SMBs Turn Focus to Security in the Era of Flexible Working

LONDON RESEARCH
Research Powered Content

In partnership with

Adobe

Contents

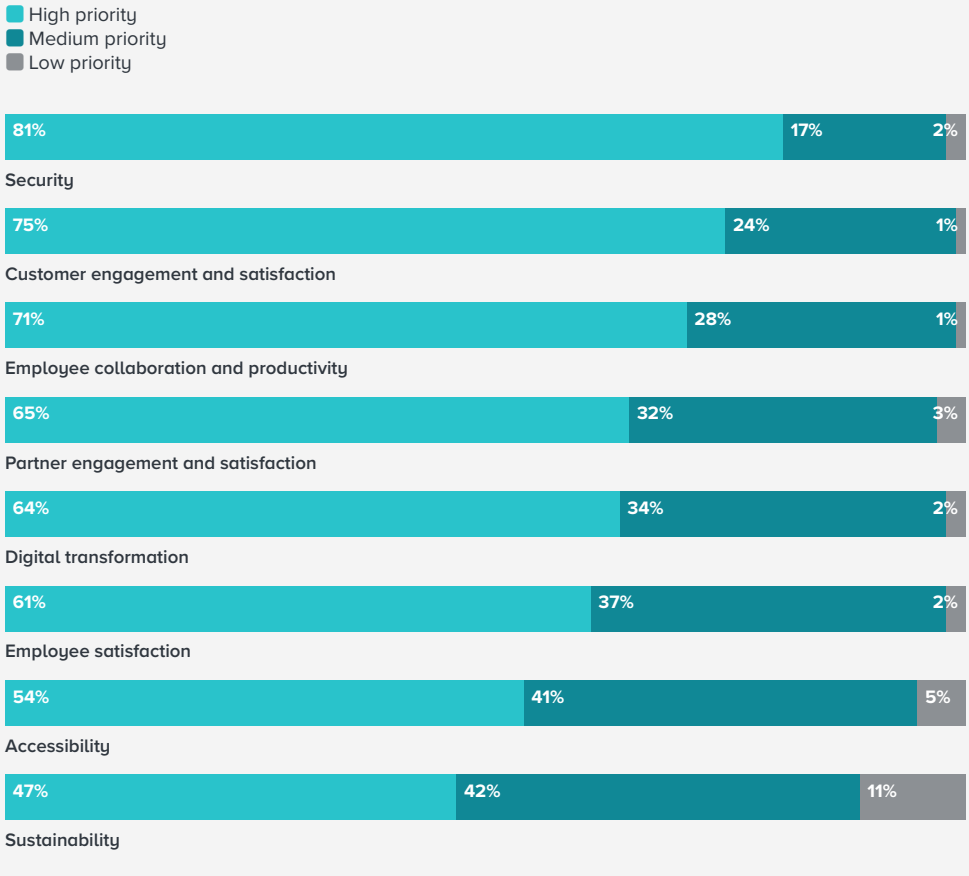
Introduction

Flexible working is now the biggest headache for people in charge of IT, and it's not because their staff are working wherever and whenever they want. It's because everyone else in the organisation is. And by doing so, they're causing massive security concerns. In a 2023 survey of IT leaders at small and medium businesses (SMBs) across EMEA, conducted in partnership with Adobe, four out of five IT executives (83%) said more of their company's employees are working from home now than before. And almost three-quarters (71%) of them said that this increased remote working makes their companies more vulnerable to security issues.

In fact, security was a high priority for 81% of those surveyed (*Figure 1*), above customer satisfaction (75%), employee productivity (71%) or preparing for the digital future (64%). And for most of them (63%), it's also a concern that has become more pressing in the last 12 months.

FIGURE 1

How much of a priority are the following areas for your CTO/CIO in 2023?

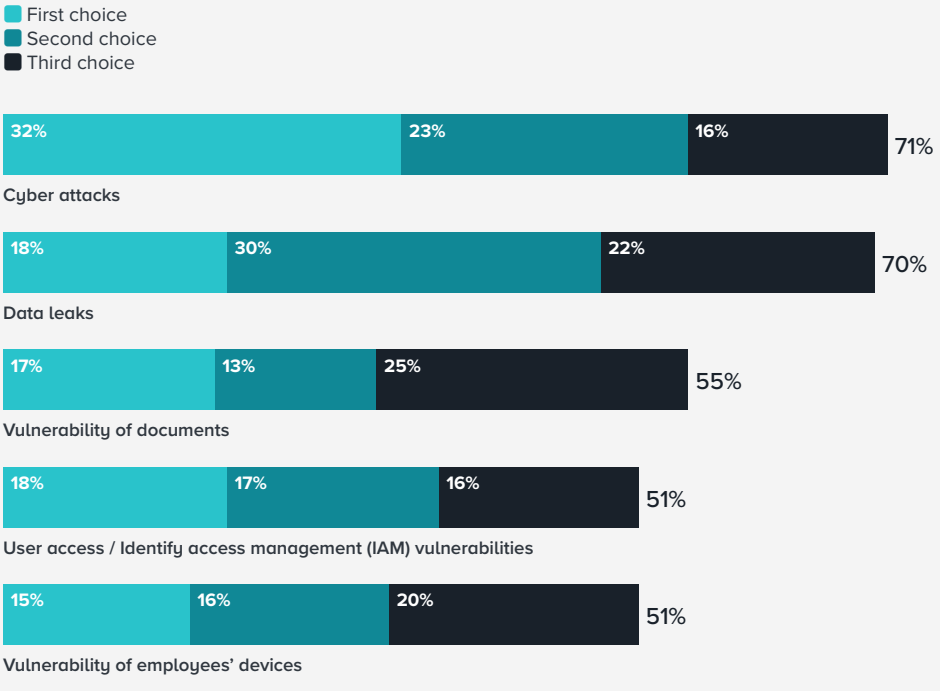


The reason for this is straightforward. No matter how expert you are at maintaining the security and integrity of the company's IT infrastructure when everyone's working inside the firewall, it's infinitely harder when people start accessing company servers via unsecured networks, or on their personal laptops, tablets and mobile phones.

So, when we asked our SMB IT leaders what kind of worries were most likely to keep them awake at night, it was no surprise to see that the vulnerability of sensitive documents was in the top three, after cyber attacks and data leaks (*Figure 2*).

FIGURE 2

Which of the following security challenges and concerns are most likely to keep you awake at night?



Document management in the age of flexible working
Document security has three main components:

User security

Does it stop unauthorised access to documents?

Content security

Does it stop unauthorised sharing of complete documents, or of sensitive details from within documents, and allow identification of shared documents that have been tampered with?

System security

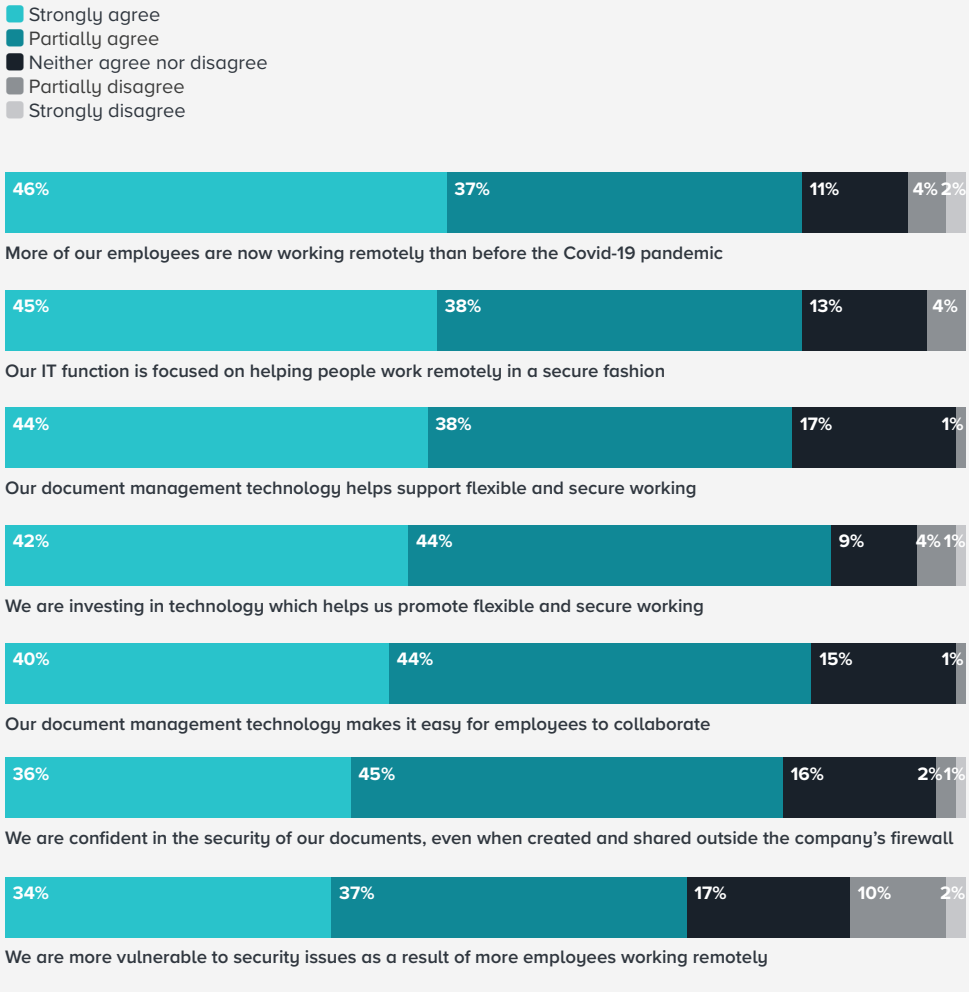
Does it protect the organisation's wider systems from malicious attempts to write to, or read from, a computer's file system?

In fact, more than half of our IT respondents aren't confident they've got secure document management nailed. One of the big challenges is collaboration. Helping staff work together while remote is a priority for IT departments, as we've seen. But securing point-to-point communications between employees and the company servers is one thing; when all those employees start sharing, reviewing and editing documents among themselves, the difficulty – and therefore the risks – rise exponentially.

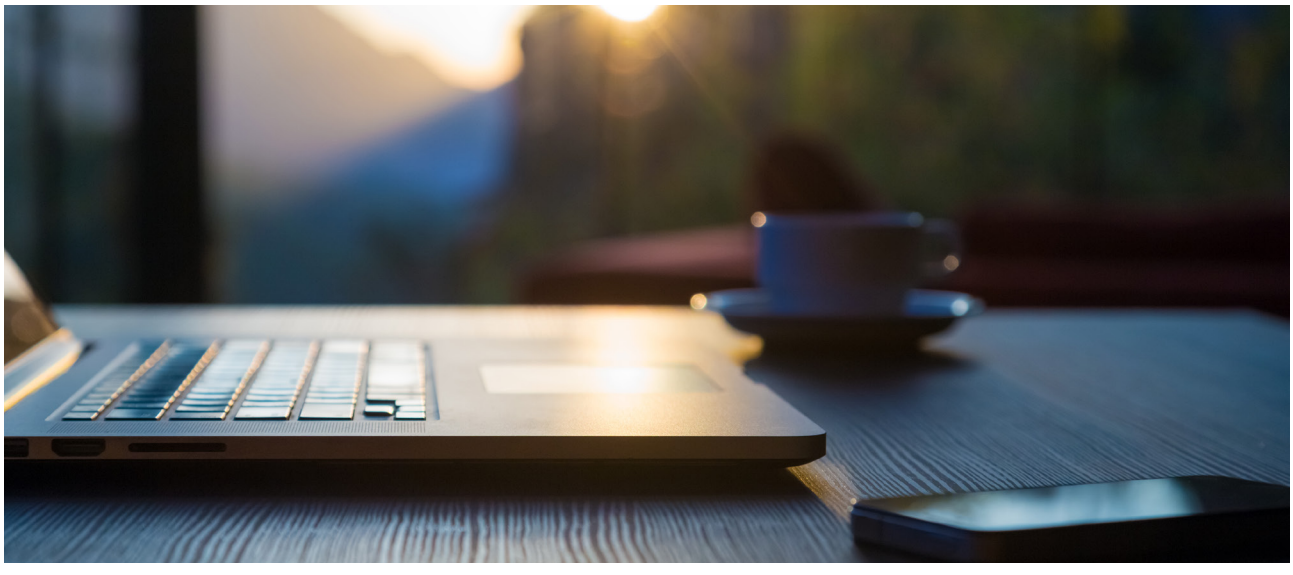
As *Figure 3* shows, only 44% strongly agree their document management technology helps support flexible and secure working, and fewer still (36%) strongly agree they're confident in the security of their documents, even when they're created and shared outside the company's firewall. In contrast, 45% only partially agreed they're confident in the security of their documents.

FIGURE 3

To what extent do you agree or disagree with the following statements relating to secure working practices within your organisation?



It therefore makes sense from the SMB IT perspective that investment in document management is justified by a reduction in security risks, as well as increased employee productivity. In the search for technology to support remote working, businesses need to understand that flexibility and security are equally important. Either one is worthless without the other.

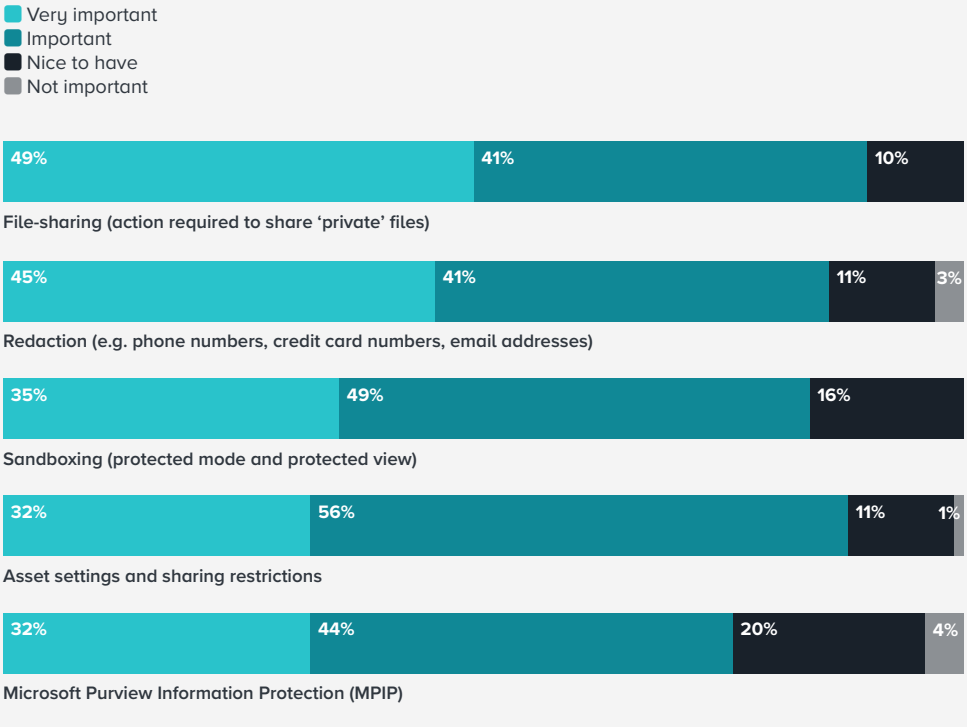


Importance of document management capabilities

On the shopping list of security-related document management software functionality requirements for SMB IT leaders, by far the two most important elements are a privacy-first approach to file-sharing, and the ability to redact sensitive or confidential information in a document before it's distributed. These features were chosen as being 'very important' by 49% and 45% of our respondents, respectively (*Figure 4*).

FIGURE 4

How important for your organisation are the following security-related document management features and capabilities?



Other features, such as sandboxing, asset settings and sharing restrictions, and Microsoft Purview Information Protection, were still widely seen as 'important' but are much less likely to be deal-breakers.

Over half of our IT executives also say their companies' employees place a high value on security in their day-to-day role (*Figure 5*). It's the only feature that more of them rate as 'very important' than 'important'. It's also one of the lowest rated as just a 'nice-to-have'.

FIGURE 5

How important are the following document management features for your company's employees in their day-to-day role?

Once again, this shows the importance of balancing security with ease of use. Certain features that might be expected to be regarded as part of a secure system – such as accountability and authentication, or access control – are significantly less likely to be rated as very important by users.

These figures also suggest that, when end users think about security, they're not necessarily thinking about the same thing as their IT counterparts are. And it points to another issue for organisations coming to terms with increasing levels of remote working.

While users may recognise the importance of security at a theoretical level, that recognition can, in practice, go out of the window when faced with a deadline. Education plays an important role here, but even better is to have systems that are designed to be 'secure by default', that nudge users towards taking the secure route while still making it easy for them to complete their work.

What could possibly go wrong?

According to research by IBM[1], the global average cost of a data breach in 2022 was $4.35m, up by 12.7% from 2020. The average 2022 cost in the UK was $5.05m, in Germany $4.85m, and in France $4.34m. And the US National Cyber Security Alliance found that 70% of all cyber attacks target small and medium-sized businesses, simply because their cyber security is often less stringent[2]. The costs can include:

- **Ransom payments**
- **Falling share price (for publicly-traded companies)**
- **Lost revenues due to systems being down**
- **Remediation**
- **Legal and audit fees.** Harvard Business Review[3] reports: "The audit fees for companies following data breaches can be about 13.5% higher than those for firms without breaches".
- **Increased insurance premiums**

But the impacts go further than that. You might also face:

- **Loss of intellectual property**
- **Price hikes.** 60% of companies that suffer a data breach have to pass the cost on to their customers by raising prices, according to The Ponemon Institute[4].
- **Financing becoming more difficult and more expensive.** HBR also points out that cyber risks can result in a credit-rating downgrade.
- **Damage your brand.** Customers – and potential customers – may regard you as less trustworthy. A 2022 PwC[5] report found that, in the previous three years, 27% of businesses worldwide had lost customers, and 23% had suffered reputational or brand damage due to a cyber breach or data privacy incident. Brand damage will also mean increased PR costs as you attempt to rebuild your reputation.
- **Being fined by regulatory authorities.** If the breach results in the exposure of customers' personal data, you could be breaking legal obligations. Under the GDPR[6], national data protection authorities can impose a maximum fine of €20m or 4% of the company's global turnover – whichever is greater – for infringements. Lesser penalties include warnings and reprimands, temporary or permanent bans on data processing, ordering the rectification, restriction or erasure of data, and suspending data transfers to third countries.

1 https://www.ibm.com/reports/data-breach
2 https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses
3 https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach
4 https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/
5 https://www.pwc.com/gx/en/news-room/press-releases/2022/global-digital-trust-insights-survey.html
6 https://gdpr.eu/fines/

Recommendations for SMB IT leaders

Think flexible and secure working

It's no good enabling your staff to work from anywhere if doing so leaves you open to data breaches and cyber attacks, and compromises the security of your documents. Equally, it's no use making your security so tight that people struggle to use the authorised platforms. In fact, it's worse, because if they can't use the official channels, they'll find workarounds, and then you'll have no security at all.

Think integrated solutions

Managing mass remote working is hard enough without having to worry about bringing together multiple tools – for document management, file-sharing and electronic signatures – across multiple channels. The simpler you make life for staff, the more productive they'll be. And the more productive you'll be.

Think security-by-default

Don't rely on your staff to think about security when they've got other pressures to worry about. Aim to make it easier for them to do the right thing rather than the wrong one.

Think Adobe

Maximise the security of your technology stack and your data by working with integrated digital document solutions from a company that has engrained security deeply in everything it does.

Think Adobe

Trust & Identity in Acrobat Sign

Acrobat Sign: Created with trust in mind

With Acrobat Sign, you get the reassurance of using a digital signature – a combination of an e-signature and a digital certificate. A digital signature is recognised as being more secure than a simple e-signature and provides a higher degree of trust in many countries around the world – including in the United States and the European Union. It uses cryptography to bind the digital certificate to the signed document to help prove the signer is who they say they are. Plus, with a timestamp and tamper-evident seal, it helps to give you more confidence in the authenticity of your document.

Data Centre in the European Union / EMEA

Regional Data Centres: Performance and security closer to your business

Our Document Cloud data centres include data centres based in EMEA / the European Union. These regional data centres bring your data closer to your business – delivering better performance, and enhanced collaboration and access. By unifying storage across Document Cloud and Creative Cloud, you're able to unlock the full potential and features of Document Cloud services – including creating, editing, and sharing PDFs directly in Microsoft 365 apps. Plus, you get more control, which helps to accelerate enterprise adoption and enhance storage efficiency.

C5 Attestation

C5: Keeping your security top of mind

Adobe Document Cloud is compliant with C5 (Cloud Computing Compliance Criteria Catalogue), an attestation scheme introduced in Germany by the Federal Office for Information Security (BSI), backed by the German Government. C5 attestation leverages internationally recognised IT security standards to provide a consistent security framework for certifying cloud service providers. Completing C5 attestation is part of our ongoing commitment to provide best in class cloud security – offering transparency of data protection and assurance that your data will be managed in accordance with IT security standards.

Methodology

This London Research whitepaper, commissioned by Adobe, is based on a survey of 200 IT decision makers at small and medium businesses with responsibility for document management software working in the UK, France and Germany. The survey was fielded in February 2023. SMBs are defined as organisations with annual revenues of less than £100m.

About us

LONDON RESEARCH
Research
Powered
Content

London Research, set up by former Econsultancy research director Linus Gregoriadis, is focused on producing research-based content for B2B audiences. We are based in London, but our approach and outlook are very much international. We work predominantly, but not exclusively, with technology vendors and agencies seeking to tell a compelling story based on robust research and insightful data points.

As part of Communitize Ltd, we work closely with our sister companies Digital Doughnut (a global community of more than 1.5 million marketers) and Demand Exchange (a lead generation platform), both to syndicate our research and generate high-quality leads.

Learn more

Adobe Acrobat

Business still runs on documents, and today's teams expect to work seamlessly on them from anywhere using trusted, well-integrated software. Made by the inventor of PDF, Adobe Acrobat is the single PDF and e-signature tool made for today's hybrid organisations. With an all-in-one solution from a trusted brand like Adobe Acrobat, your organisation can operate with confidence in the flow of work.

Learn more


LONDON
RESEARCH
Research
Powered
Content