across the office and home environments – must be a strategic priority. Quocirca's Print Security Landscape 2020 study reveals increasing concerns around the risks of printing, and declining confidence in the ability to protect the print infrastructure against security breaches. The attack surface has now expanded to encompass remote endpoints such as home printers, which may fall through the gap of traditional print security measures.

This heightened exposure to possible data loss is leading organisations to lose confidence in the security of their print infrastructure. Just 21% of IT Decision Makers (ITDMs) say they are completely confident, compared to 33% prior to the COVID-19 pandemic. In the past six months, 64% have reported a data loss as a result of unsecure printing practices, with reasons ranging from improper disposal of confidential information by employees to device malware. This is leading to an average cost of a data loss reaching £1.2 million in the US and £825,000 in Europe, significantly higher than in 2019. This can be attributed to the likelihood that organisations are improving their capabilities around detecting and reporting on data losses.

Despite the significant levels of data loss and associated cost, ITDMs still place print security much lower on the IT security agenda. While email, networks and cloud are ranked in the top three, securing printing is in seventh place. With 77% of ITDMs indicating that printing will remain critical (29%) or very important (48%) to their businesses in the next 12 months, organisations cannot afford to be complacent.

While many are implementing a range of measures such as risk assessments, pull-printing, analytics and content security, adoption varies widely by region. According to Quocirca's Print Security Maturity Index, based on the number of measures implemented, just 19% of organisations are considered Print Security Leaders. This rises to 28% in the US and falls to 12% in the UK and Germany. Print Security Leaders are more likely to spend more on print security and report higher levels of confidence.

Adapting to any crisis requires action. As remote working becomes a permanent feature for many organisations, ITDMs cannot ignore the potential threats and vulnerabilities from printing in the home environment. As more organisations turn to a zero trust model to enforce more stringent access controls both inside and outside the network perimeter, the print infrastructure must adapt accordingly. The hybrid workplace is here to stay and it is imperative that organisations mitigate the risk of data loss by protecting printing endpoints in both the home and office environments.

This study is based on the views of 508 IT Decision Makers (ITDMs) in the US and Europe. The report also includes detailed profiles of print security offerings from the major print manufacturers and key ISVs. The following vendors participated in this study:

Manufacturers: Brother, Canon, HP, Konica Minolta, Lexmark, Ricoh, Xerox

ISVs: EveryonePrint, LRS, MPS Monitor, PaperCut, Pharos, Printix, Ringdale, Y Soft

Table of Contents

Executive Summary	2
Key findings.....	5
A year of pandemic-driven change.....	6
Remote working is here to stay	6
The cloud-enabled business.....	7
Printing moves to the cloud.....	8
Shifting IT investment priorities.....	8
Organisations will continue to rely on printing.....	10
Print security is low on the IT security agenda.....	11
Complacency or lack of awareness?	12
Taking measures to address print security	12
Print security spend set to increase over next 12 months.....	12
Organisations adopt a range of print security measures	13
The Quocirca Print Security Index	15
Declining print security confidence	16
Print-related data losses.....	19
Supplier choice and satisfaction.....	21
Buyer Recommendations.....	22
Conclusion – dealing with permanent change	23
Vendor Profiles – MPS Monitor	24
Appendix 1: Demographics and research process.....	26
About Quocirca	27

Table of Figures

Figure 1. Average percentage of workforce working fully or predominantly from home	6
Figure 2. To what extent is cloud computing used to support overall IT requirements?	7
Figure 3. Cloud print service adoption.....	8
Figure 4. Top technology investments for the next 12 months (Top 3 selected)	9
Figure 5. The importance of printing to businesses	10
Figure 6. Expected change in print volumes over next 12 months	10
Figure 7. Which of the following areas pose the greatest security breach risk?	11
Figure 8. Expected print security spend over next 12 months.....	13
Figure 9. Print measures already implemented	14
Figure 10. Quocirca’s Print Security Index.....	15
Figure 11. Concerns with home and office print security.	16
Figure 12. Confidence in print security (office and remote workplace).....	17
Figure 13. Confidence in print security (By Region)	17
Figure 14. Impact of print security index on print security confidence	18
Figure 17. Data loss by print environment	19
Figure 18. Estimated average cost of a data loss.....	20
Figure 19. Satisfaction levels.....	21
Figure 20. Supplier choice for print security.....	21

Key findings

- **COVID-19 has accelerated the move to remote working and cloud computing.** Before the pandemic, an estimated 39% of employees worked from home all or part of the time; this is expected to rise to 48% after offices fully reopen. The crisis has also embedded confidence in the use of cloud services – 34% of organisations are currently using cloud for all their IT requirements, rising to 43% of organisations by the end of 2021.
- **IT security remains the top investment priority over the next 12 months.** 67% of ITDMs say IT security is one of their top three investment priorities. Cloud is second in importance (44%) followed by managed IT services (42%) and managed print services (35%). Today 63% of organisations are using an MPS, while half report that they are using a Cloud Print Service.
- **An ongoing reliance on printing creates the need for effective print security.** 28% of organisations indicate that printing will be critical to their business in the next 12 months. Once offices reopen, 73% expect home printing volumes to increase, with 59% anticipating that office printing volumes will do likewise. As the hybrid workplace evolves to encompass both home and office printing, ITDMs need effective print security tools in place to minimise the risk of this expanded threat landscape.
- **Adoption of print security measures varies widely by region.** The most commonly implemented measure is a formal procedure for responding to print security incidents (48%). 43% of ITDMs have revised their BYOD policy for home printers; this is most likely to be the case in the US (48%) and least likely in the UK (33%). Pull printing, where output can only be released to authenticated users, is least common in France. Overall, 34% of organisations overall have adopted a zero trust model, rising to 44% in the US.
- **According to Quocirca's Print Security Maturity Index, only 19% of the organisations can be classed as Print Security Leaders.** These organisations have implemented six or more security measures, and report higher levels of confidence in the security of their print infrastructure. This rises to 28% in the US and falls to 12% in the UK and Germany. Print Security Leaders are more likely to spend a higher amount on print security and report higher levels of confidence.
- **Confidence in how well the print infrastructure is protected against security breaches has decreased since the onset of COVID-19.** Prior to the pandemic, 33% of ITDMs said they were completely confident, compared to 21% now. The steepest drops are in the US (50% to 33%) and the professional services sector (43% to 27%).
- **In the past six months two thirds of organisations have experienced data losses due to unsecure printing practices.** This rises to 74% in the US and drops to 57% in Germany. This has led to a mean cost per data breach of £1,023,168 (£1,238,411 in US and £825,243 in Europe). SMEs are more likely to have suffered a print-related data loss in the past six months (69%), with professional services the most affected sector.
- **Just over a third (37%) of ITDMs are very satisfied with their suppliers' print security capabilities.** This drops to 31% amongst SMEs, and 23% within the public sector. Just 18% of organisations in Germany are very satisfied, compared to 55% in the US. Notably, just 17% of ITDMs overall would turn to an MPS provider for print security guidance, while 23% would consult a print manufacturer.
- **Almost 40% turn to Managed Security Service Providers (MSSPs) for print security advice.** 37% indicate that MSSPs are their primary source of guidance, rising to 45% in the US and 40% among SMEs. 23% would turn to a print manufacturer and 17% would consult an MPS provider. This points to an opportunity for MPS providers and channel partners to collaborate more strongly with MSSPs.

A year of pandemic-driven change

Both the private and public sectors have demonstrated flexibility and resilience in maintaining operations in the face of disruption. COVID-19 has driven organisations to fast-track their adoption of new technologies to support the almost overnight shift to remote working. Flexible workplace arrangements supported by cloud-based services and remote access have become a must-have, with technology rollouts taking just days rather than weeks or months.

Remote working is here to stay

Before the pandemic, an average of 39% of employees were working fully or predominantly from home. This is expected to rise to almost half (48%) once offices fully reopen (Figure 1). Pre-COVID, 51% of the US workforce worked from home on average, compared to 27% in Germany. France is expected to see the highest increase in working from home, from 30% to 43%. On average, 48% of those in business and professional services were working from home, compared to just 27% in the public sector. When offices reopen, retail is expected to see the highest increase in employees working from home, from 29% to 44%.

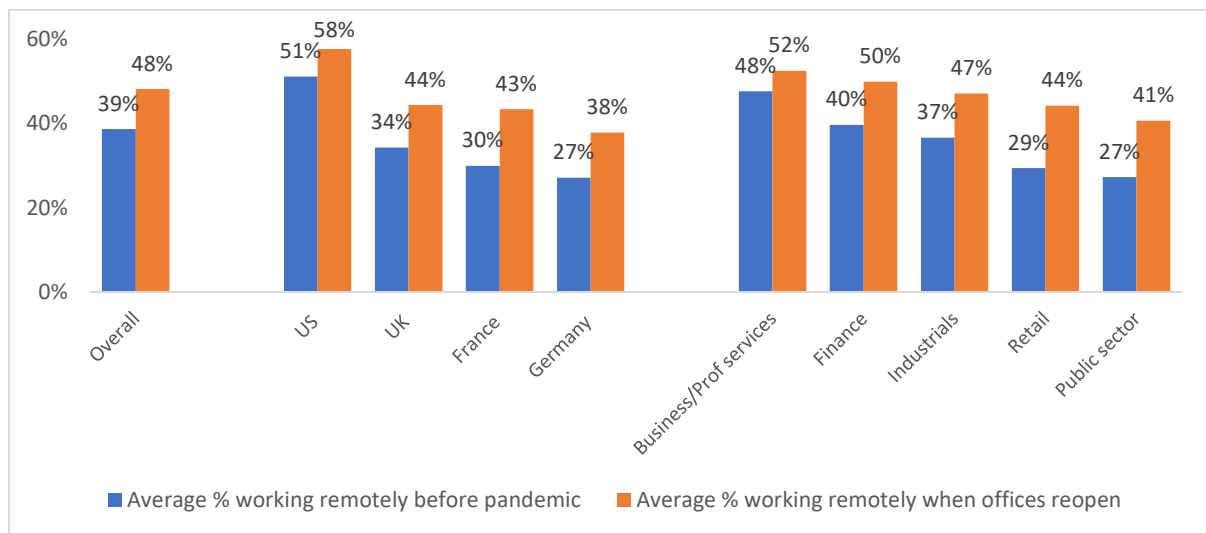


Figure 1. Average percentage of workforce working fully or predominantly from home

The cloud-enabled business

The pandemic has accelerated the uptake of cloud services, especially those that enable remote collaboration such as Zoom and Microsoft Teams. The resilience of cloud services throughout the crisis has increased confidence where there was hesitation before. More than a third (34%) of organisations now use cloud for all their IT requirements, with 43% expecting this will be the case by the end of 2021 (Figure 2).

The figure is highest in the US where 46% of organisations already use cloud for all IT requirements, well ahead of Europe, where the figure for Germany is just 22%. Use of cloud services for all IT requirements is set to surge from 21% to 43% in retail, and from 32% to 46% to the industrial sector over the next 12 months, while the public sector will lag behind at just 27%.

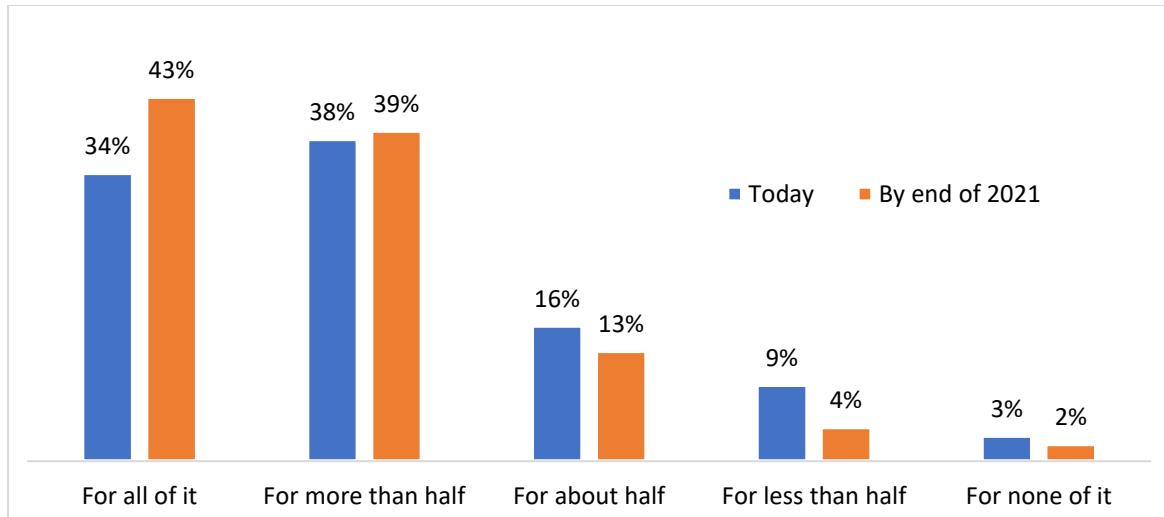


Figure 2. To what extent is cloud computing used to support any of overall IT requirements?

Printing moves to the cloud

Cloud adoption is extending to the print infrastructure (Figure 3). A cloud-based print service enables organisations to eliminate all or some of their on-premises print servers and host them in a cloud environment, which is managed by a third party MPS provider. This reduces IT burden, lowers costs and provides flexibility and scalability to add or remove printers as business needs change. A cloud print service can also help address security concerns by ensuring printing is tracked for both home and office workers.

Cloud print service adoption is highest in the US (57%) and lowest in the UK (40%). Just 33% of organisations in the public sector use a cloud print service, compared to 54% in retail. Adoption is highest in larger enterprises (52%).

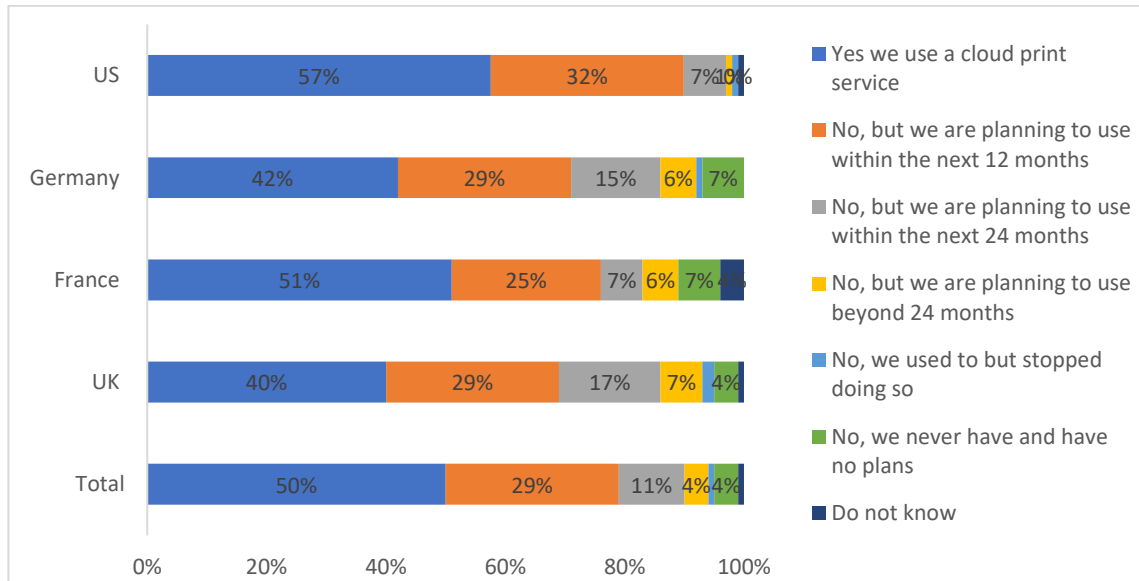


Figure 3. Cloud print service adoption

Shifting IT investment priorities

The pandemic has accelerated the pace of digital transformation, and technology is playing a pivotal role in reshaping business. This is shifting investment priorities over the next 12 months (Figure 4). Above all, organisations are looking to improve cyber resilience and cloud migration.

The top investment priority is IT security, cited by 67% of all respondents, rising to 71% in the US and Germany. This is followed by cloud services (45%) and managed IT services (41%), which will be key to supporting business continuity, particularly for those organisations that lack IT resources. Midmarket organisations (500-999 employees) are more likely to prioritise investment in managed IT services (49%), along with the business/professional services sector (53%). US organisations are most positive about managed IT services, with 54% prioritising investment in these, compared to 29% in France.

Overall, 35% expect that Managed Print Services (MPS) will be a key investment priority over the next 12 months, rising to 45% in France. Certainly, with many organisations potentially looking to operate offices at lower capacity, the need to evaluate current printer fleet deployment and implement solutions that support both office and remote workers will come to the fore.

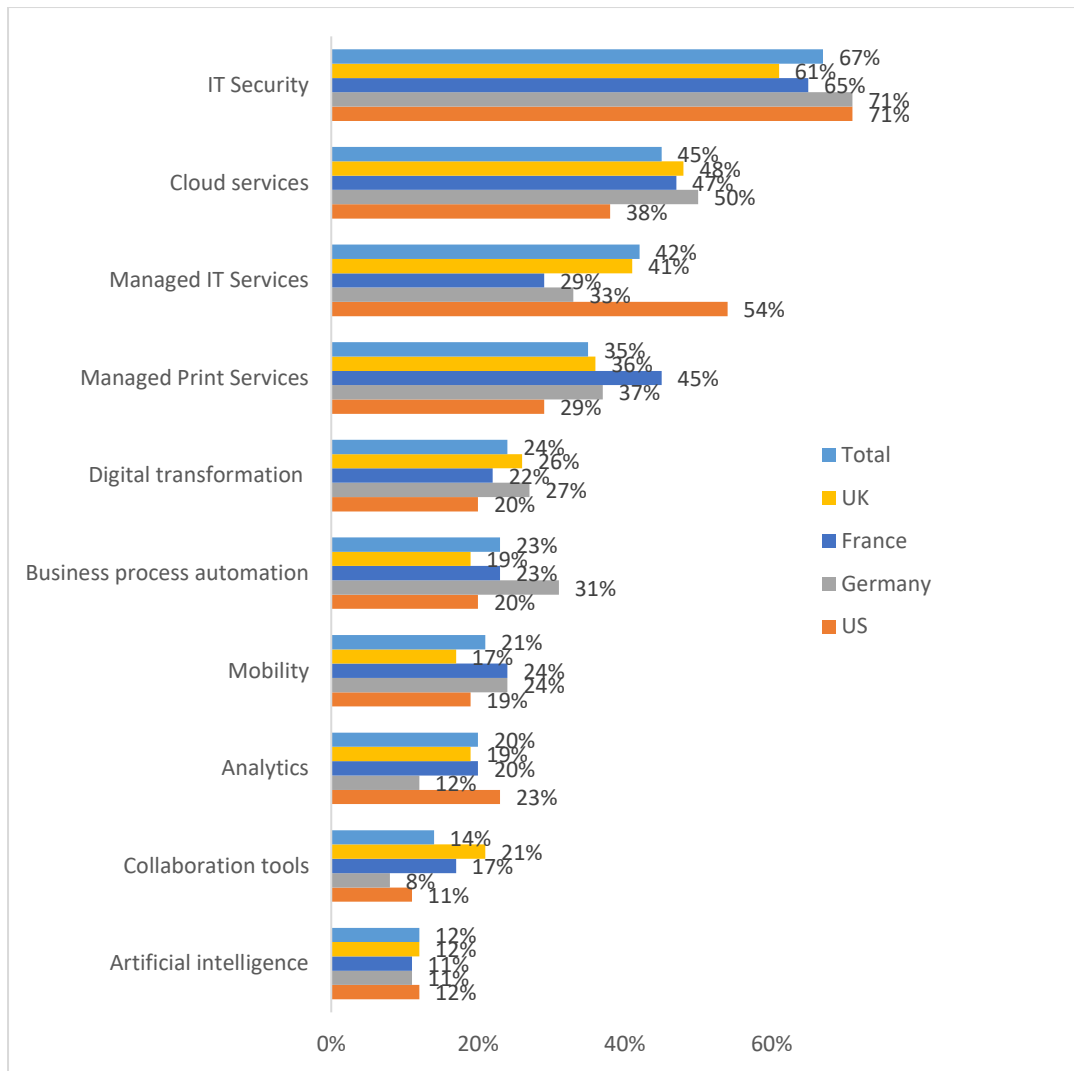


Figure 4. Top technology investments for the next 12 months (Top 3 selected)

Organisations will continue to rely on printing

Despite the increase in homeworking, printing is still critical to 29% of organisations today (Figure 5). Overall 77% indicate printing will be critical or very important to their business in the next 12 months, down only slightly from 83% now. Printing is most likely to be critical to the public sector both now (38%) and in the next 12 months (36%), closely followed by finance, with 36% of respondents saying printing is critical now, dropping to 28% in the next 12 months.

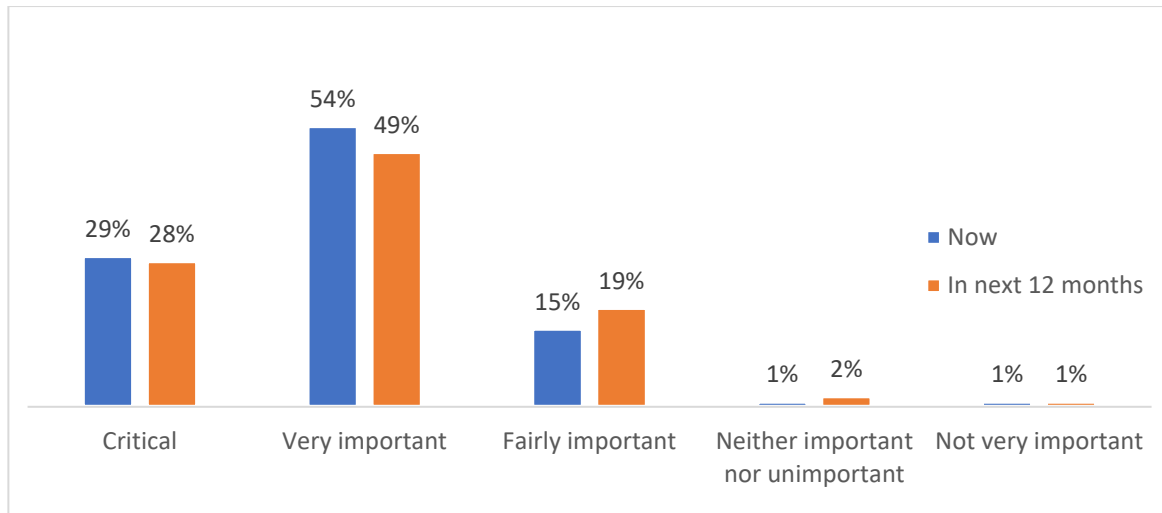


Figure 5. The importance of printing to businesses

While office closures have severely impacted office print volumes, the majority of respondents expect print volumes to increase over the next 12 months (Figure 6). This reflects the situation once lockdown measures are relaxed and employees return to the office – even if it’s on a flexible basis. For many home workers, home printers will not be suitable for the professional quality required or volume of print that is common in the office environment. Overall, three quarters (73%) of ITDMs expect home printing to increase over the next 12 months. More than half (59%) also predict office printing will increase, but 18% anticipate a decrease.

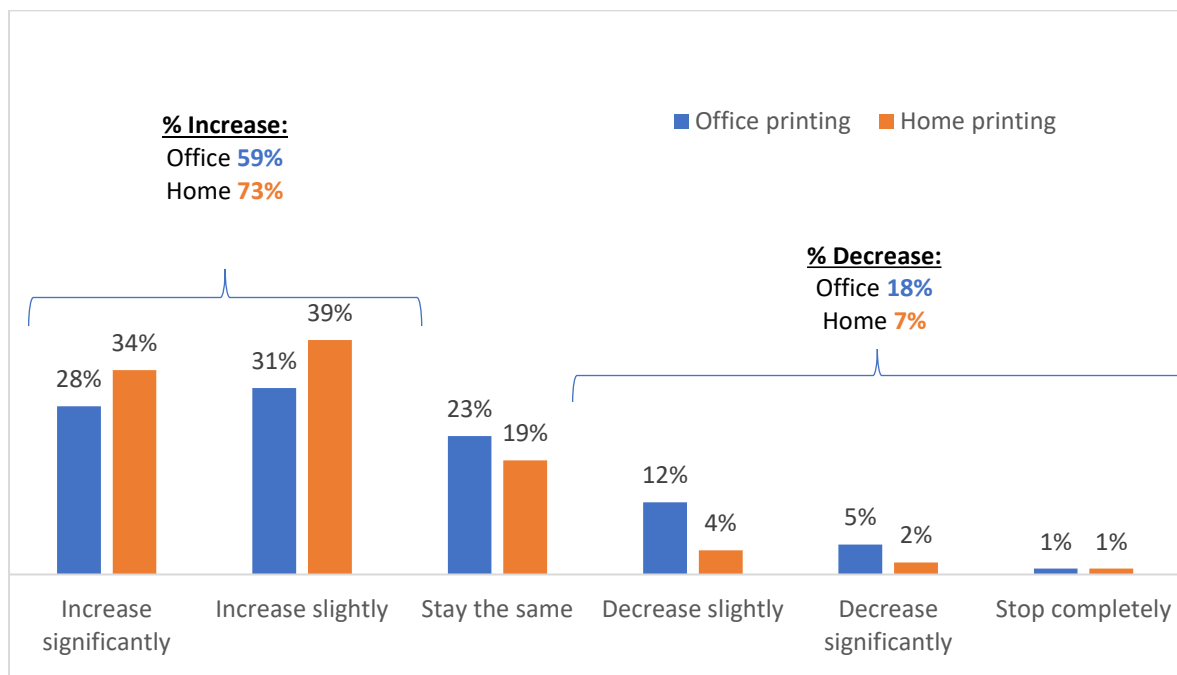


Figure 6. Expected change in print volumes over next 12 months

Print security is low on the IT security agenda

Print security continues to be lower on the security agenda than other elements of the IT infrastructure (Figure 7). The risk from printers is less recognised than other risks, such as email (selected by 44%), networks (41%) and traditional end-points (36%). As a result of this prioritisation, print security may often be neglected and not treated with same urgency as other IT security issues.

Overall 32% of ITDMs consider employee-owned home printers a potential security risk, rising to 39% in the US and dropping to 25% in Germany. Organisations in the US are also most concerned about office print (35%), compared to 19% in France. 37% of respondents from the finance sector ranked office printing as a high risk, compared to just 19% in the public sector.

Smaller companies (250 to 499 employees) are more concerned about employee-owned printers (35%), while concern is highest in business/professional services companies (38%), which are more likely to have employees printing at home. Overall, employer-provisioned devices in the home were considered safest, with just 23% selecting them as a top-five risk. This is likely to be because the employer maintains control of the device, and sensitive print output is less likely to be seen by the wrong eyes in an employee’s home than in an office.

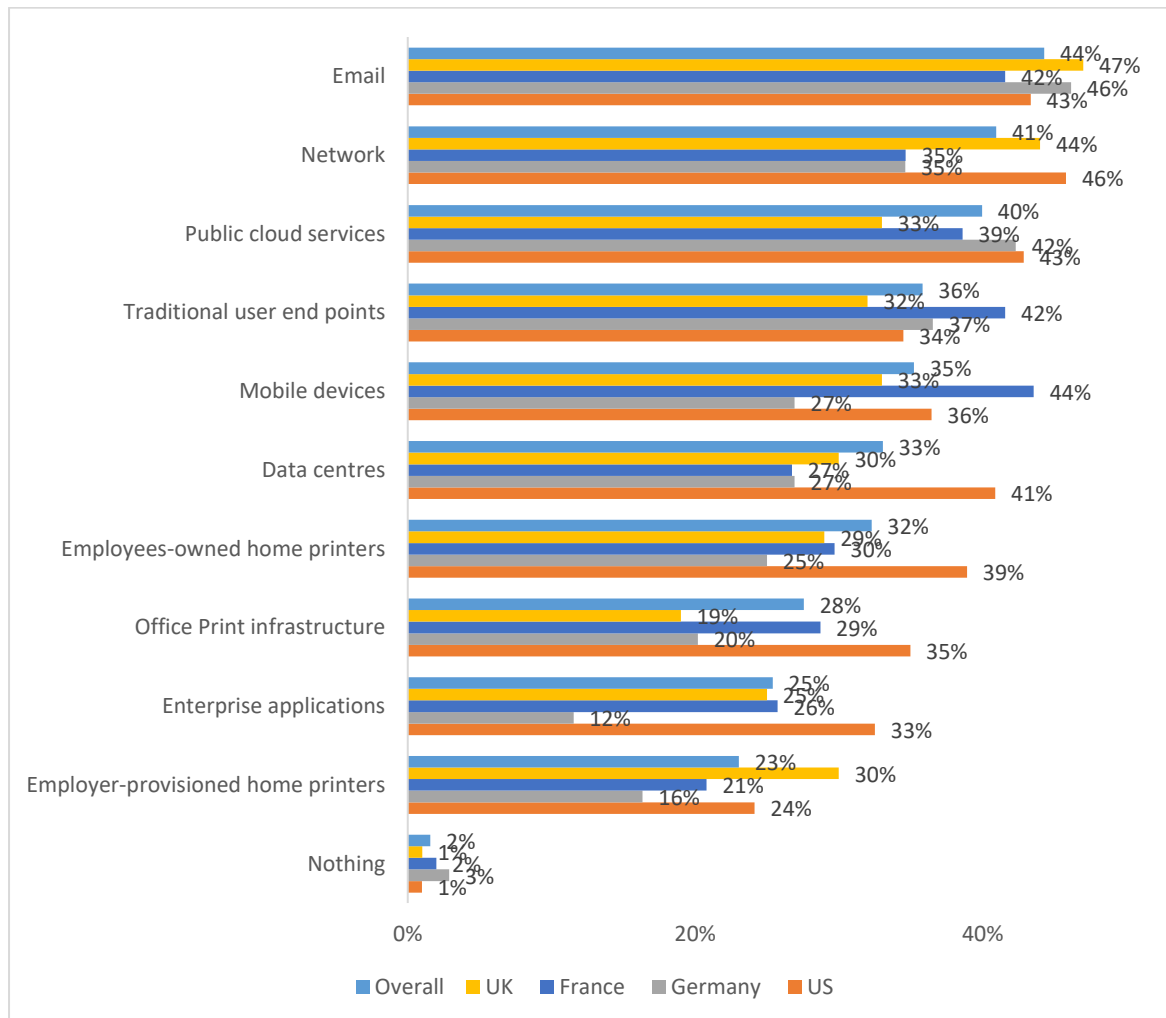


Figure 7. Which of the following areas are considered to pose the greatest security breach risk? (Select up to five)

Complacency or lack of awareness?

Print vulnerabilities

This lower priority applied to printing could either be down to complacency or a lack of awareness of the potential vulnerabilities. However, print infrastructure is vulnerable for several reasons:

- Neglected printers can be easy entry points for deeper network penetration
- Printers themselves can store sensitive information which, if compromised, can be a source of data leaks, although home printers tend not to have their own hard disks
- Print output, if left unattended, is a potential source of data leaks
- Printers have their own processing power and, if insecure, may be recruited to botnets

The risk of home printing

Home printers exacerbate all these problems. They add to the heterogeneity of the overall fleet, they have to be managed remotely and whatever employees do with printed output is beyond the control of the physical environment of an office, where, for example, the disposal of paper can be controlled.

A decision must be made, often on a case-by-case basis as to how home printing is supported. There are three basic options:

1. Block all home printing
2. Provide printers to employees which are owned by the business, and use is limited to these printers whilst other print devices are blocked
3. Support employee-owned printers

Taking measures to address print security

Comprehensive security strategies can help organisations mitigate the risk of data loss through unsecured printing in both the remote and office environment.

Print security spend set to increase over next 12 months

Overall, 78% of organisations expect their print security spend to increase over the 12 months (Figure 8). This rises to 87% in the US and drops to 69% in Germany.

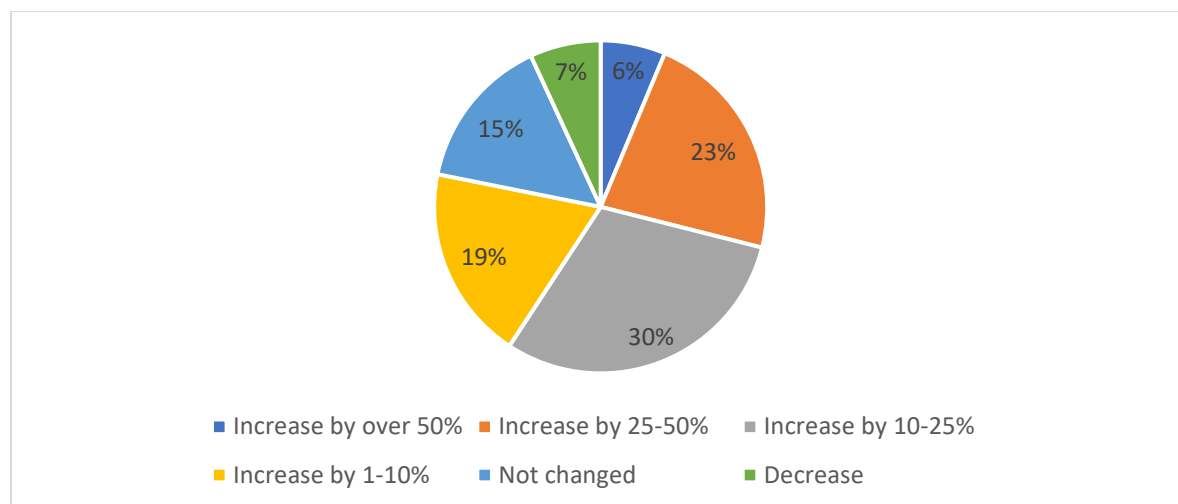


Figure 8. Expected print security spend over next 12 months.

Organisations adopt a range of print security measures

A range of print security technologies and processes are being adopted (Figure 9). The most widely implemented measure is a formal procedure for responding to print security incidents (48%). 43% of ITDMs have revised their BYOD policy for home printers; this is most likely to be the case in the US (48%) and least likely in the UK (33%). Pull printing, where output can only be released to authenticated users, is least common in France.

The finance sector is most likely to adopt a number of print security measures, including those specifically addressing home working; 52% of finance organisations provide printers to home workers compared to 29% in the public sector.

Notably, 42% of ITDMs overall have undertaken print security risk assessments, which are fundamental to evaluating the current print security posture of any organisation. This rises to 49% in the US, but drops to 32% in Germany.

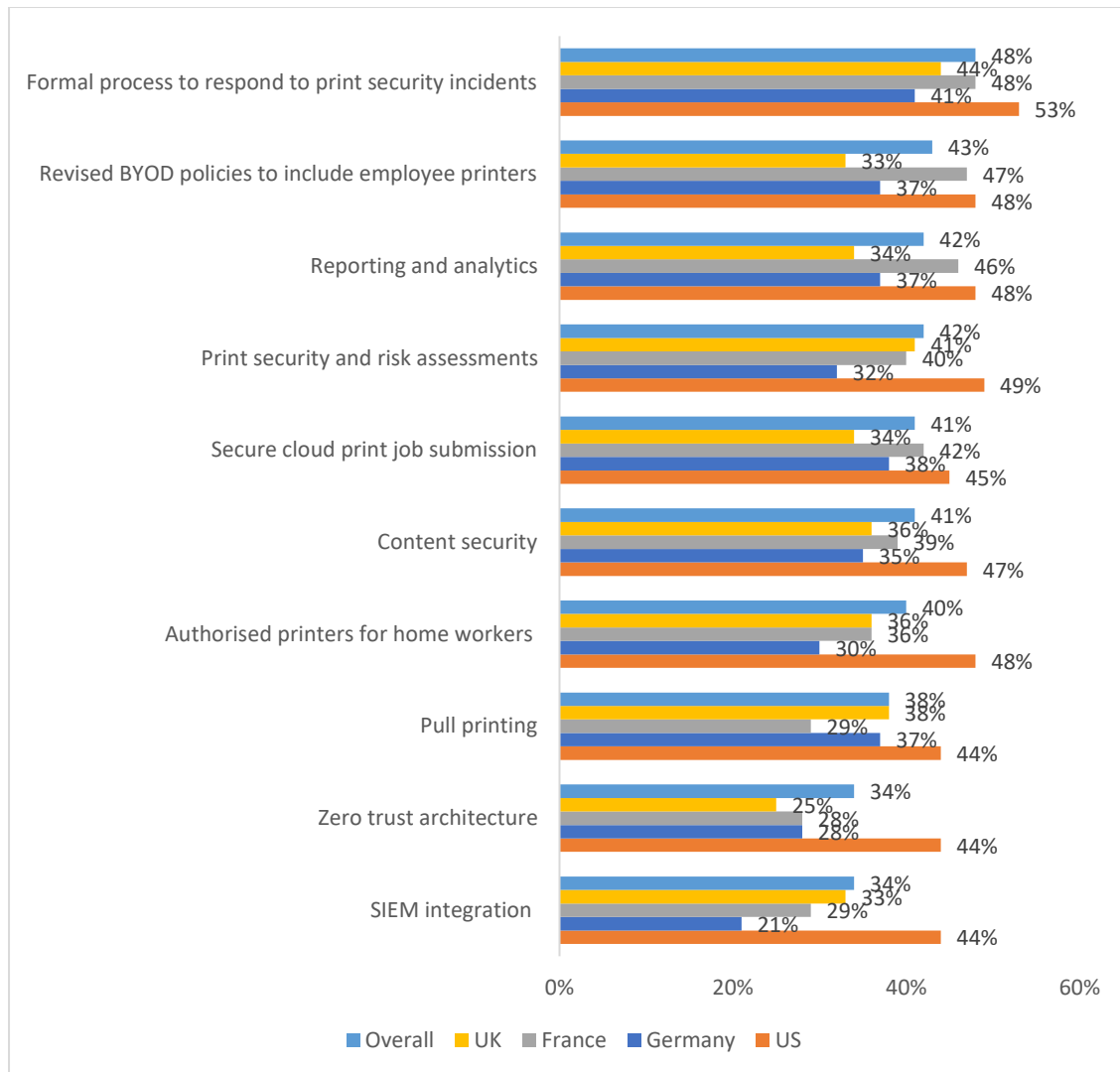


Figure 9. Print measures already implemented

The Quocirca Print Security 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.
- **Followers** have implemented between two and five measures.
- **Laggards** have implemented one or none of the measures.

Overall, just 19% are classed as print security leaders, rising to 28% in the US and 26% in the finance sector. 36% of public sector organisations are qualified as laggards, while only 12% in the UK and Germany are in the leader category (Figure 10).

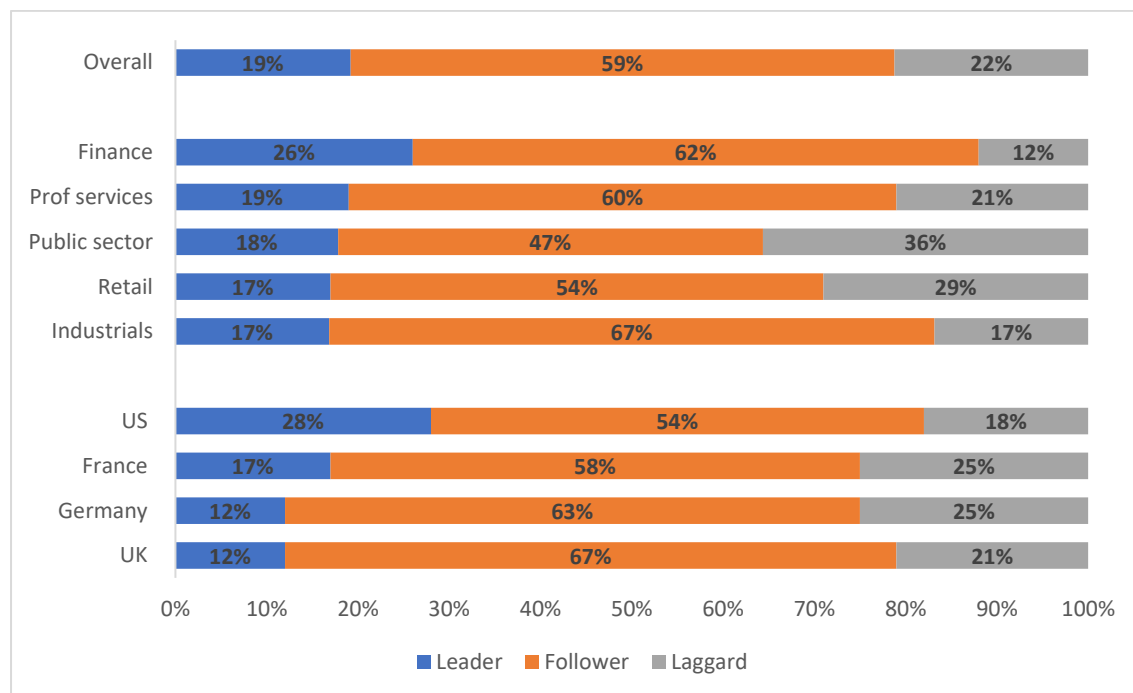


Figure 10. Quocirca’s Print Security Maturity Index

Declining print security confidence

The rapid shift to remote working is undoubtedly increasing the risk of security incidents in general. The attack surface has expanded to include home printers, which are not only often insecure, but also create concerns around how documents are protected in the home environment.

There is certainly more concern around security breaches due to insecure printing practices with home printing (76%) compared to office printing (63%) – Figure 8. ITDMs in the US are most concerned about both office (78%) and home printing (85%), while those in Germany are least concerned (40% and 58% respectively).

71% of ITDMs in business and professional services companies are concerned about office printing security, compared with just 51% in the public sector. CISOs are most concerned about security breaches resulting from office (73%) and home printing (80%), while those in non-managerial IT roles are least concerned (44% and 59%).

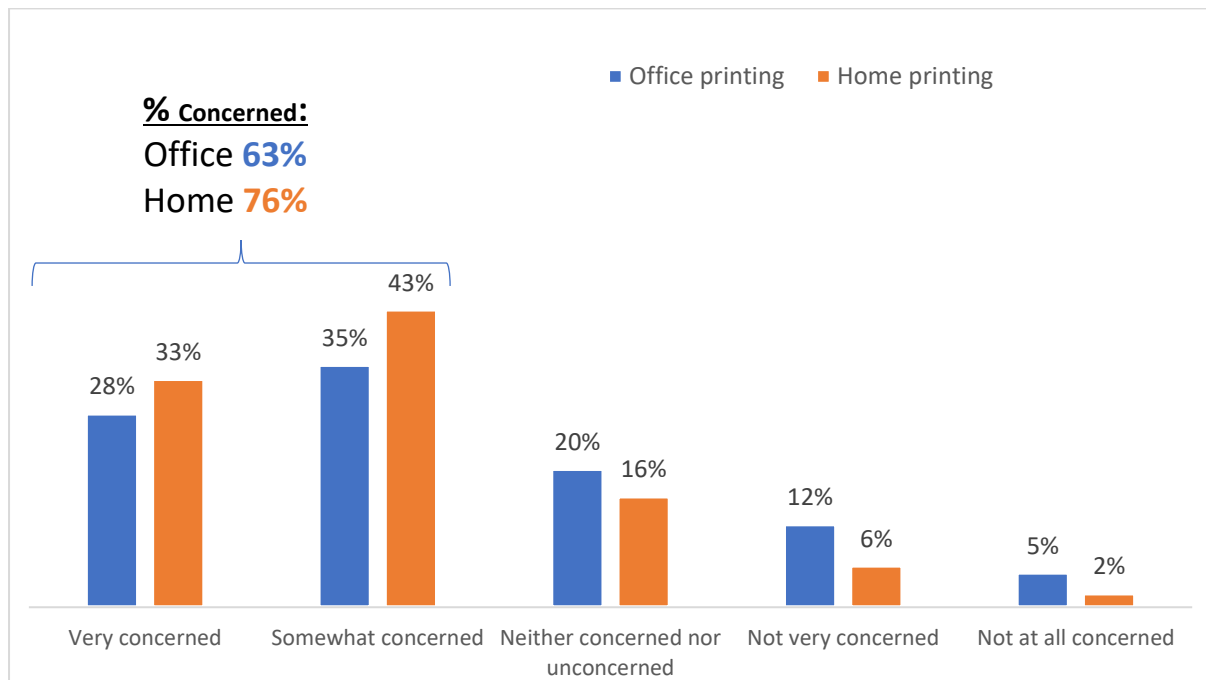


Figure 11. Concerns with home and office print security.

As explained above, print security is lower on the IT security agenda than other elements of the IT infrastructure. This is perhaps the reason behind an overall lack in confidence around how well the print infrastructure is protected.

Before COVID-19 33% of ITDMs were completely confident, compared to 21% now (Figure 12). There have been steeper drops in print security confidence in the US and UK (Figure 13). While 50% of US organisations were completely confident prior to the pandemic, this now stands at 33%. The UK has seen a similar decrease, from 33% to 16%. Those respondents in business and professional services companies are most likely to have been completely confident pre-COVID (43%), and also now (27%), while those in the public sector demonstrate the lowest confidence levels, both pre-COVID (22%) and today (12%).

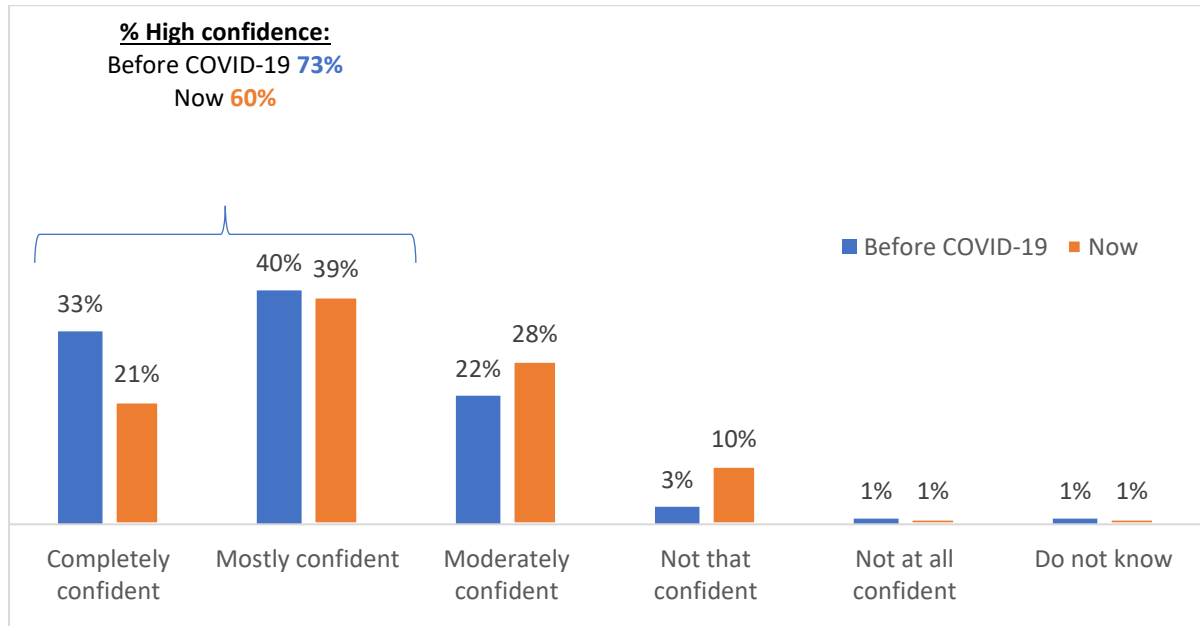


Figure 12. How confident are you that your organisation's print infrastructure (office and remote workplace) was/is protected from security breaches and data loss?

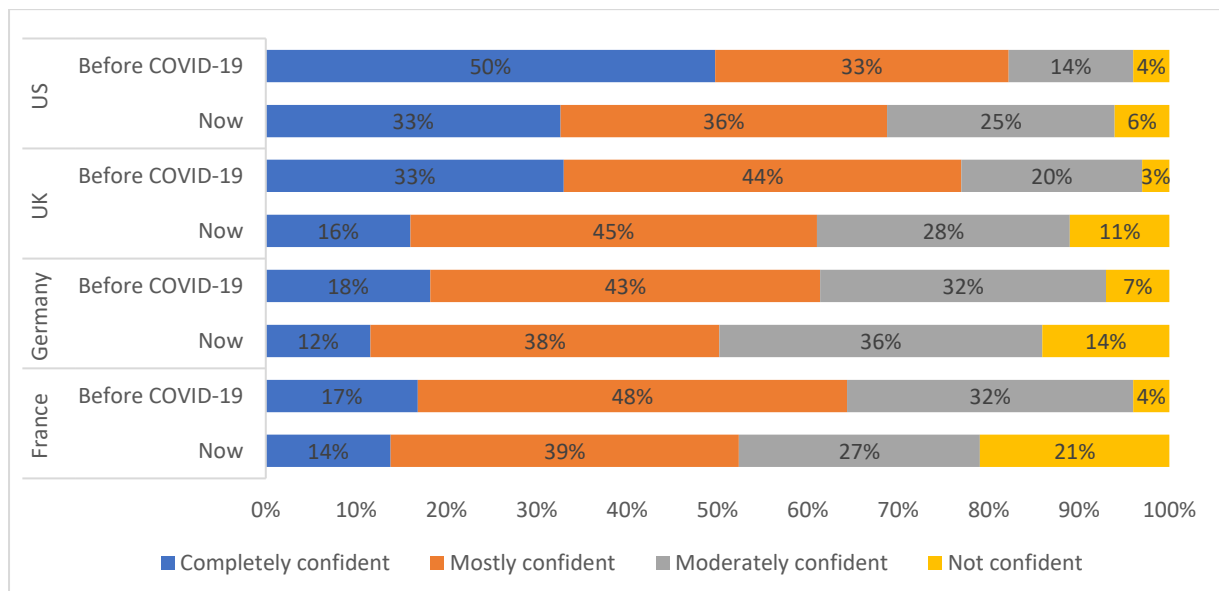


Figure 13. How confident are you that your organisation's print infrastructure (office and remote workplace) was/is protected from security breaches and data loss? (By Region)

Print security leaders report higher levels of confidence (Figure 14). 58% were completely confident before the pandemic and 47% afterwards, while just 18% of followers and 7% of laggards are completely confident in the security of their print infrastructure now.

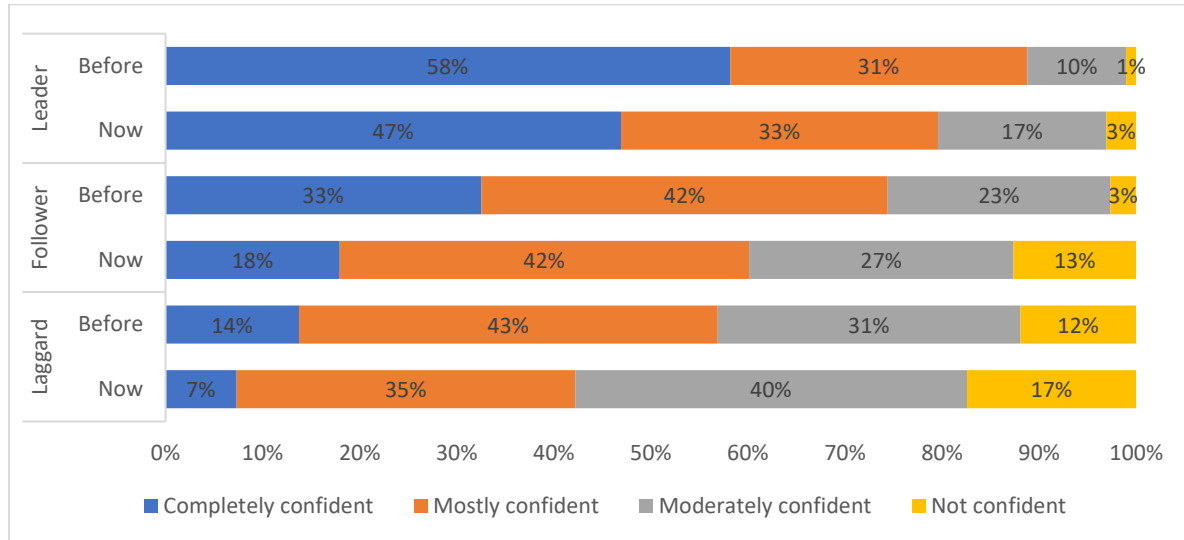


Figure 14. Impact of print security index on print security confidence

Figure 15 illustrates the varying levels of print security confidence by sector, size and industry post-pandemic.

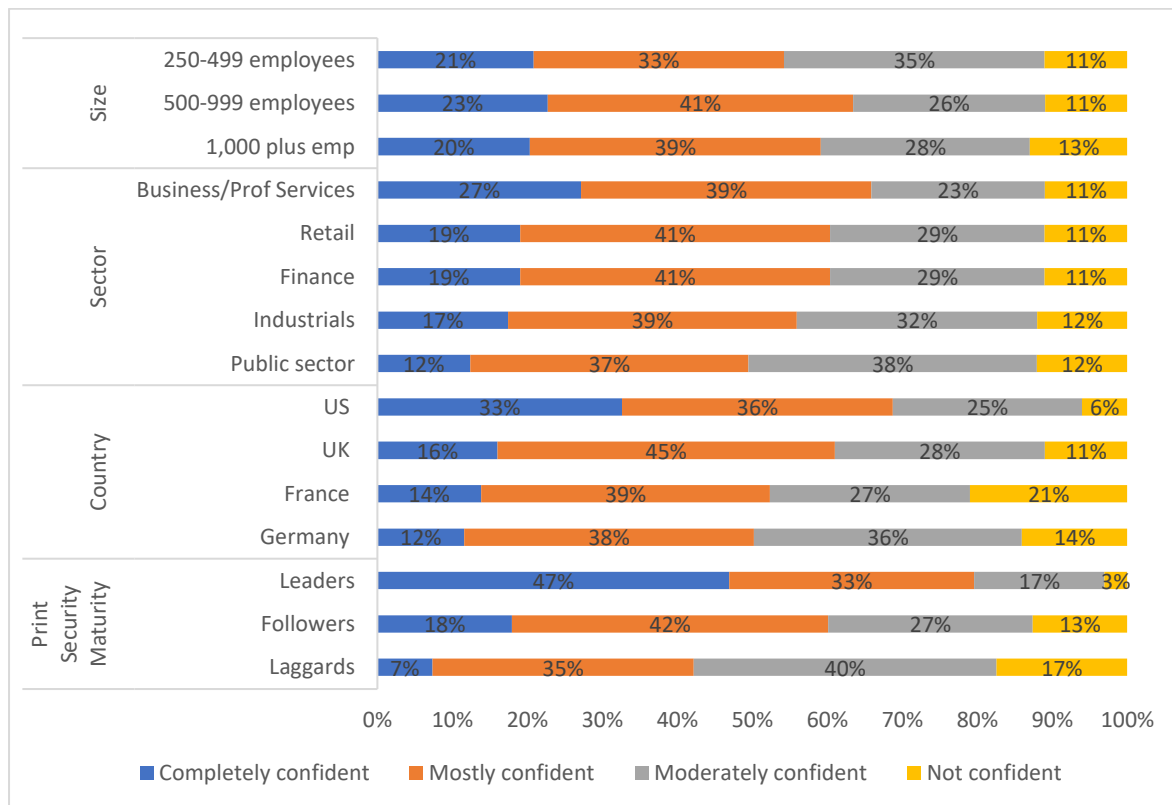


Figure 15. How confident are you that your organisation's print infrastructure now (office and remote workplace) was/is protected from security breaches and data loss? (By Region)

This indicates a significant opportunity for MPS providers to help organisations achieve higher levels of confidence. Broader implementation of security measures will certainly help to improve security preparedness and resilience, and mitigate the potential risks of print related security breaches.

Print-related data losses

Given the lack of confidence in the security of their print infrastructure, it's not surprising that the majority of ITDMs have reported at least one print related data loss over the past 18 months (Figure 16). 64% reported having suffered a print related data loss in the past six months, compared to 66% prior to COVID-19.

Those in the US are most likely to have experienced data losses both pre- and post-pandemic (75% and 73% respectively). 51% of organisations in Germany experienced a data loss pre-COVID, and 54% in France post-COVID. Business and professional services companies were most likely to have experienced a data loss during either period (72% and 69%), while those in the public sector were least likely (56% and 49%).

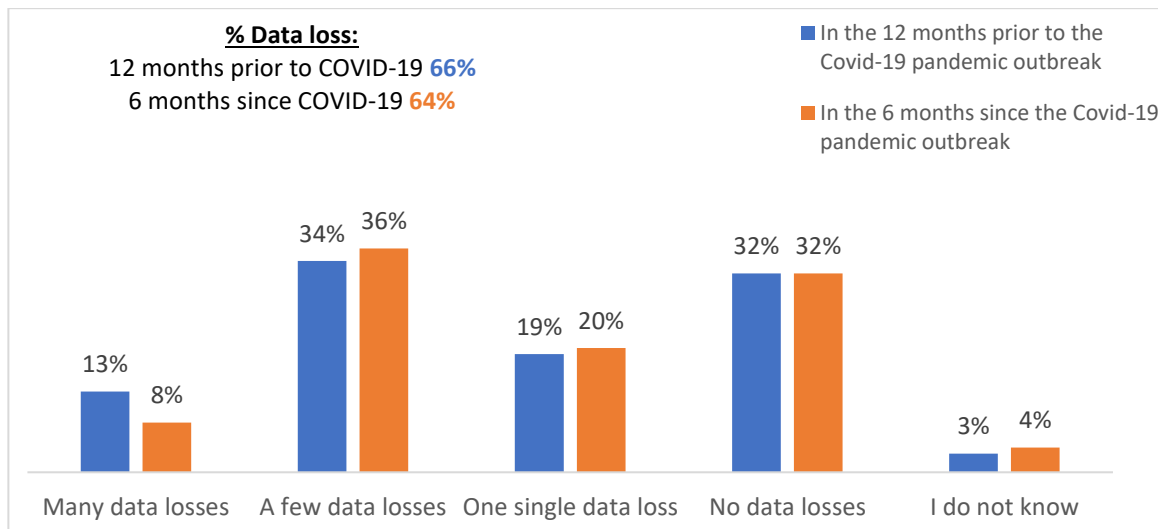


Figure 16. Level of data losses through printers/MFPs due to insecure printing practices

When asked to consider the reasons behind the print related data losses they had suffered, the top reason cited by ITDMs was home workers not disposing of confidential information securely (32%). 27% indicated it was due to printer malware (rising to 36% in the US), and 27% cited confidential information being accessed at the output tray by unauthorised users, rising to 36% in the finance sector.

Notably, data loss is more prevalent in multivendor environments. 42% of ITDMs that operate a standardised fleet report no data losses, compared to 28% that are using a multivendor fleet (Figure 17). Unless integrated print security measures are applied consistently, it is more challenging to secure a diverse mixed fleet. This is because a standardised environment is much more likely to include integrated security controls which also can be easier to track and manage.

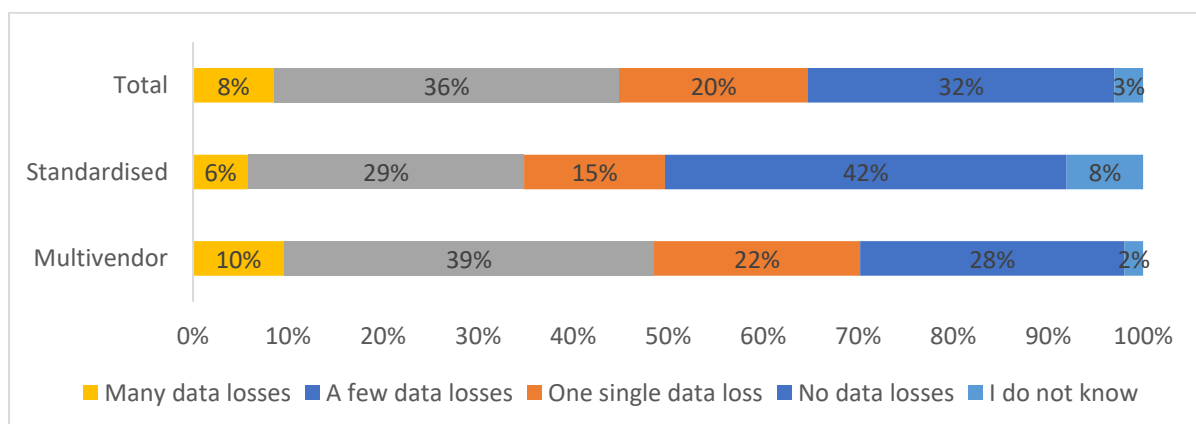


Figure 17. Data loss by print environment

These data losses are costing organisations an estimated average of £1 million, rising to £1.2m in the US and dropping to £825K in Europe (Figure 18). The 2020 figure is skewed by some high individual estimates of more than £10m. This may be due to improving capabilities to quantify losses, or simply down to growing awareness that data leaks are more expensive than previously understood for a range of reasons, including the cost of regulatory fines and of executing the required actions following a loss, through to the cost of damaged customer confidence and reputation.

The costs are highest in the US and the UK, where there are more print-related data losses, and within the finance and professional services sectors and larger businesses.

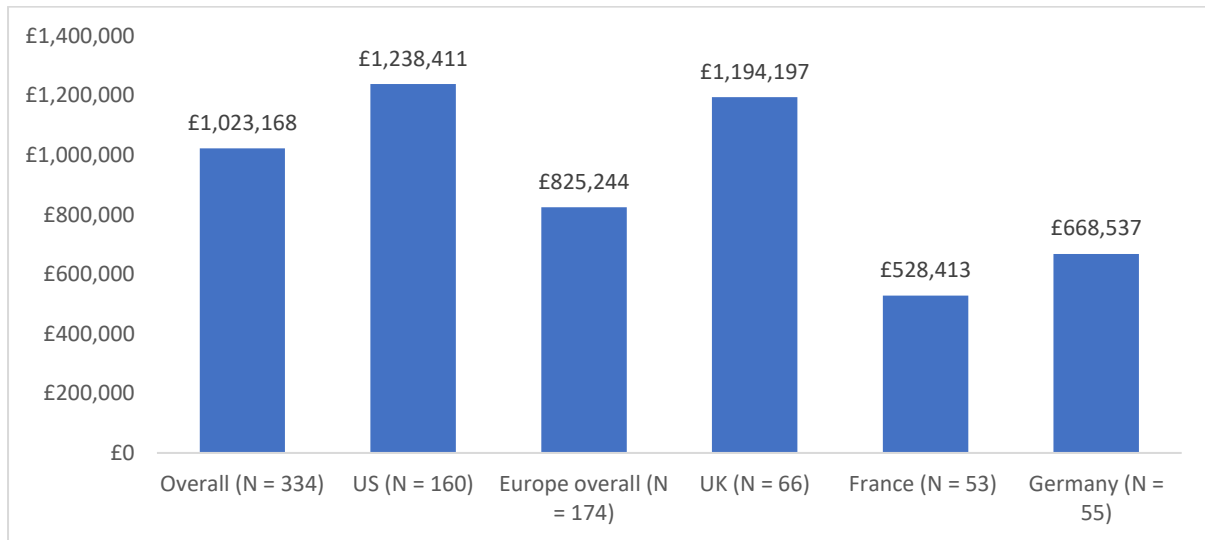


Figure 18. Estimated average cost of a data loss

Supplier choice and satisfaction

US organisations are most satisfied with their print suppliers’ print security capabilities (Figure 19), with German respondents least satisfied. Notably, they also tend to be least confident in their print security.

Just 23% of public sector organisations are *very satisfied* compared to 44% of professional services 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.

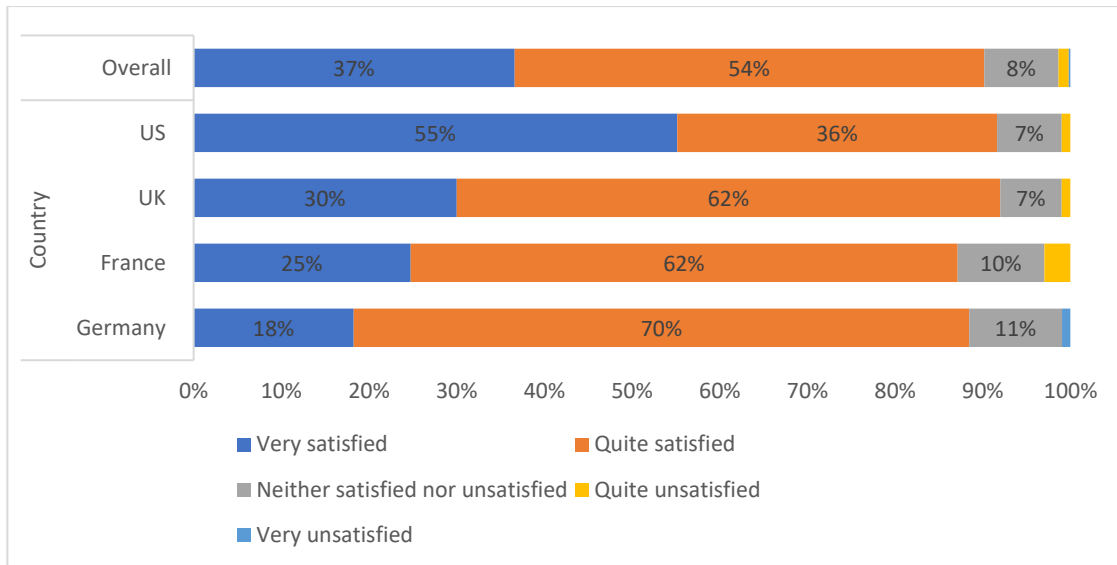


Figure 19. Satisfaction levels

Managed security service providers (MSSPs) are a popular choice for print security advice (Figure 20); overall, 37% of ITDMs say they would turn to an MSSP in the first instance. 23% would turn to a print manufacturer, with smaller businesses most likely to do so as they’re more likely to have a single supplier. 17% of ITDMs overall would consult an MPS provider for print security advice. However, in reality print manufacturers and MPS providers overlap, as both tend to be seen as suppliers by their customers, so taken together they dominate – except in the US, where MSSPs prevail.

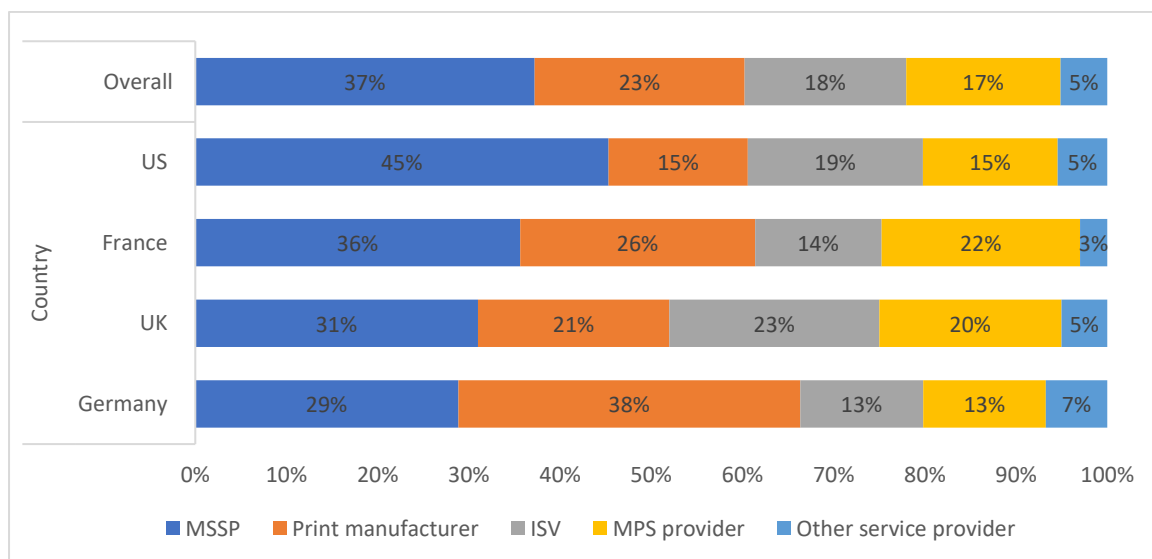


Figure 20. Where would your organisation go first for more information about improving print security?

Buyer Recommendations

Print infrastructure remains an integral element of the overall IT landscape. As devices become more sophisticated, organisations must pay far closer attention to ensuring the print environment is protected, particularly as the potential threat landscape has increased with the rise in home printing. This study has demonstrated that investment in the following areas can build print security confidence, and ultimately lead to improved resilience. Through being better prepared, organisations can improve the prevention of data breaches and losses, as well as the monitoring and remediation required when they do happen.

Quocirca recommends that buyers evaluate the following processes, policies, tools and technologies, in addition to evaluating the hardware security features of MFPs.

- **Authorised printers for home workers:** Quocirca's research shows that employees continue to rely on the printed word as they work from home. One approach to making printing in the home more secure is to only allow the use of authorised printers. This can be achieved in two ways, either by issuing employer-owned printers and blocking other printers, or by certifying the use of employee-owned home printers that can be made safe (for example, those which can provide sufficient log data to a SIEM system). A third approach is to block all home printing – but this will impede productivity.
- **Content security:** Specific policies can be set based on the sensitivity of content, for example: *'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.
- **A formal process to respond to print security incidents:** Even when all available security measures are in place, data leaks – including those that occur via printing – are likely to happen. Most of the respondents to Quocirca's latest research had at least some security measures in place, but 75% still experienced at least one print related data loss in the past 18 months. Organisations must accept the risk, and put appropriate processes in place to respond to them. These should include the allocation of security staff to assess the nature and seriousness of an event, and to enact the follow up, for example contacting impacted data subjects and co-ordinating with regulators.
- **Pull printing:** This allows certain types of sensitive output to be printed only when the user requesting it is actually at the print device ready to release and receive it. Pull printing is most useful for printers 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 print jobs to be tracked at a central level.
- **Print security and risk assessments:** Making sure an organisation's print security requirements are fit-for-purpose is an ongoing task, requiring regular review. This can be carried out internally, or by third parties such as managed security service providers (MSSPs) or managed print service (MPS) providers. Even where an existing assessment was in place before the on-set of the pandemic, it will almost certainly need updating as many employees have started working, and printing, from home.
- **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 broader log management tools. Service providers, including MSSPs and MPS providers, will also have the tools to produce reports and carry out analytics.
- **Revised BYOD policies to include employee printers:** The term bring-your-own-device (BYOD) was first devised when employees started using their own mobile devices to access corporate networks. With the rise of home working, any policies need to be extended to incorporate home printers. Even though content security systems can be used to block home printers, the starting point should be for employees to understand their own responsibilities and the sanctions that can be applied if they try to work around the rules; this is the essence of an effective BYOD policy.
- **Secure cloud print job submission:** Whilst 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 that submits the job never sees the output, for example,

letters to be mailed to customers. 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.

- **SIEM integration:** SIEM (security information and event management) systems use device log data to seek out events in order to check and tune the security status of IT infrastructure. Devices covered can include any printers made visible to a given SIEM system – including those located in employees' homes. The system will be able to identify unexpected access requests to printers, incidents of sensitive content being sent to insecure printers, and so on.
- **Zero trust architecture:** Zero trust is the concept of 'never trust, always verify'. Zero trust operates on the principle that no device, whoever owns it, should be fully trusted as being secure. Typically this approach has been applied to user end-points, giving a company-issued device the same level of trust as one owned by an employee. Any attempt to compromise a device will meet the same rigid security barriers. This approach can be extended to printers, especially those in the home, so no printer, whether company-owned or employee-owned has a lower security state than is considered minimally necessary.

Conclusion – dealing with permanent change

There is no doubt that 2020 has been a year of massive change for businesses and society as whole. As the year draws to an end, and with the real possibility of vaccines to address the COVID-19 pandemic on the horizon, it is not yet clear which of these changes will endure. However, the trends towards more home working and increased adoption of cloud computing seem unlikely to go into reverse.

It is also clear that these changes have not led employees to rush away from printing and paper, and as a result the security problems specific to the use of printers have been exacerbated. To address these risks, organisations need to deploy more of the print security measures available to them, and seek advice from service providers and manufacturers about how best to do so.

Vendor Profiles – MPS Monitor

A managed print service (MPS) is fundamental to ensuring that an organisation operates a secure and cost-efficient print infrastructure. Next-generation print management tools are expanding their capabilities beyond traditional cost and usage reporting to the security threat detection and monitoring of connected printers and MFPs.

Quocirca opinion

MPS Monitor 2.0 is a cloud-based print management platform that offers a robust solution for MPS providers and channel partners to provide integrated print management to their customers. The solution is also available in a number of OEM-branded versions, including HP. The HP SDS Action Center provides easy and secure access to HP Smart Device Services 2.0 technology for partners.

MPS Monitor achieved ISO/IEC 27001 certification in 2017. All systems that run the services provided by MPS Monitor to customers and partners worldwide are included in the ISO/IEC 27001 certification perimeter, and all run within a certified Information Security Management System (ISMS). The company will also conduct a SOC 2 Audit in Q1/2021, to ensure compliance to AICPA Trust Services Criteria for Security, Availability, Confidentiality and Privacy.

With many organisations operating a mixed fleet environment, particularly across a remote and office environment, the ability to remotely track and manage devices involves additional layers of risks that need to be adequately mitigated. MPS Monitor offers a comprehensive set of features to remotely monitor a multi-vendor print and MFP environment and adopts a holistic approach to the security of the entire print environment.

MPS Monitor offers some notable features which enable channel partners to proactively deliver print security management. The platform allows partners to detect for outdated firmware and apply firmware updates where needed. On HP devices specifically, thanks to the integration with HP Smart Device Services technology, security policies can be defined, assessed and remediated. Device compliance can be continually checked and integrated reporting is provided through MS Power BI Embedded analytic dashboards.

The cybersecurity risks associated with having a connection between the customer's network and the cloud management platform, through the presence of an active DCA in every customer, are mitigated by ensuring full compliance to a broadly recognised security standard like ISO/IEC 27001. This requires continuous monitoring and improvement of enforced security policies and best practices.

As with all SaaS cloud solutions, MPS Monitor requires users to manage credentials to access an external cloud service over the internet. MPS Monitor has a comprehensive set of features to reduce these risks including password complexity, two-factor authentication, and integration with single sign-on for customers using Active Directory.

MPS Monitor is working closely with Microsoft Corp. to allow MPS Monitor users worldwide to access Universal Print features seamlessly from within their printer management application. This will add an extra layer of cloud print security for users, in line with Microsoft's strategy on security in Universal Print. The Beta release of MPS Monitor Universal Print integration is planned for December 2020.

MPS Monitor provides an effective way for channel partners to deliver foundational print security management to their customers. Print management is one part of a multi-layered print security model that includes hardware, software and services. A tool like MPS Monitor can detect potential risks through the continual monitoring of devices and support a wider print security strategy that includes assessment, device deployment and remediation from print security incidents.

Product overview

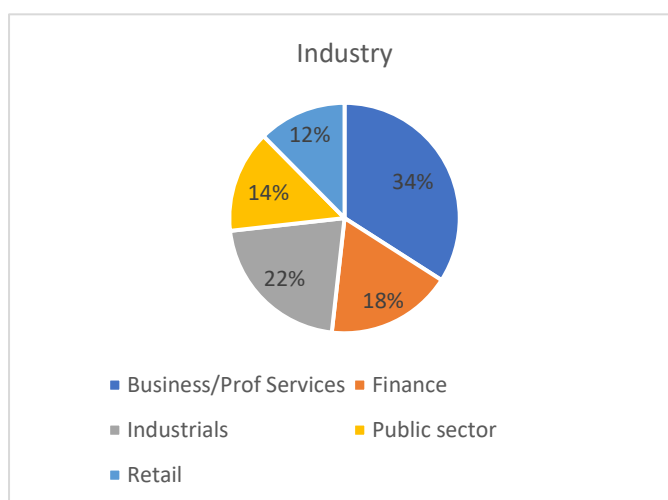
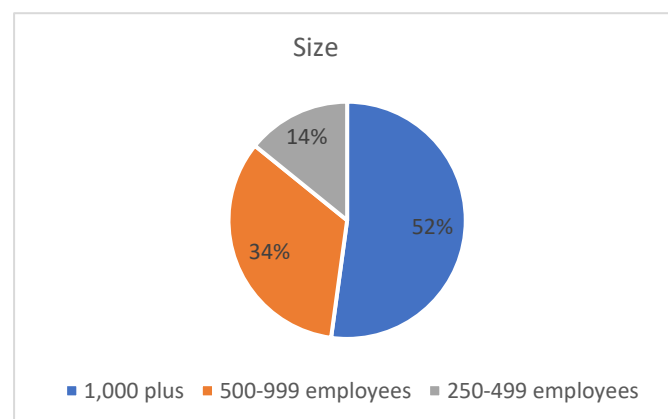
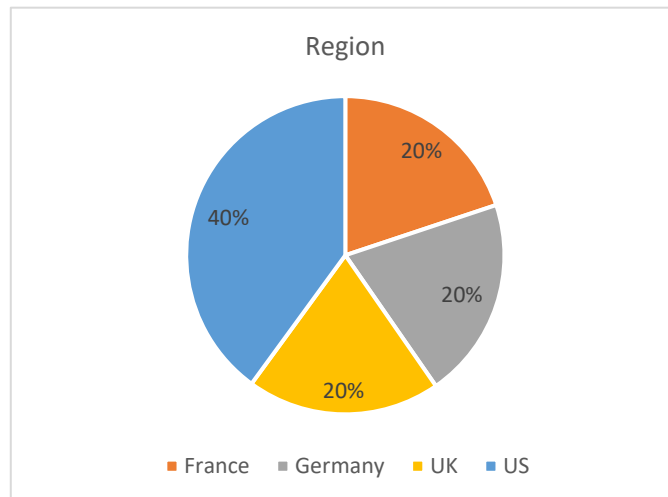
Key features include:

- **Data security.** Both MPS Monitor 2.0 and HP SDS Action Center systems run on the same MPS Monitor cloud infrastructure, and are both operated inside the MPS Monitor ISO/IEC 27001-certified ISMS perimeter.
- **GDPR compliance.** Processing of personal data within the system is performed in full compliance with the GDPR, for all customers and dealers where this regulation is applicable. Confidential information masking can be applied at the user level, and a highly granular user profiles structure is available.
- **User account security.** Two-factor authentication can be activated on all user accounts. Integration with Okta provides single sign-on to Active Directory users. System admins' passwords have to meet specific complexity requirements and are required to be changed every six months or earlier.
- **Cloud infrastructure and customers' IT security.** MPS Monitor cloud infrastructure, code and the network is subject to continuous security monitoring, testing and audits.
- **High security data centre.** The physical infrastructure that hosts the MPS Monitor cloud services is located in a top level, high security data centre.
- **DCA.** A multi-platform DCA and clustered DCA technology provides maximum reliability and security in data collection. From a cybersecurity point of view, the DCA is continuously assessed by a team of security experts, to ensure that its installation within the customer's internal network poses no security risk for the IT environment.
- **Analytics and business intelligence.** A complete business intelligence platform that includes security performance, based on Microsoft PowerBI Embedded technology, is now fully integrated into MPS Monitor 2.0.
- **Built-in security with HP Smart Device Services.** The SDS integration includes features that allows the dealer to access the embedded web server of any HP printer from inside MPS Monitor, to update devices' firmware remotely and in a planned way, and to create, assess and remediate fleet-wide security policies that involve all the main security parameters and configuration items on printers. Once policies are created, checks can be run on a daily basis to ensure compliance and enforce policies where required.

Appendix 1: Demographics and research process

508 IT decision makers were interviewed, all with responsibility or involvement in the management and control of their organisation's print infrastructure and its security. They were based in the USA, UK, Germany and France. A range of business sizes and industry sectors were covered including professional services, industrials, financial services, the public sector and retail.

The breakdown of the 508 interviews by country, industry sector and business size is provided below:



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.

© Copyright 2020, Quocirca. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Quocirca. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.