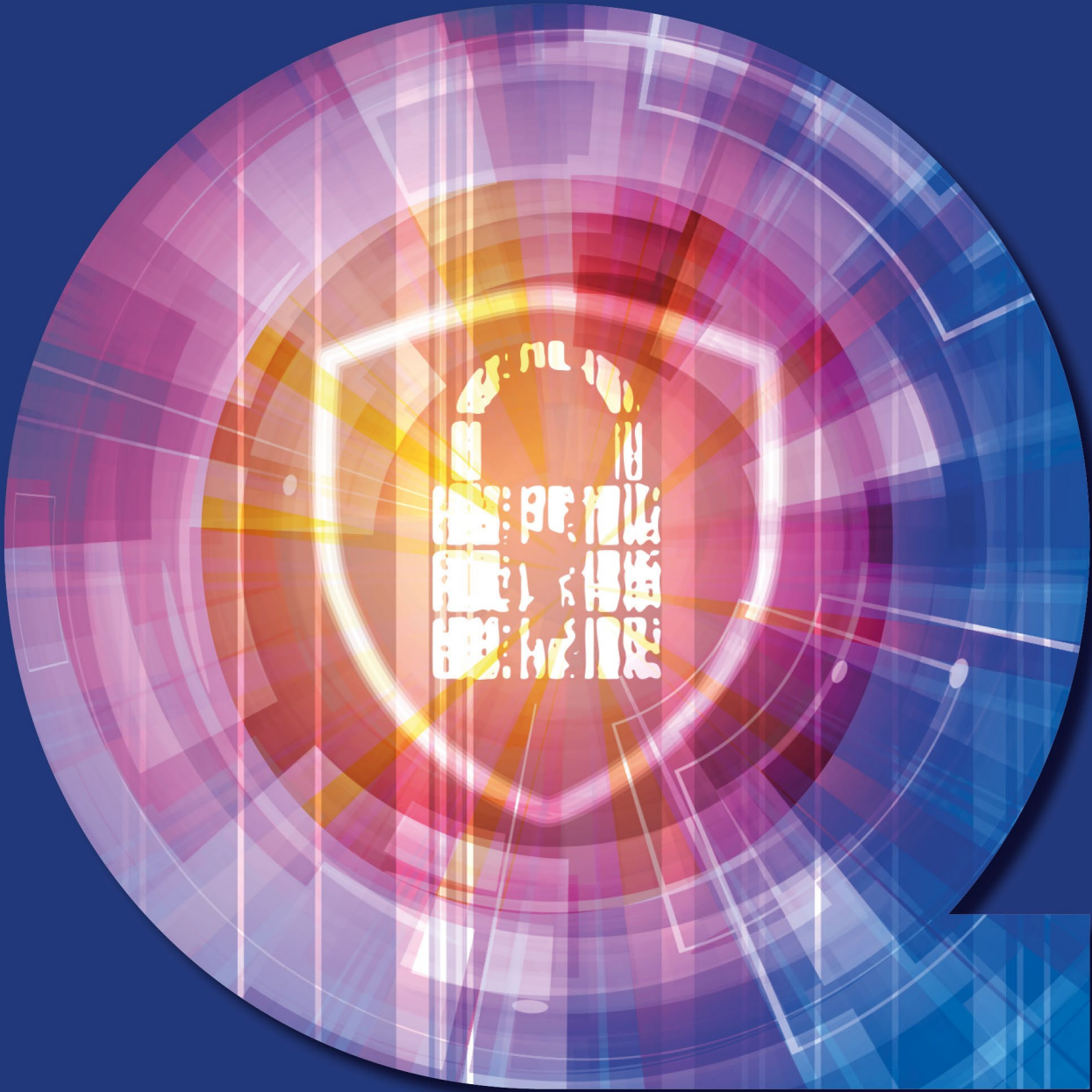


The Print Security Landscape, 2023

Securing the print infrastructure amidst a growing threat landscape



Excerpt report: Print security trends in the US and Europe
May 2023

QUOCIRCA

Executive summary

Quocirca's Global Print Security Landscape 2023 report reveals that organisations face ongoing challenges in securing print infrastructure. Home printing continues to cause security concerns, with employee shadow purchasing making it harder to control document security. Print-related data breaches remain prevalent, with 61% of respondents reporting at least one data loss in the last 12 months, rising to 67% amongst midmarket organisations. This is leading to lower confidence, particularly among SMBs, in the security of print infrastructure.

Notably, the research reveals a strong disconnect between the perceptions and attitudes to print security amongst chief information officers (CIOs) and chief information security officers (CISOs). Expectations for security spend growth in the coming 12 months are similar, with 84% of CIOs and 81% of CISOs expecting their print security spend to increase. Only 28% of CISOs believe it has become harder to keep up with print security challenges, compared to 50% of CIOs. Similarly, only 45% of CISOs are very or somewhat concerned about the risks of unsecured printers, compared to 72% of CIOs. This chasm between CIOs and CISOs means the two individuals responsible for the overall technical security of the print environment when serving the business are not seeing things in the same light – and this has ramifications for the business itself.

Fortunately, print security leaders are mitigating risks. As shown by Quocirca's Print Security Maturity Index, organisations classed as leaders, which 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. For print manufacturers, MPS providers, and the rest of the print channel, bridging this gap between the two security camps is a must. However, this cannot be done simply – it will require a two-pronged approach to bring the two parties closer together, as well as ensuring the business itself is more aware of the security issues around print.

Therefore, 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. Becoming a trusted advisor and provider of print security solutions that fit with an organisation's existing security environment is key. Ensuring data and information flow, along with device and output security, will create new revenue capabilities for the print channel.

The Global Print Security Landscape 2023 study is based on the views of 507 IT decision-makers (ITDMs) in the US and Europe. Respondents include 20% from the UK, 20% from France, 20% from Germany, and 40% from the US. In terms of organisation size, 24% represent small and medium-sized businesses (SMBs) (250 to 499 employees), 26% are from mid-size organisations (500 to 999 employees), and 50% are from large enterprises (1,000+ employees). Respondents are drawn from a range of verticals, including business and professional services, finance, industrials, public sector, and retail.

The study also includes the print security vendor landscape, which features Quocirca's assessment of service offerings from major print manufacturers.

The following vendors participated in this study: Brother, Canon, Epson, HP, Kyocera, Konica Minolta, Lexmark, Ricoh, and Xerox.

Key findings

- **Cybersecurity incidents continue to rise.** Overall, 42% of organisations report an IT security breach in the past year, rising to 55% among mid-market organisations and dropping to 36% amongst large enterprises, along with 51% in the finance sector, dropping to 32% in the public sector. The highest incidence across all organisations is malware, with phishing highest in the mid-market. Security breaches increased for 61% of organisations in the past year, rising to 70% in the US and 66% in business and professional services. On average, 27% of IT security incidents were related to paper documents.
- **Reliance on printing creates a need for effective print security.** Despite rapid digitisation over the course of the pandemic, 70% remain dependent on print today, rising to 72% in large organisations. A majority (80%) have changed the composition of their printer fleet over the last two years, rising to 88% in the mid-market. Overall, 79% expect to increase their print security spend in the next year, rising to 86% in the US and 85% in business and professional services and retail.
- **Print security is lower on the security agenda than other elements of IT infrastructure.** Cloud or hybrid application platforms, email, public networks, and traditional end points are seen as top security risks. Employer-owned home printers come in as the seventh top security risk (21%), ahead of the office print environment (20%). Notably, there is a disparity between CIOs and CISOs. Just 18% of CIOs consider office printing a key security risk compared to 30% of CISOs.
- **Organisations are taking different approaches to managing the security of their print infrastructure.** While 31% indicate they use an MPS provider, over half (54%) indicate that they use a managed security services provider (MSSP) to manage both print and IT security. This rises to 58% amongst smaller organisations (249–499 employees).
- **Organisations are finding it harder to keep up with print security demands.** Overall, 39% say it is becoming harder, rising to 50% in the midmarket (500–999 employees). The top challenge is keeping print management software up to date (35%), protecting sensitive and confidential documents from being printed (34%), and securing printing in the remote/home environment (31%). Hardware security is a key concern for SMBs (29%), and highest in the finance and industrial sectors (31%) and for CISO respondents (38%).
- **Organisations using MPS or that are classified as print security leaders are more confident in the security of their print infrastructure.** The visibility and control provided by an MPS appears to ease the security burden for users. While overall, only 19% of respondents are completely confident in the security of their print infrastructure, this rises to 26% amongst organisations using MPS. Overall, a further 50% say they are mostly confident. This reflects the growing complexity and challenges associated with securing both devices and documents across a hybrid workplace.
- **In the past 12 months, 61% of organisations have experienced data losses due to unsecure printing practices.** This is a fall from 68% in our 2022 study. Mid-market organisations are more likely to report one or more data losses (67%) than large organisations (57%) and the public sector (49%). On average, the cost of a print-related data breach is £743K. Beyond the financial loss, the top impact of a data breach is the lost time in addressing the breach and the impact on business continuity (30%). Vulnerabilities around home printing, such as home workers not disposing of confidential information securely, was cited as a top factor contributing to data losses.
- **Quocirca's Print Security Maturity Index reveals that only 27% of the organisations studied can be classed as Print Security Leaders,** meaning they have implemented six or more security measures. The number of leaders rises to 31% in the US and falls to 18% in Germany, which also has the highest number of laggards (29%). Print Security Leaders are likely to spend more on print security, experience fewer data losses, and report higher levels of confidence in the security of their print environment. When compared by vertical, business and professional services have the largest percentage of leaders (37%), with the public sector having the least (18%).
- **Less than one-third (32%) are very satisfied with their print supplier's security capabilities.** This rises to 50% amongst US organisations and drops to 17% in Germany. Those using an MPS have far higher satisfaction levels (39% are very satisfied) than those not currently using an MPS or with no plans to use one (23%). Print security leaders – those that have adopted a range of measures, including security assessments, pull printing, and formal print security policies, are most likely to report higher satisfaction levels – 53% of leaders are very satisfied, compared to 27% of followers and only 15% of laggards.

Table of Contents

Executive summary	2
Key findings	3
Introduction	5
Hybrid work and cloud adoption are shaping print security challenges	6
Print security remains low on the IT security agenda	7
Print security challenges are harder to keep up with	8
Taking measures to address print security	10
Print security spend is increasing	11
Print security leaders are most confident in the security of the print infrastructure	12
Print-related data loss, cost, and impact	14
The majority report print-related data losses, particularly in smaller organisations	14
The cost of a print-related data breach.....	15
The broad consequences of a data breach	16
Organisations using MPS are most satisfied with print security	17
Overall brand perception	18
Recommendations	19
Supplier recommendations	19
Buyer recommendations.....	19
Vendor profile: Pharos	21
About Quocirca	23

Introduction

As organisations adjust to managing remote and hybrid teams, supporting digital transformation, and navigating an uncertain and volatile global economy, they face an ever-expanding landscape of vulnerabilities and increasing risk. Quocirca's research reveals that 42% of organisations have experienced a cybersecurity incident in the past year, rising to 51% in the finance sector and 55% amongst midmarket organisations. The volume of security incidents has increased in the past year for 61% of organisations.

Supply chain disruption and geopolitical situations such as the Russia-Ukraine war have further intensified the threat landscape. The increased prevalence of ransomware, ransomware denial of service (RDoS), distributed denial of service (DDoS), social engineering, and supply chain attacks is driving increased concerns around cybersecurity and the resilience of business-critical functions.

This is further compounded by a raft of technological challenges. As organisations migrate more applications and services to the cloud to support digital transformation initiatives, new security challenges emerge. The growing amount of business-critical data hosted in the cloud becomes vulnerable to attack and compromise.

This risk is heightened due to remote workers accessing data from potentially unsecure home networks. Security threats include misconfigured access points, weak passwords, lack of identity and access management (IAM), and failure to use multifactor authentication. A fragmented approach to threat detection and monitoring means security teams are struggling to keep up.

The print infrastructure is not immune to security risks – on average, paper documents represent 27% of IT security incidents. Today's intelligent multi-function printers (MFPs) not only pose a risk of paper output falling into the wrong hands – whether accidentally or maliciously – but also can be exposed as gateways into the rest of an organisation's environment. Home printers pose an additional risk, particularly those that were purchased by employees. This shadow purchasing means home printers may not meet corporate security standards or be monitored through centralised security tools.

Although print remains low on the IT security agenda, organisations continue to report print-related data losses. In our 2023 study, 61% of respondents report a print-related data breach, with an estimated average cost of £743K for one data breach. With both the reputational and financial impact of any security incident far reaching and substantial, organisations cannot afford to be complacent.

These risks can be mitigated through adopting a never trust, always verify zero-trust security approach. Implementing data and network encryption, security monitoring, and remediation, along with micro-segmentation, can help reduce the attack surface, improve threat containment, and strengthen regulatory compliance.

This report highlights the risks and challenges associated with securing the print infrastructure for the hybrid workplace. It discusses security confidence levels, print security measures adoption, and the disconnect between CIOs and CISOs that must be overcome. The report also includes an analysis of the security products, services, and solutions from the major print manufacturers in the market.

Hybrid work and cloud adoption are shaping print security challenges

Despite the ongoing shift to digitisation, organisations remain reliant on print. Quocirca's study shows that the majority (70%) believe print will remain very important or critical to their organisation in the next 12 months. Meanwhile, hybrid work is here to stay. On average, 25% of workforces are fully remote, 33% are hybrid, and 42% are fully in the office. A higher proportion of SMB workforces are fully in the office (49%) than of those at large enterprises (39%). This creates challenges for managing and securing print in the hybrid work setting.

With the return to the office now well underway, print volumes are beginning to recover. Overall, 68% expect to see growth in office print volumes in the next 12 months, with 64% expecting growth in home printing of business documents. Overall, 80% have changed the composition of their printer fleet over the last two years, rising to 88% in the mid-market. In addition, 69% operate a multivendor fleet, rising to 73% and 71% in finance and business and professional services, respectively.

In terms of MPS usage, 57% use a managed print service (MPS) and 53% some form of cloud printing, rising to 60% in large organisations. Although currently only 4% operate their print infrastructure fully in the cloud, this is set to rise to 18% by 2025. Today the majority are taking a hybrid approach (29% operate a mix of cloud and on-premise print management).

The need to implement more effective security for print infrastructure means addressing not only the office print environment, but also employee-owned printers and MFPs, because of data traversing public networks. Without effective security controls, this reliance on printing amidst an expanding threat landscape exposes organisations to security risks.

A multivendor fleet may not have consistent security controls across a mixed fleet of devices, home printers may not be authorised or monitored, and a fragmented approach to cloud printing may create further security risks around access and authentication. Although previous Quocirca research has shown that organisations tend to regard cloud platforms as more secure than on-premise systems, nothing should be taken for granted as the threat surface increases and novel threats continue to emerge.

Print security remains low on the IT security agenda

Perhaps unsurprisingly, given the broader IT security threat landscape, printers are ranked lower than other areas of IT when it comes to security risks (Figure 1). This varies distinctly by region. US and UK organisations are most likely to rank office printing as a top risk (25% and 26%, respectively), with US organisations most likely to consider home printing a risk – 25%, compared to just 14% of UK organisations.

Notably, CISOs are more likely to consider office printing a security risk (30%), compared to just 18% of CIOs. This disconnect reflects the potential challenges around priorities that organisations are placing on print security. If these stakeholders can work more closely to understand the print security risk, organisations can gain stronger resilience around their print infrastructure.

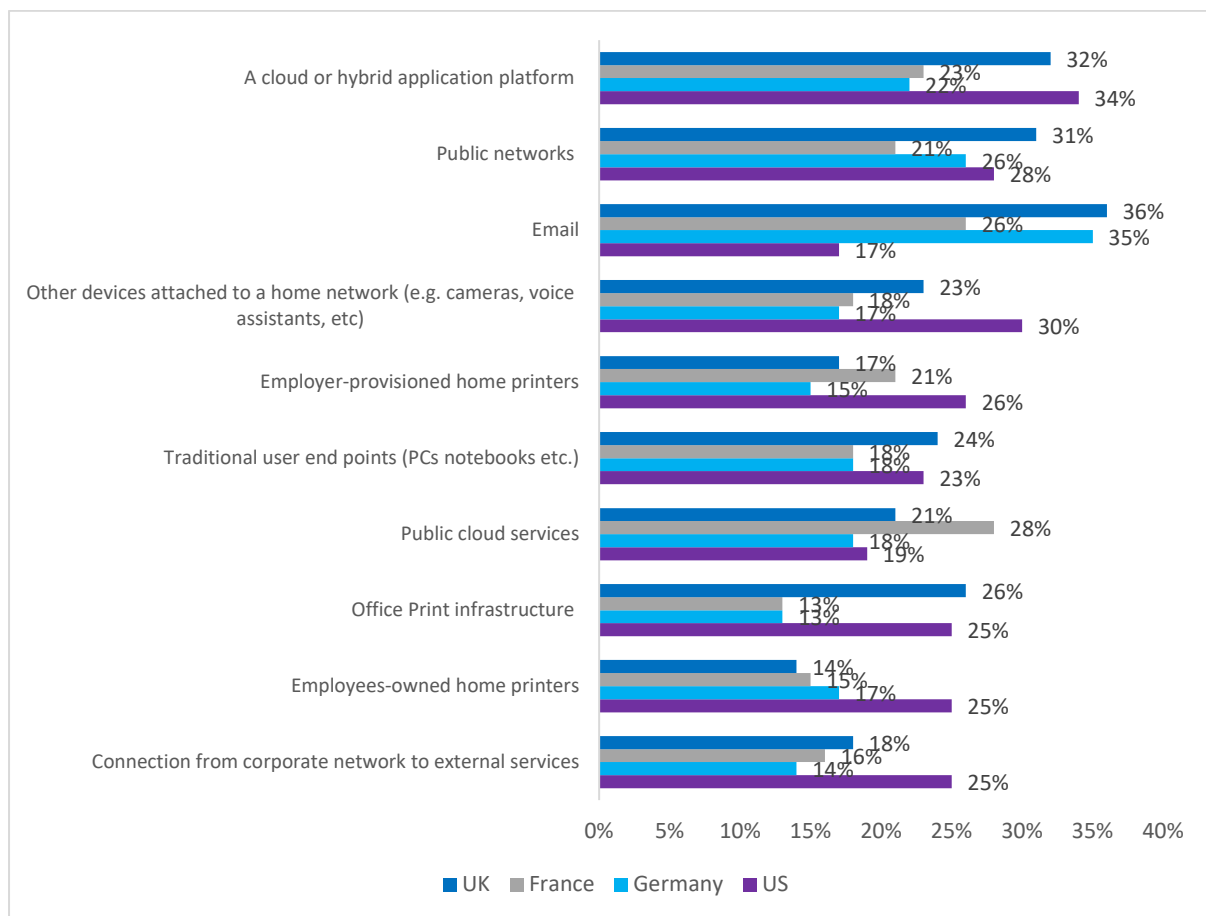


Figure 1. Which areas are considered to pose the greatest security breach risk? (Top 10 shown)

Print security challenges are harder to keep up with

When asked to identify their top three challenges around print security, 35% of respondents chose maintaining printer management software at a suitable level of security capabilities, with 34% choosing protecting sensitive or confidential documents from being printed, and 31% choosing securing printing in a remote/home environment (Figure 2). The level of disconnect between CIOs and CISOs stands out. CIOs rank their top three challenges as maintaining security levels of print management software, document security, and remote/home printing. In contrast, CISOs’ top challenges are related to data and hardware security. This may point to differing levels of understanding of the print infrastructure risks seen earlier.

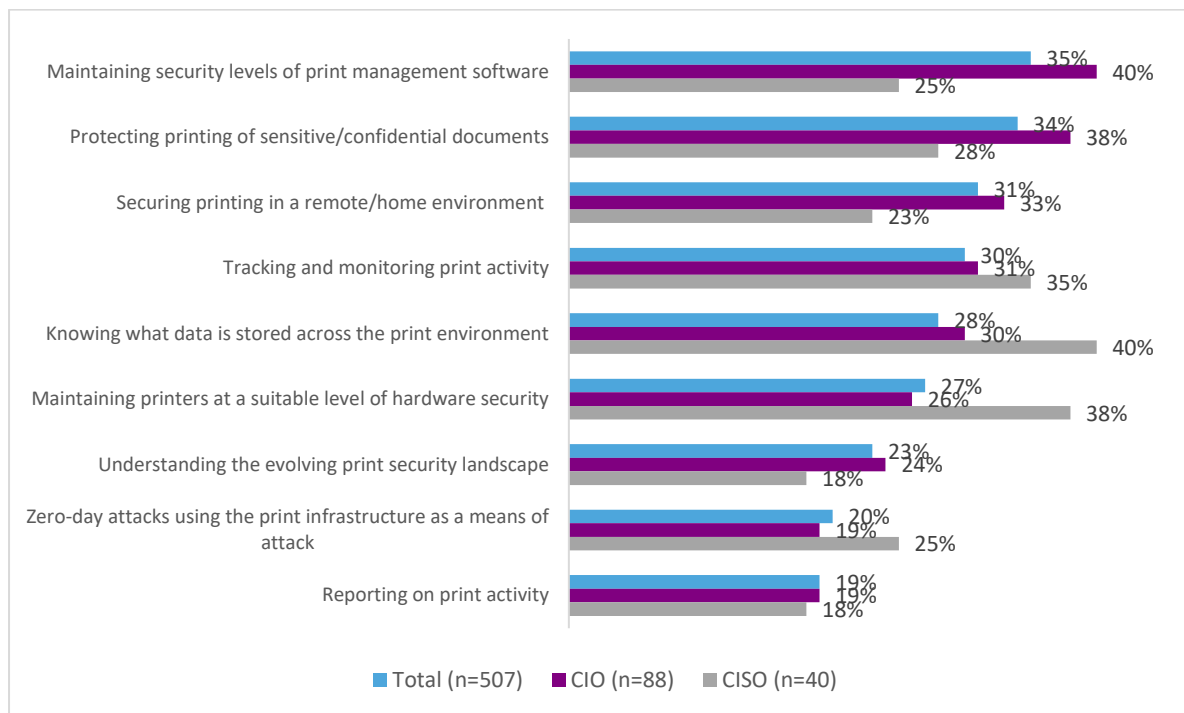


Figure 2. Which of the following do you consider to be the biggest print security challenges?

Consequently, keeping up with print security challenges remains problematic for many organisations (Figure 3), with 39% overall stating that it is either considerably or somewhat harder. This is, however, down from 2022, when over half stated that it was somewhat or considerably harder. The US has the largest number of respondents stating that it has become considerably harder (13%), but also the highest proportion stating that it has become somewhat or a lot easier (39%). Mid-market organisations are struggling the most, with 50% stating that they find it either somewhat or very difficult to keep pace with print security challenges.

CIOs are finding it far harder (50% considerably or somewhat harder) than CISOs (28%) to keep pace. This should not be a surprise: CIOs have a far broader range of issues to keep pace with, while CISOs should be more focused purely on security issues.

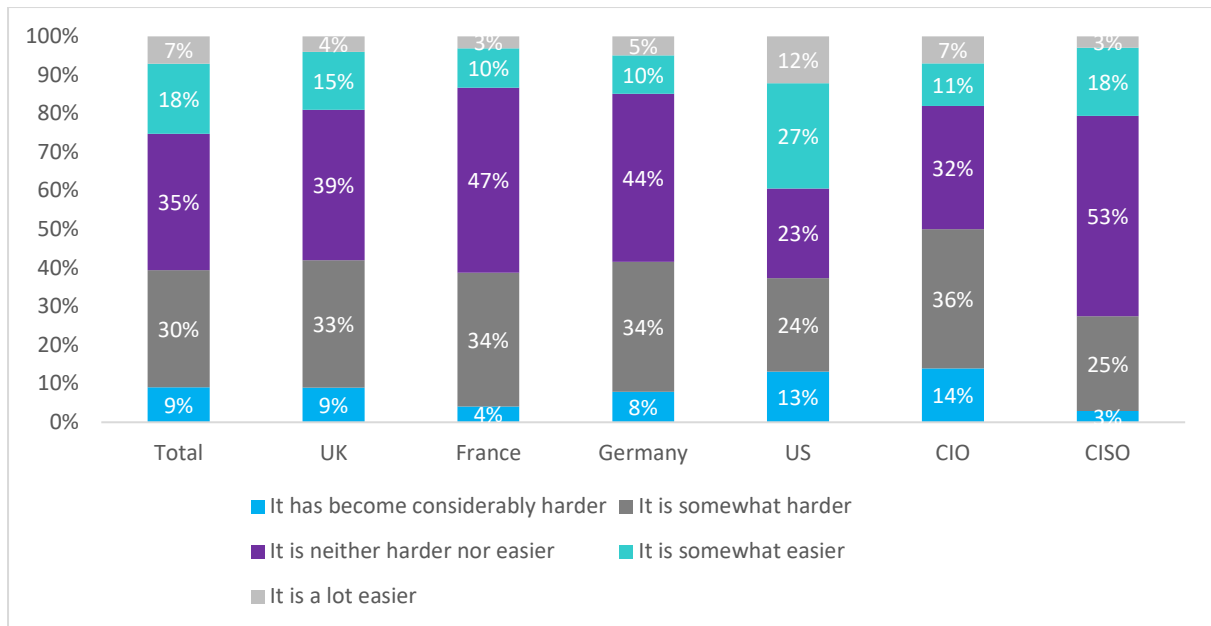


Figure 3. How do you feel about keeping up with print security challenges and demands?

Taking measures to address print security

Organisations are taking different approaches to managing the security of their print infrastructure (Figure 4). While 31% indicate they use an MPS provider, over half (54%) indicate that they use a managed security services provider (MSSP) to manage both print and IT security. This rises to 58% amongst smaller organisations (249–499 employees).

This potentially has a bearing on their concerns and confidence in managing print security.

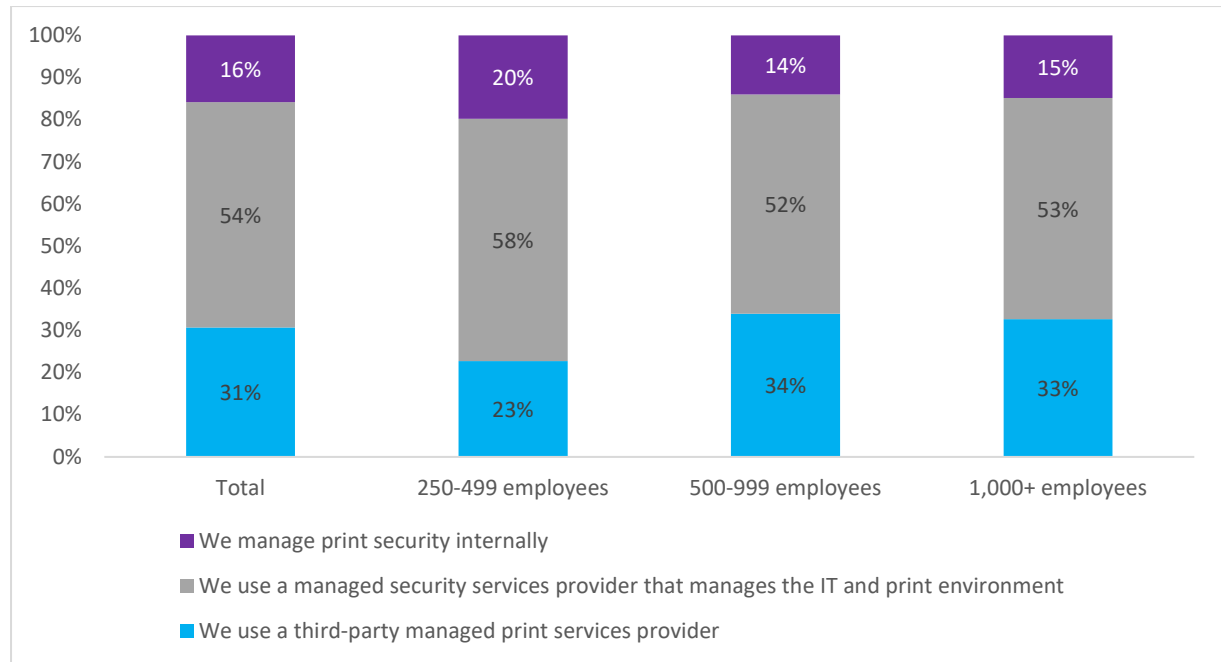


Figure 4. How do you currently manage print security?

Print security spend is increasing

Print security spend continues to rise. Overall, 79% of respondents expect their security spend to increase in the coming 12 months, rising to 86% in the US and dropping to 72% in Germany.

Organisations are using their allocated security budgets to invest in a variety of print security products and services (Figure 5). Adoption of print security varies by organisation size – larger organisations are more likely to be implementing formal print security assessments (56%) and data loss prevention (DLP) tools (58%). They are also more likely to be undertaking security audits of cloud and MPS providers (51%).

Overall, 38% have adopted a zero-trust approach to print security, with a further 39% indicating that they plan to adopt this in the next 12 months.

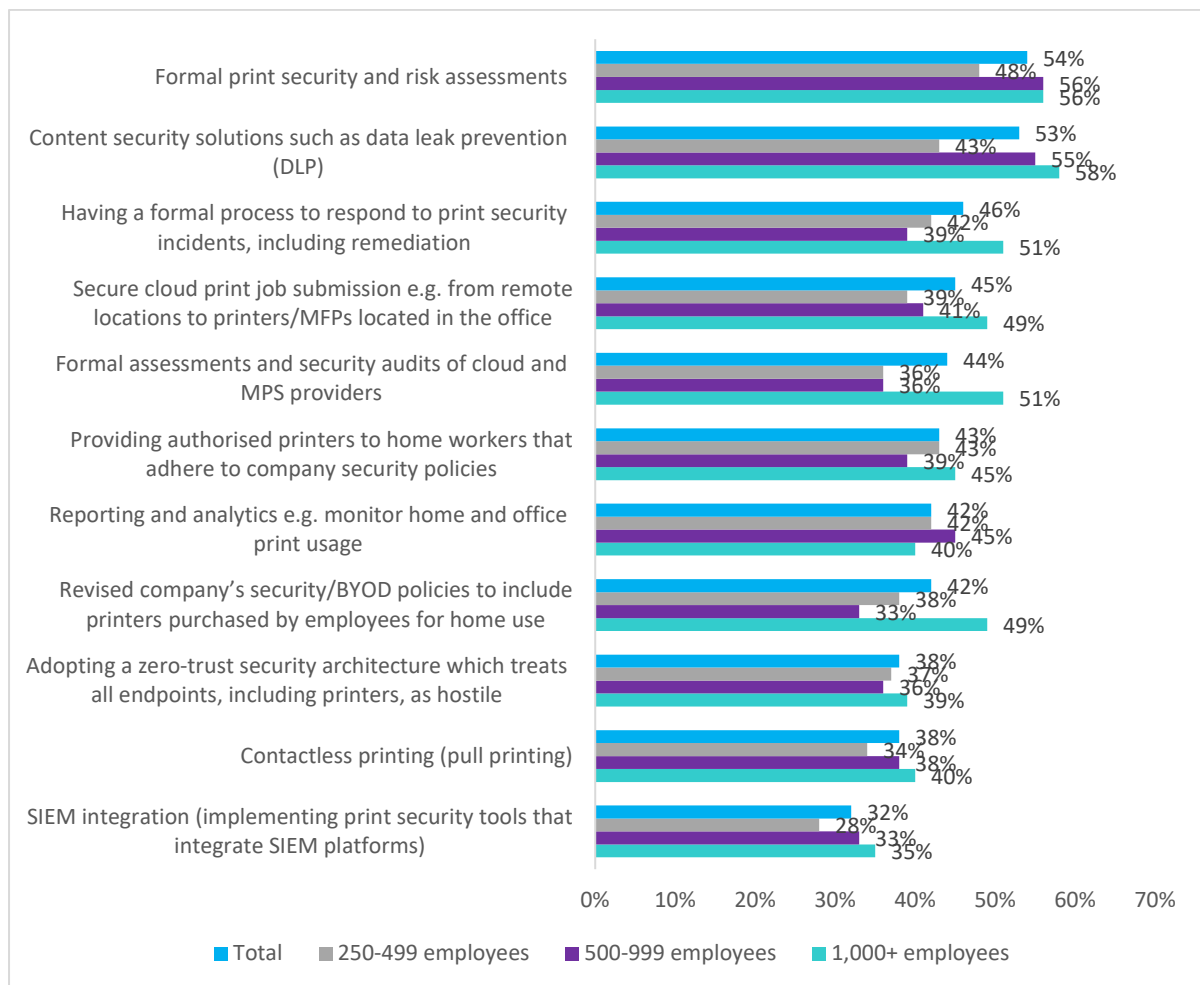


Figure 5. Has your organisation implemented any of the following print security measures?

Print security leaders are most confident in the security of the print infrastructure

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 5).
- **Followers** have implemented between two and five measures.
- **Laggards** have implemented one or none of the measures.

Overall, 27% are classed as print security leaders (up from 18% in 2022), rising to 31% in the US (Figure 6). Germany has the largest proportion of laggards (29%). Large organisations have the highest proportion of leaders (30%), with mid-market and SMBs having 23% each. Company size and being a laggard have correlation, however – 21% of SMBs are laggards, compared to 17% of the midmarket and 11% of large organisations.

Business and professional services organisations have the largest proportion of leaders (37%), followed by retail (32%). The public sector has the lowest proportion of leaders at 18%. The number of laggards is similar across all verticals, ranging from 13–17%.

Overall, 76% of print security leaders use MPS, compared with only 52% of those in the follower segment and 42% of laggards. Of leaders, 33% expect their overall security spend to increase by more than 26% over the next 12 months, compared to 20% of followers and 13% of laggards.

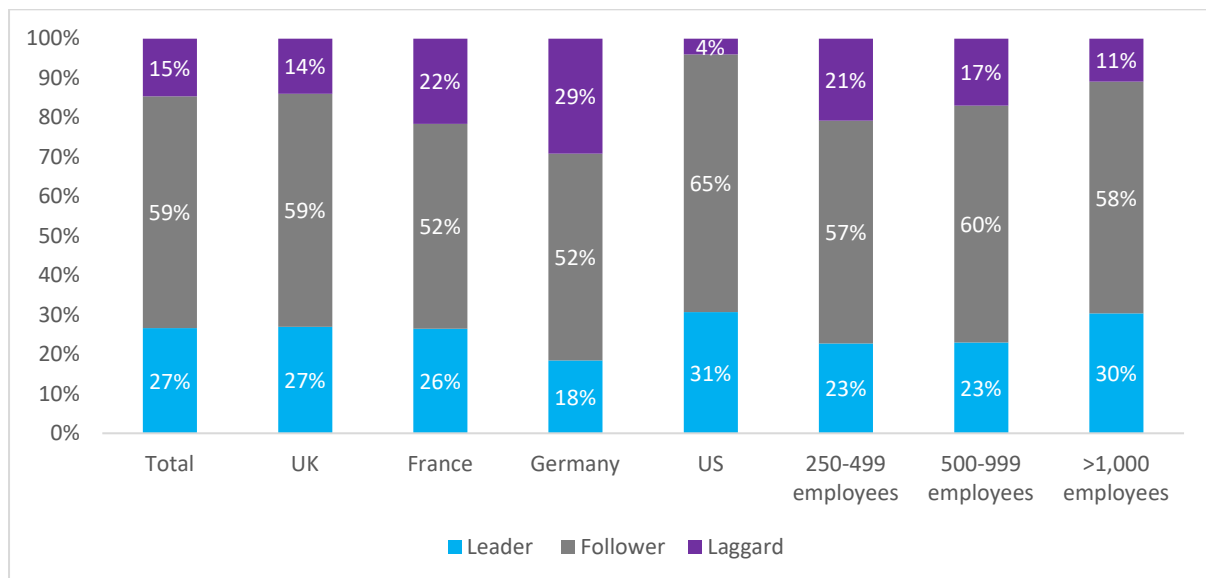


Figure 6. Quocirca’s Print Security Maturity Index by country

Overall, only 19% of respondents are completely confident that their print infrastructure is secure, compared to 23% in 2022 (Figure 7). A further 50% are mostly confident, compared to 34% in 2022.

However, overall levels of confidence are growing, with 69% being mostly or completely confident in their environment now, compared to 60% in 2022. US respondents are the most confident, with 28% reporting they are completely confident, compared to just 8% in France, 16% in Germany, and 17% in the UK. Mid-market organisations report the highest confidence (27%), compared to 19% of large organisations and 11% of SMBs. Business and professional services are the most confident at 28%, with industrials the least confident at 12%. CIOs, at 24%, are far more confident than CISOs at 15%.

Print security leaders (33% completely confident) are ahead of followers (16%) and laggards (8%). Notably, organisations using MPS have the most confidence in their print security. While just 10% of organisations not using MPS are confident in the security of their print infrastructure, this rises to 26% amongst organisations using MPS.

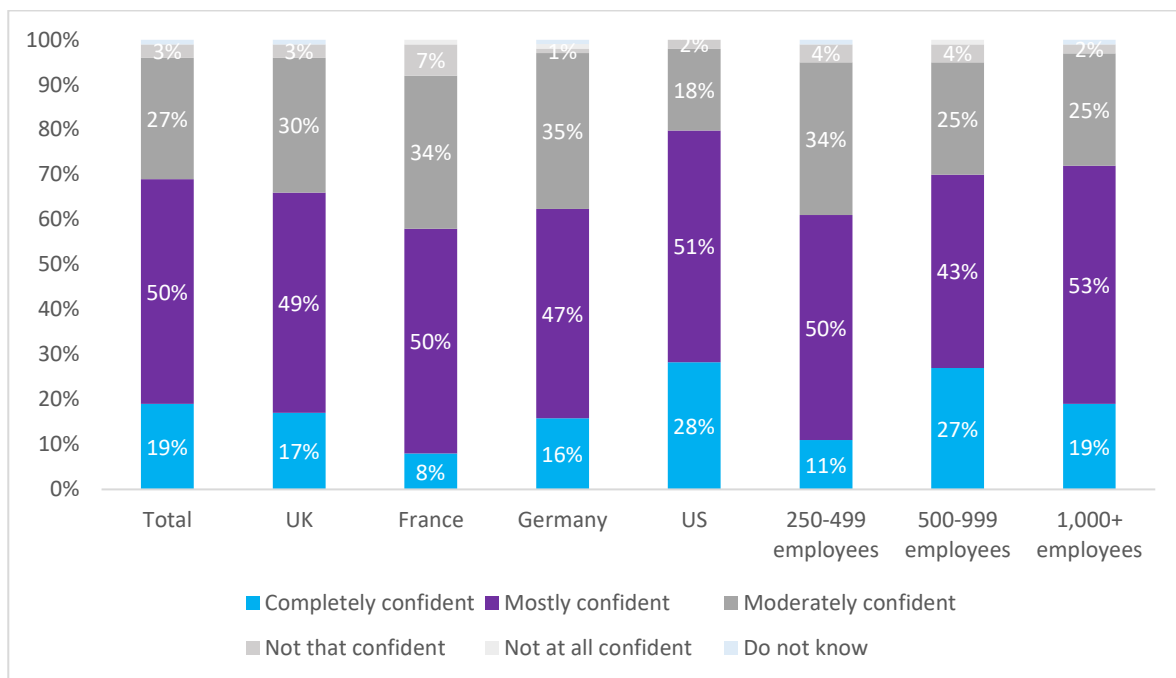


Figure 7. How confident are you that your organisation's print infrastructure (office and remote workplace) is protected from security breaches and data loss?

Print-related data loss, cost, and impact

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

The research shows that 61% of organisations have reported at least one print-related data loss over the past 12 months (Figure 8), rising to 63% in the UK and 67% in organisations with 500–999 employees, and dropping to 57% amongst large organisations. These figures are in line with the 2022 findings, showing that little has changed in enhancing the security of a print data environment. Retail organisations are most likely to have experienced a data loss during the period (67%), while the public sector reported the lowest volume of data breaches (48%). No data losses were reported by 32% of CIOs, against 25% of CISOs. Here, it seems that CISOs are not keeping the CIOs up to speed with what is happening – this is dangerous both in overall management and because of the possibility for any data leak to have reputational and/or legal ramifications.

As in 2022, midmarket organisations state the highest confidence levels in the security of their print platforms, yet also disclose the highest number of data breaches. This shows an obvious disconnect between perception and reality. The channel should help provide 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.

Reported data losses for those operating a mixed fleet of printers (63%) are considerably higher than those with a standardised fleet (56%). 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 users report a lower level of security breaches (59% reporting at least one print-related security breach) than those with no MPS or plans to implement one (66%).

The level of data loss and print security maturity also have correlation. Overall, 47% of print security leaders report one data loss or more, compared to 65% of followers and 68% of laggards. Although this shows that being a security leader does help, it is still worrying that nearly half of leaders have experienced one data leak or more. This demonstrates the need for robust security measures regardless of MPS usage, as well as for help from external partners to ensure the security measures have been implemented and are being operated effectively.

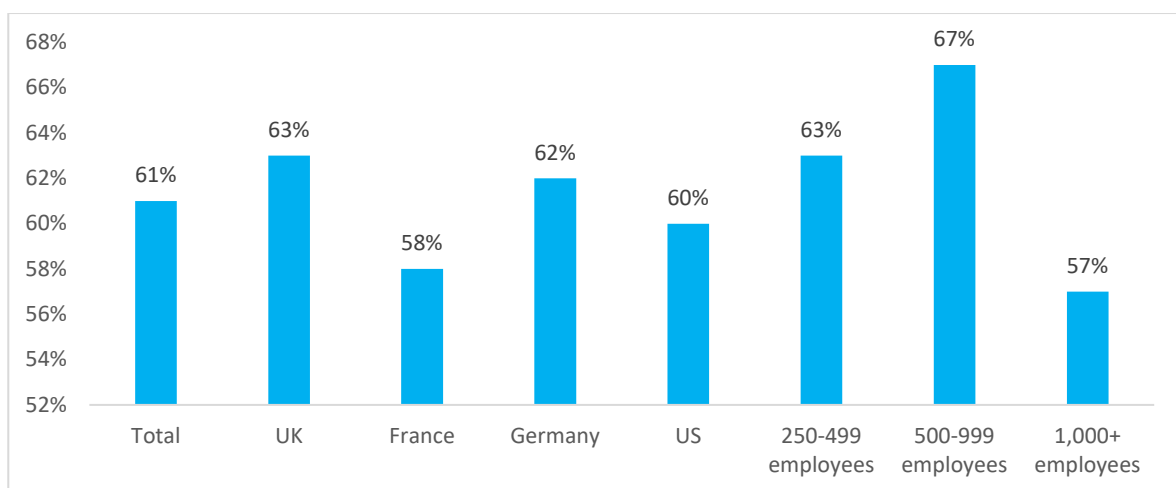


Figure 8. Level of data losses through printers/MFPs due to unsecure printing practices (in the past 12 months)

When asked to consider the reasons behind the print-related data losses they had suffered, 56% cited vulnerabilities around home printers, such as homeworkers not disposing of confidential information securely. Of these respondents, 44% indicated that confidential data had been intercepted in transit, 32% cited unsecure handling of printed output in the office, and 30% reported insecure disposal of printed output. This should focus organisations on the home-printing security issue, but it has not been the case to date. MPS providers can help

by bringing this dichotomy to the table and showing how a suitable MPS can help manage the flow and output of information across the whole hybrid workplace.

The cost of a print-related data breach

The average cost of a data breach is over £743,000 per breach, rising to approximately £1,338,000 in France and falling to a little over £492,000 in the UK (Figure 9). The sizes of organisations show correlation: large organisations see losses averaging £1,103,000 per breach, with SMBs seeing losses of £400,000. Business and professional services see the highest cost of a breach (£1,219,000), with the public sector experiencing the lowest cost (£419,000). The security index also shows correlation: security leaders see average losses of £713,500, compared to followers with £992,700 and laggards with £1,240,800. This provides a solid platform for the channel to show how lack of suitable controls can lead to major financial losses – and the probability of reputational ones piling on top of this.

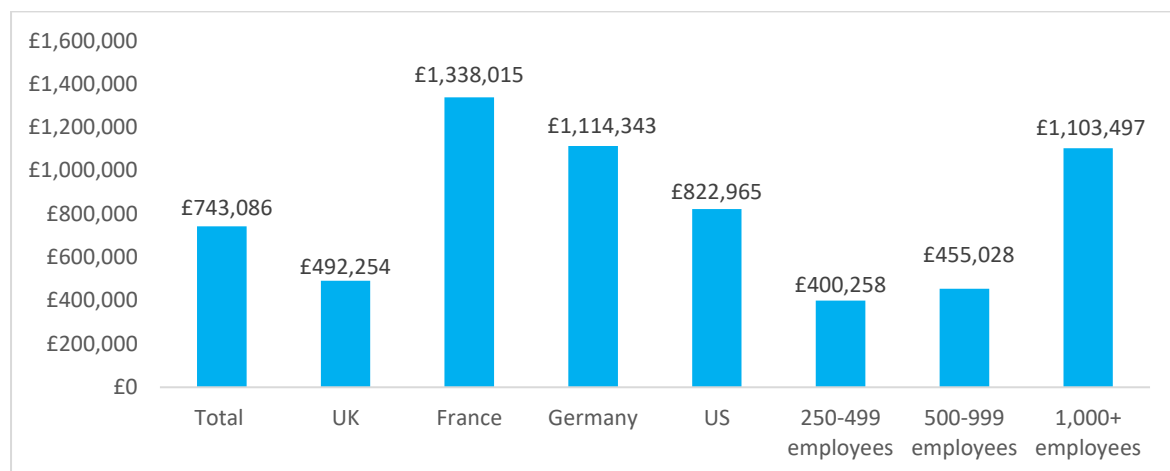


Figure 9. Estimated average cost of a data breach (n=308 that reported a data breach)

The broad consequences of a data breach

Beyond the simple direct costs of a data breach, organisations also report a range of other impacts (Figure 10). The highest impacts overall are on the amount of time it takes the IT team to respond to and manage the issue (30%), along with the negative impact on business capability (30%). Negative impact on business capability has much greater effect on large organisations (35%), compared to 23% of the midmarket and 28% of SMBs. Similarly, for 33% of large organisations, time lost to waiting for IT to respond to a breach is a major issue, compared to 26% of the midmarket and 28% of SMBs. SMBs and the midmarket find that breaches of internal personal information are of greater impact than large organisations, as well as lost revenue.

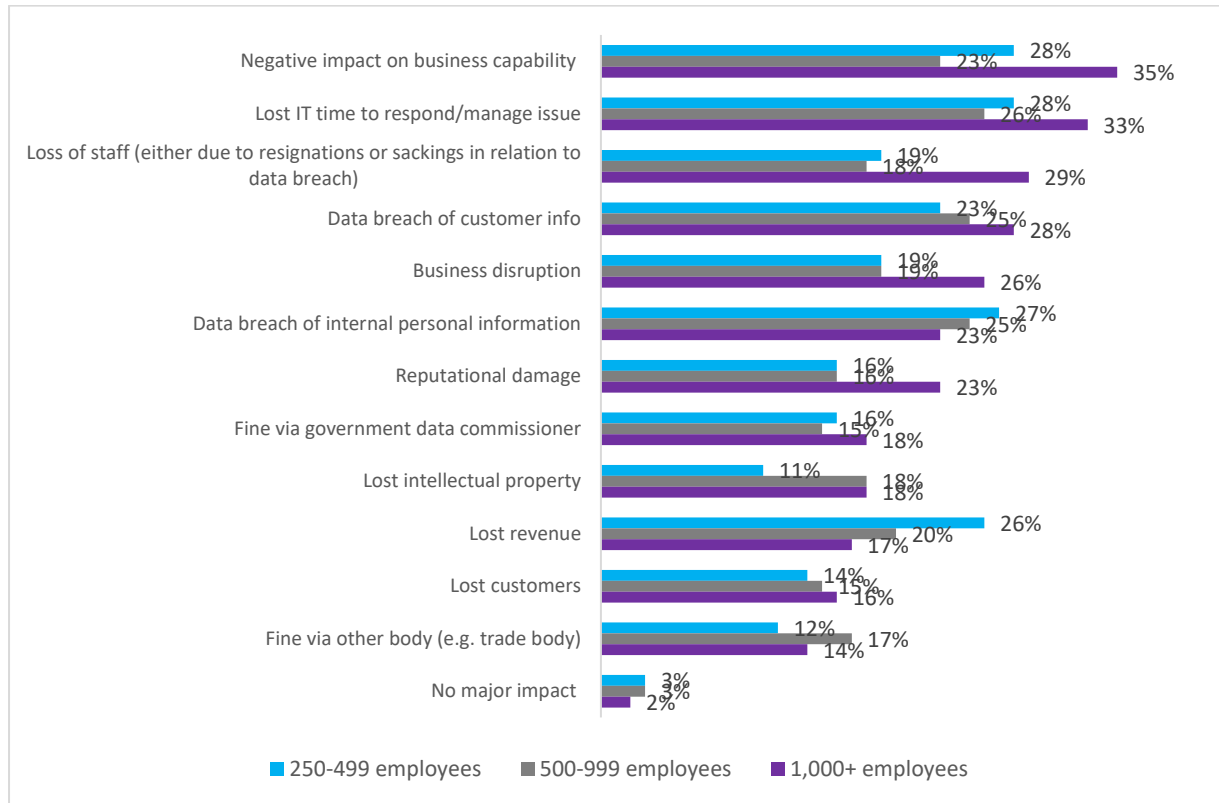


Figure 10. What were the major impacts of these data losses? Select all that apply

Organisations using MPS are most satisfied with print security

US respondents have the largest percentage (50%) that are very satisfied with their print supplier’s security capabilities (Figure 12), with German respondents least satisfied (17% very satisfied). Just 27% of industrial organisations are very satisfied, along with 28% of public sector organisations, compared to 38% of business and professional services organisations. Suppliers have an opportunity here to drive up satisfaction rates by extending their security offerings and working with customers to increase confidence in print security.

Overall, 39% of those using an MPS are very satisfied with their current print supplier, compared to 23% that are not using MPS. This shows how the services that fall under an MPS offering can lead to better relationships with customers and longer ongoing loyalty. However, whereas 42% of CIOs state that they are satisfied with their print supplier’s security capabilities, only 23% of CISOs are – yet again demonstrating a major disconnect between these two closely related roles.

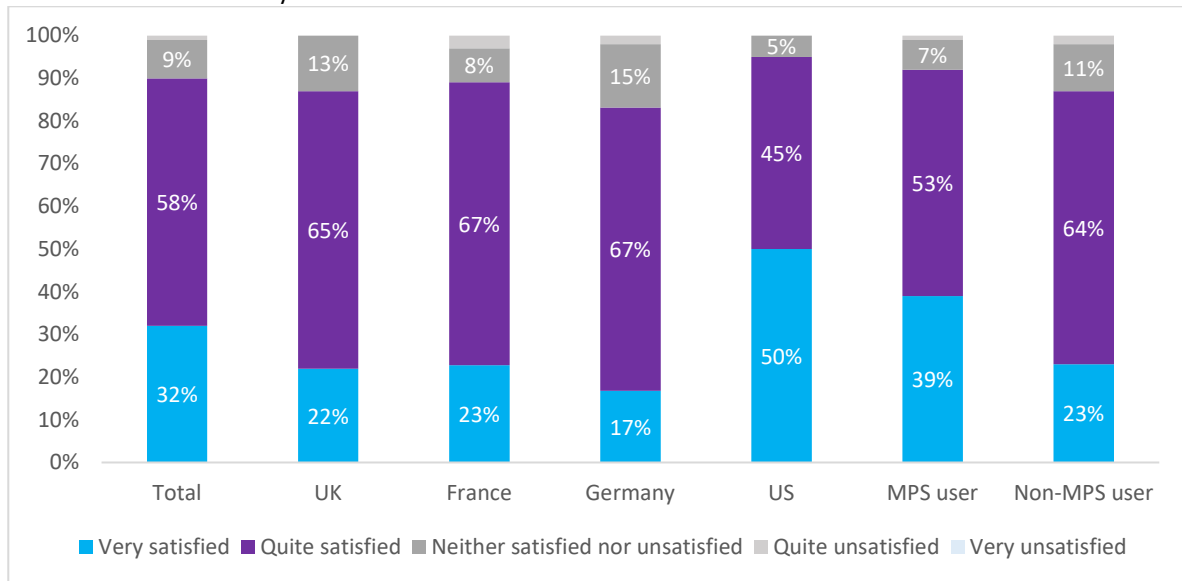


Figure 12. How satisfied are you with your print supplier’s capabilities when it comes to securing your print infrastructure?

Overall brand perception

HP scores highest in overall brand perception of print manufacturers, with 43% perceiving its capabilities as ‘strong’ (Figure 13). Canon comes next with 36%, closely followed by Epson at 35%.

Overall, the average score for being seen as ‘strong’ is 24%. Five vendors (HP, Canon, Epson, Xerox, and Toshiba) score above this level.

HP is strong across the board, but is particularly seen as strong in France (50%), as well as the business and professional services vertical (50%), with 46% of MPS users also seeing it as strong.

Canon is perceived as being strong in France as well (43%), also doing well in large organisations (42%). Epson is also perceived as being strong in France (40%), SMBs (37%), and business and professional services (48%). Xerox is perceived as being strong in the UK and US (34%), large organisations (34%), and retail (36%). Toshiba is seen as strong in the US (32%), SMBs (29%), and retail (31%).

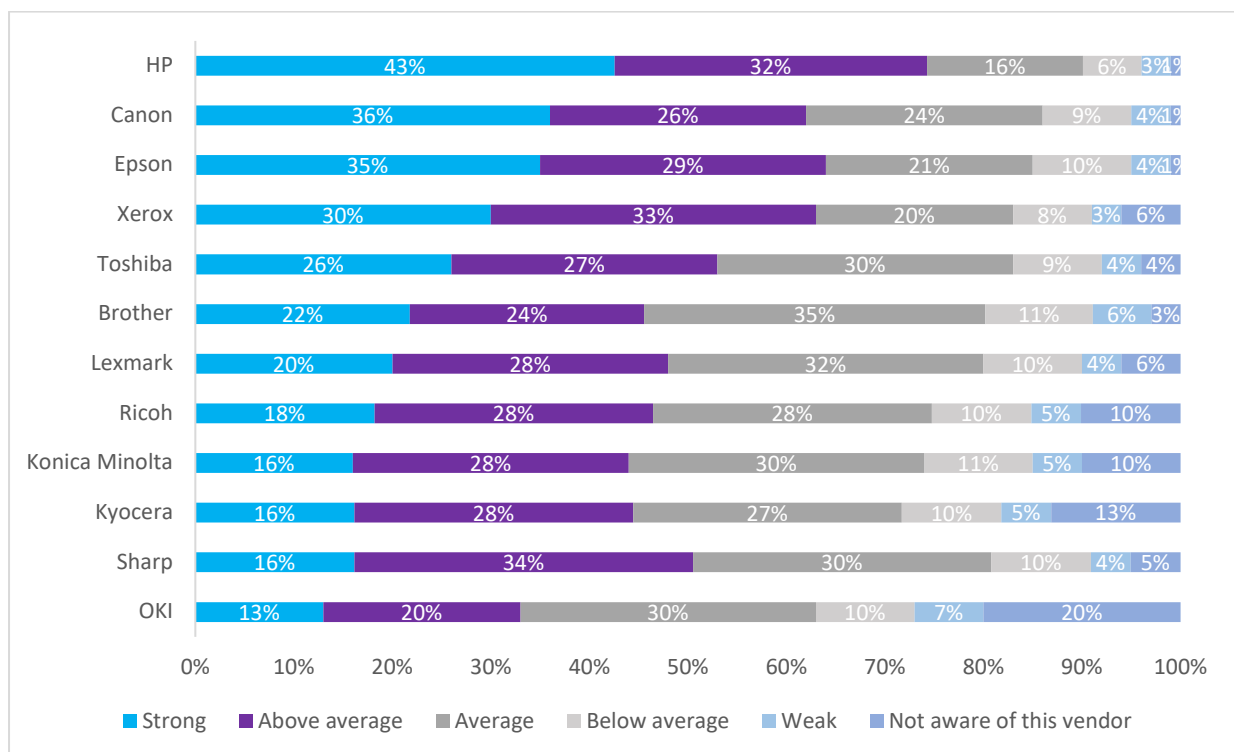


Figure 13. How strong do you believe print security offerings are from the following vendors?

However, overall strength of each manufacturer’s offerings is good: when the ‘not aware of this vendor’ responses are disregarded, fewer than 20% of respondents perceive any single vendor’s capabilities as ‘below average’ or ‘weak’. For organisations that did not score well, this shows how better messaging is needed on what differentiates the vendor’s capabilities from the rest of the field. Vendors must provide the basic messages that the channel can then use.

Recommendations

Print security spend is expected to continue to grow over the next 12 months, creating ongoing opportunities for print manufacturers, managed print service providers, and channel partners. It is clear that organisations using MPS and those that have adopted a range of print security measures are ahead of the curve. Demonstrating how MPS can improve the security resilience of the print infrastructure will enable suppliers to shape their propositions across both the office and home printing environments.

Supplier recommendations

Quocirca recommends that suppliers address the following areas:

- **Bridge the CIO and CISO divide.** In larger organisations, the responsibility for print security may often be fragmented across different IT and business stakeholders. While CIOs have a strategic focus across the IT infrastructure, CISOs are fully focused on security. Given the awareness gap across these decision-makers, suppliers should elevate positioning and messaging of print security to a strategic level. This can support the alignment of print security priorities as CIOs and CISOs develop a more collaborative relationship.
- **Deliver consistent security across the hybrid environment.** Many home printers that are purchased by employees will not conform to the security requirements of the business. Ensure that security-led MPS offerings help address this shadow purchasing through either centralised remote monitoring or provision of authorised devices for home use. While standardised environments generally have a higher level of hardware security compared to a mixed-fleet environment, many organisations operate a mix of device brands across office and home environments. This creates a need for integrated third-party print management platforms that can manage document security consistently across a heterogeneous fleet. Nevertheless, this presents an opportunity for MPS providers to transition customers to a standardised environment to gain tighter security across their print infrastructure.
- **Create clarity around zero trust-led offerings.** There is no one-size-fits all to zero trust. Be clear on how this works with legacy devices and avoid the misuse of the term zero trust – or ‘zero trust-washing’ – to create the perception of robust security. Zero trust in the print landscape can be best achieved through micro-segmentation and integration with multifactor authentication and identity and access management (IAM) platforms. Demonstrate credentials and expertise in this area through focusing on strategic principles and partnerships. This will also build trust with customers that need a secure move to a cloud-based print infrastructure.
- **Harness MPS as an enabler for enhanced security.** Organisations using MPS and a range of security measures – from formal security assessments, audits, and solutions – are ahead of the print security curve – in terms of both confidence and lower data loss. Scalable and flexible security services and solutions will appeal to smaller organisations that are not immune to security risks yet do not have the budget to implement advanced print security measures. Offering regular security reviews as business needs change will also be key to improving satisfaction levels around print security.

Buyer recommendations

The print security threat landscape has expanded to include a variety of home and office devices to support new hybrid ways of working. As intelligent networked devices, MFPs present a weak link in IT security. This can be mitigated with a range of measures based on an organisation’s security posture.

Buyers should consider the following actions:

- **Treat print security as a strategic priority.** Print and IT security must be integrated and considered a higher priority. Elevate the importance of securing the print infrastructure to both CIO and CISO stakeholders so that they are aligned on understanding the risks, and the measures that can be implemented to mitigate risks, of unsecured printing.

- **Conduct in-depth print security and risk assessments.** Organisations should look to providers that can offer in-depth assessments of the print environment. Security audits can uncover potential security vulnerabilities across device and document security. For organisations operating a mixed fleet, this may help in understanding the opportunities for device optimisation using a single fleet with consistent hardware security features.
- **Ensure remote and home workers can print securely.** Ensure printers conform to corporate security standards, and in cases where employees have purchased their own printers, develop security guidelines on whether and how these printers can be used. Evaluate print management platforms for support and security monitoring of home printing.
- **Build a cohesive print security architecture.** Piecemeal security solutions rarely deliver consistent and robust security, particularly across a hybrid work environment. Consider an integrated security platform that can support capabilities such as pull printing, remote monitoring, and reporting across the full fleet. Extend print security to content and workflow through the use of content security and data loss prevention (DLP) tools at the application level. Carefully evaluate vendor zero-trust claims and ensure integration with multi-factor authentication platforms already used in the organisation. Evaluate whether secure print management solutions can operate in a microsegmented network.
- **Formalise processes to respond to print security incidents.** Organisations must ensure that they are prepared for this and have the right processes in place in order to deal with the technical, legal, and reputational fallout from such a breach. This requires the organisation working together to create an embracing set of policies.
- **Continuously monitor, analyse, and report.** Ensure that data from existing security devices, such as security information and event management (SIEM) devices, is collected and analysed to show what has been happening, what is happening now, and what may happen in the future. Ensure that such systems cover as much of the overall platform as possible, and use the insights gained to work on plugging holes in your organisation's security.

Vendor profile: Pharos

Quocirca opinion

Founded in 1992, Pharos Systems International has a strong heritage in the print management software and services market. The company has historically been very strong in the enterprise and education sectors with its on-premise solutions, and in 2013 launched its cloud-native SaaS platform, Pharos Cloud. Pharos stands out for its strong focus on security across both its on-premise and cloud platform, its proven expertise in supporting the complex and high-availability requirements of large enterprises, and a mature approach to zero-trust security. In addition, Pharos offers advanced analytics, notably extended to support work-from-home printing with the Pharos Print-at-Home solution.

In February 2023, Pharos achieved ISO/IEC 27001:2013 certification, demonstrating its continued commitment to information security and formalisation of IT security policies and procedures to help ensure the confidentiality, integrity, and availability of its corporate assets, as well as its Pharos Cloud product.

Pharos Cloud is built on Amazon Web Services (AWS) and supports local data privacy and data sovereignty requirements by providing over 20 predefined geographic regions where secure-release print jobs can be stored at rest in the region where the user is located. These regions correlate directly to secure AWS S3 repositories globally. In addition, administrators can define different metadata collection settings based on region. Pharos Cloud regularly undergoes vulnerability testing and examination by external security specialists, and has received an A+ rating using the Qualys SSL server test. Pharos Cloud supports zero-trust security principles to enable printing in mature zero-trust network environments.

Additionally, in September 2022, Pharos introduced secure scanning capabilities to its cloud platform, enabling users to securely digitise and share documents by scanning to email, network folder, and OneDrive. The initial release supported Ricoh devices only, and in March 2023, the company extended support to Canon (pending certification), HP, Konica Minolta, and Toshiba MFPs.

Pharos is a good choice for large enterprises looking to take advantage of a secure, cloud-based infrastructure while still benefiting from traditional secure print functionality. Along with functionality to support printing in the home environment and secure scanning, Pharos is currently one of the more fully featured print management platforms.

Product overview

In addition to the Pharos Cloud platform, Pharos also offers on-premise print management software, which includes Pharos Blueprint for corporate enterprises and its student pay-for-print software, Pharos Uniprint, which enables colleges and universities to recover and reduce printing costs.

- **Pharos Secure Release** is a cloud-based secure print application that requires users to authenticate themselves at the printer before documents are released for printing, and is a common feature across the company's entire portfolio. Secure Release allows printing across networks, and authentication can be done using various methods, such as PINs, ID cards, and mobile devices. The Delegate Print feature allows a job owner to designate another user or users to release their documents on their behalf. If the document owner and delegate are in different regions, the data privacy settings of the document owner apply. If the document owner and can delegate in different regions, the data privacy settings of the document owner apply. In addition, users can submit Secure Release print jobs from their mobile devices and release them by scanning a QR code at a printer with the mobile app (iOS and Android).
- **The Pharos Cloud platform** leverages end-to-end encryption and supports zero-trust security principles. With Secure Release, users can send print jobs across networks to a centralised queue, which can be accessed from any secured printer within the network. Data is encrypted as it is transmitted from the user's computer to the printer, ensuring that sensitive information remains secure during transmission. Direct Print enables the in-office, direct-to-printer workflows employees are familiar with. The platform also provides comprehensive audit trails and reporting capabilities, allowing organisations to monitor printing activities and ensure compliance with industry regulations.

- **Pharos Direct Print** migrates the in-office, direct-to-printer workflows that employees are familiar with to the cloud and simplifies driver management. Direct Print supports manufacturers' print drivers and simplifies driver management by reducing the number of print drivers that need to be managed. Pharos's advanced IPP-Everywhere print driver, which supports all manufacturers, can be deployed to the majority of users, and manufacturers' drivers can be used only where needed. In addition, Direct Print simplifies driver deployment and makes it easy for employees to find the right printers by automatically adding or removing print queues based on their location.
- **Pharos Insights** provides a singular, comprehensive view of enterprise-wide print operations via intuitive dashboards. Admins can drill down from an intuitive dashboard to view granular job-level data by individual devices, users, and print jobs – and quickly identifies top cost-producing users and under-/overutilised print devices.
- **Pharos Print-at-Home** enables employees to add and print to their home office printer from their work computer. Pharos Print-at-Home supports networked laser and inkjet printers and utilises Internet Printing Protocol (IPP) to create and send the print job for 'driverless' queue management, and provides visibility and control over employees' at-home printing.
- **Secure Scan** feature within Pharos Secure Release enables IT administrators to manage printing and MFP scanning across an organisation, and provides users with a simplified and consistent user experience across all supported manufacturers.

Key differentiators

- **Strong focus on security and zero trust.** Pharos Cloud is ISO 27001 certified and enables printing in mature zero-trust network environments. The platform delivers a robust, highly secure cloud service with an architecture that can address each of NIST's zero-trust security principles. Data is secured in transit and at rest with end-to-end encryption.
- **Monitoring home printing.** Pharos Print-at-Home functionality utilises Internet Printing Protocol (IPP) to create and send print jobs for 'driverless' queue management and provides visibility and control over employees' at home printing.
- **Comprehensive print analytics** provides deep insights into the printing environment through interactive dashboards.
- **Adhere to local data privacy and data sovereignty requirements.** Pharos Cloud supports over 20 regions within a single customer tenant, in which organisations can customise data privacy collection settings and store secure release jobs between submission and release in the cloud in a user's region.
- **Zero-knowledge encryption.** Print jobs are encrypted at the workstation with AES 256-bit zero-knowledge encryption. Customers are provided with a system-generated site encryption key. The system does not retain a copy of this encryption/decryption key, and Pharos is not able to view the customer's site encryption key, which means only the customer has access to print job content.

About Quocirca

Quocirca is a global market insight and research firm specialising in 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 are at the forefront of the rapidly evolving print services and solutions market, trusted by clients 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.

Usage rights

Permission is required for quoting any information in this report. Please see Quocirca's [Citation Policy](#) for further details.

Disclaimer:

© Copyright 2023, Quocirca. All rights reserved. No part of this document may be reproduced, distributed in any form, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Quocirca. The information contained in this report is for general guidance on matters of interest only. Please note, due to rounding, numbers presented throughout this report may not add up precisely to the totals provided and percentages may not precisely reflect the absolute figures. The information in this report is provided with the understanding that the authors and publishers are not engaged in rendering legal or other professional advice and services. Quocirca is not responsible for any errors, omissions or inaccuracies, or for the results obtained from the use of this report. All information in this report is provided 'as is', with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this report, and without warranty of any kind, express or implied. In no event will Quocirca, its related partnerships or corporations, or its partners, agents or employees be liable to you or anyone else for any decision made or action taken in reliance on this report or for any consequential, special or similar damages, even if advised of the possibility of such damages. Your access and use of this publication are governed by our terms and conditions. Permission is required for quoting any information in this report. Please see our [Citation Policy](#) for further details.