Unlocking Print Security: Key Opportunities for Channel Partners

February 25, 2024

[Articles](#), [Channel](#), [Digital Transformation](#), [Managed Print Services](#), [Security](#)

[Quocirca's SMB Attitudes to Print Security 2024 Report](#) reveals that despite 63% of SMBs experiencing a costly print-related data breach in the past year, only 20% are concerned about print security, creating a significant opportunity for vendors and partners to plug the gap with strong security propositions across hardware, solutions, and services.

The research, based on the views of 507 ITDMs with responsibility for print infrastructure in organisations with 250+ employees, of which 120 are SMBs, demonstrates that print security is low on the agenda for SMBs, despite considerable exposure to data loss in the last year. The survey was conducted across the UK, the US, Germany, and France, and a range of verticals including business/professional services, industrials, finance, public sector, and retail were covered.

SMBs are less engaged with print security

SMBs tend to be less engaged and have lower confidence in their ability to manage the range of risks, as well as lower satisfaction with suppliers.

Office print infrastructure concerns just one-fifth (20%) of respondents. A similar proportion feel that employer-provisioned home printers and employee-owned home printers are concerns. Meanwhile, email (31%) and cloud or hybrid application platforms

(29%) are most likely to occupy the top positions among SMBs regarding security, and it appears that this is where they are investing their energies and finances.

Many respondents state that keeping up with print security challenges is becoming harder (40%) and say they are less confident (61% completely or mostly confident) than the largest firms (72%) in their resilience to cope with issues and attacks. Apportioning lower importance to the issues, combined with shaky confidence, translates into lower satisfaction with suppliers compared to their larger counterparts.

It appears that they are not really engaging with print security specifically, and as a result, may feel unsupported. Suppliers that reach out to them with targeted messaging and clear practical suggestions for impactful strategies are likely to stand out.

Revenue loss is a more significant impact for SMBs

Revenue loss is a more significant impact for SMBs than their larger counterparts, but it may help to illustrate that investment in support could mitigate the extent of the loss.

The average cost of each breach is £400,000, only slightly lower than that seen among mid-market organisations, suggesting they are being hit with a disproportionate impact when things go wrong in terms of their size and level of turnover.

Currently SMBs are more likely than larger firms to be managing their print security internally, and there is an overall sense that they are less focused on the specific risk of paper-related breaches, possibly because the majority use a single MSSP to cover print security within the overall IT security environment.

Awakening SMBs to the specific risks of print security and impacts when incidents occur may help them to focus on, and invest more, in more tailored solutions for this part of the overall security picture. This may be best done through an expression of the annual investment against potential loss, in both monetary and other terms that can hit smaller organisations particularly hard.

The risks of multivendor fleets

Overall, 71% of SMBs say they have a multivendor fleet (compared to 64% of mid-market and 76% of large organisations). SMBs need to be alerted to the risks of securing a multivendor fleet. A multivendor fleet may not have consistent security controls across devices, and any home printers may not be authorised or monitored. Overall, reported data losses for organisations operating a mixed fleet of printers (63%) are considerably higher than those with a standardised fleet (56%).

Over three-quarters (78%) of SMBs have changed the composition of their print fleet in the last two years, and a greater proportion of MFPs are in place than previously. While they offer many productivity benefits, MFPs not only pose a risk of paper output falling into the wrong hands – whether accidentally or maliciously – but more concerningly, can act as gateways to the wider IT environment for malicious actors. Helping SMBs

understand types of risk alongside digitisation benefits may be the first step in assisting them with better security controls across device types and brands.

SMBs are deploying a mix of print security measures

SMBs are most concerned with protecting sensitive documents. In terms of top print security challenges, 32% cite preventing printing of sensitive or confidential documents, followed by maintaining the security of print management software (31%) and print hardware (29%).

Although SMBs are deploying a range of print security measures, with formal print security and risk assessments most common (48%), followed by providing authorised printers to home workers that adhere to company security policies, they are behind in terms of implementing most measures. This is likely to explain, at least in part, the extent to which they are suffering from data breaches, and communication that makes the link between the necessary measures and reduced impacts is likely to cut through.

What does this mean for suppliers?

SMBs are at as much risk as larger organisations in terms of data breaches, and when these occur, the damage is considerable – indeed, the damage could be more severe for SMBs as they tend to have lower levels of resource, both financial and in terms of time, than larger organisations. There is plenty of opportunity for suppliers, but cutting through to address SMBs about a subject that currently has low salience will be a challenge, and it needs to be presented in terms that feel relevant and results that feel achievable.

Vendors need to address SMBs' comparatively poor understanding of print security risks and guide them through priorities in terms of both actions and investment. Guidance and support to identify and implement cost-effective, flexible solutions should deliver easy wins for SMBs without impacting their resources. Ensuring frictionless bolstering of cyber-resilience to protect their business capacity, time, and profits should deepen trust and pave the way towards more effective provider relationships overall. If SMBs understand the correlation between the losses they are experiencing and the measures they can take to make themselves more resilient, it will be easier to engage them and ultimately increase their confidence in combatting the different challenges with appropriate solutions.

Narrowing the maturity gap between the smallest organisations and their larger counterparts through channel partners is likely to be valued, especially given their current lower satisfaction with providers' security capabilities. Their greater degree of reliance on MSSPs suggests that partnering with managed IT providers to ensure integration of services can offer value for MPS providers and may be an appropriate route to reach SMB clients.

Find out more in Quocirca's SMB attitudes to Print Security Report

Related Posts

Print 2025: A vision for the future of the print industry

Print Industry Trends, 2024

6 takeaways from the Xerox Global Partner Summit

Stay ahead with industry insights

Receive Quocirca's latest articles and research updates

First Name

Last Name

Email

Privacy

I have read and agree to the terms of use and privacy policy

Subscribe me to the Quocirca newsletter

Subscribe

In the spotlight with Quocirca

In conversation with industry leaders

Find out more

Contact

Get in touch with Quocirca to find out more.

enquiry@quocirca.com

Get in touch

Print 2025

A global market insight study

Visit Print 2025

Services

Expert and actionable insight to inform business innovation and strategy.

View Services

Sign up for regular updates

Sign up to receive regular news and updates about our industry research and projects.

First Name

Last Name

Email

Privacy ☐ I agree to the Privacy Policy

Register