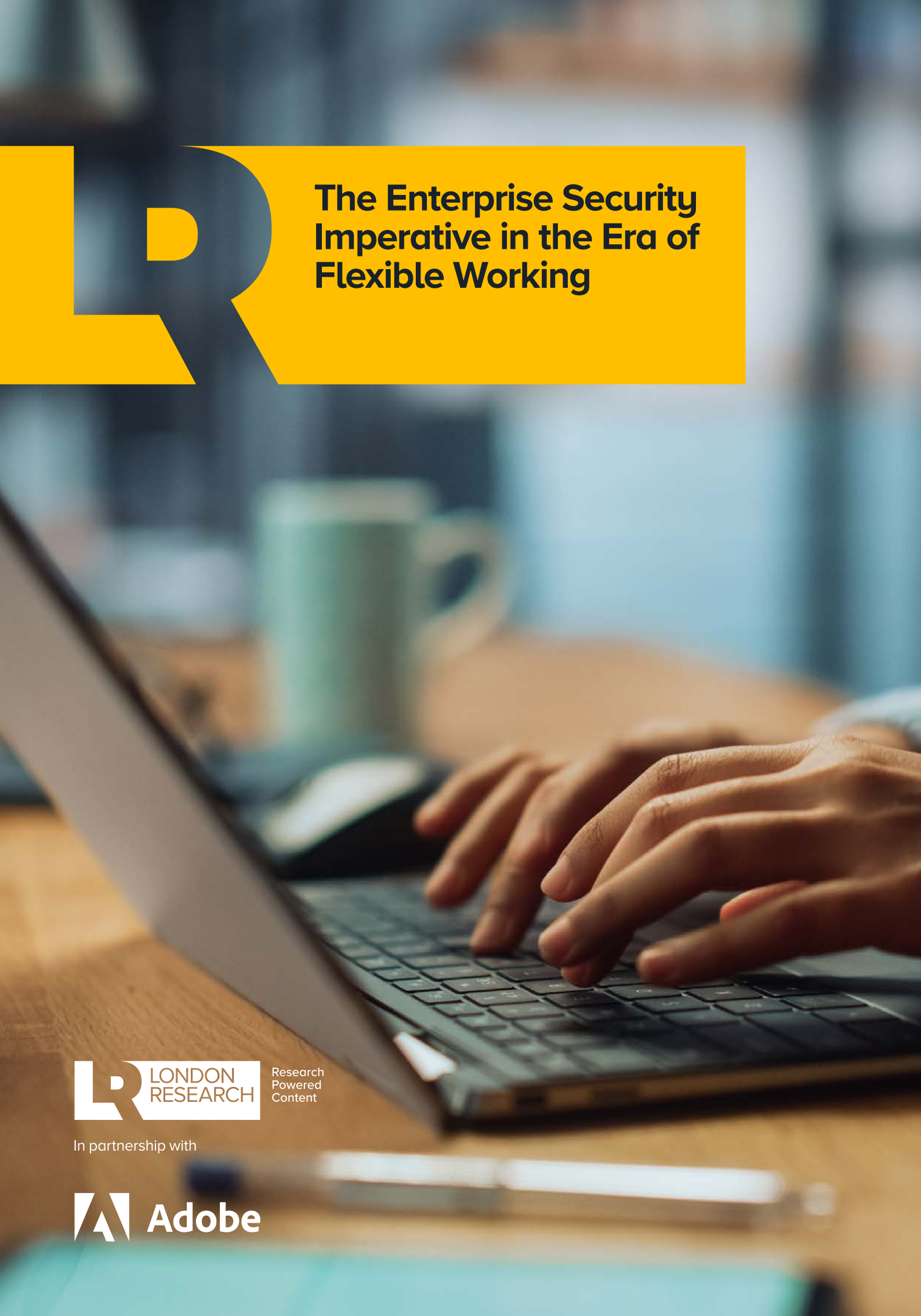
The Enterprise Security Imperative in the Era of Flexible Working



LONDON RESEARCH
Research Powered Content

In partnership with

Adobe

Contents

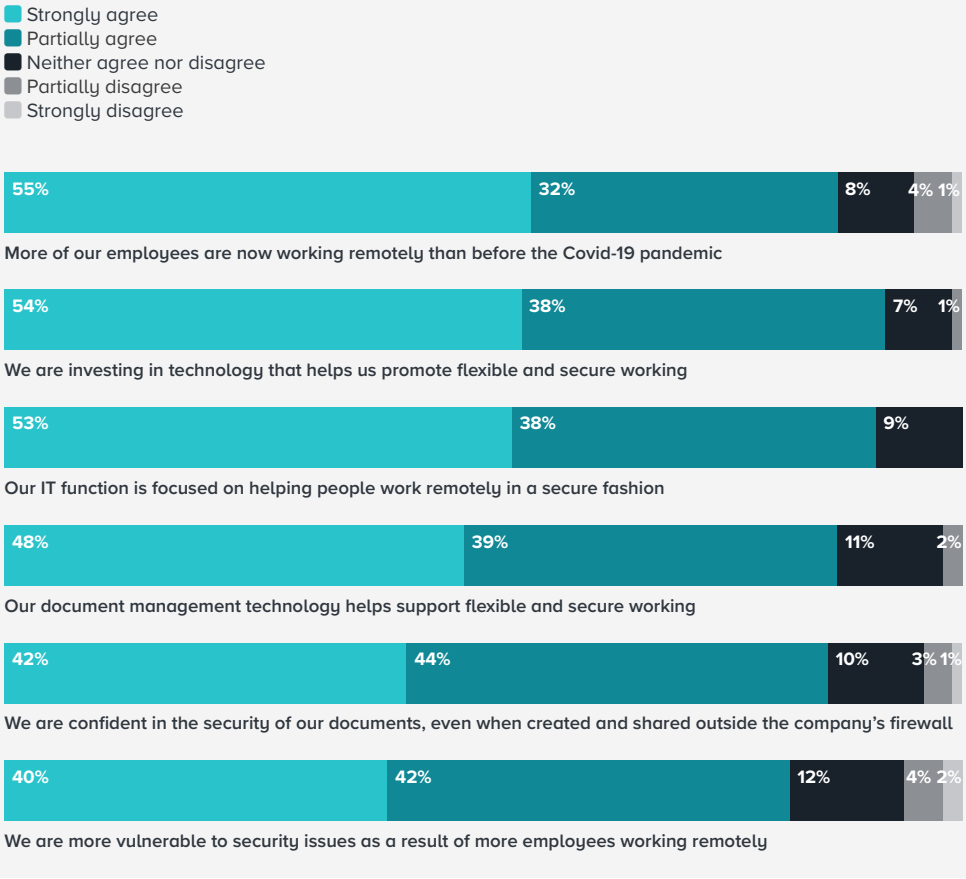
Introduction

Data security has always been crucial for enterprise businesses, but the stakes have never been higher than they are now. That is partly because the average cost of a data breach globally reached $4.35m in 2022, $5.05m for the UK, $4.85m for Germany, and $4.34m for France. But mainly it is because businesses suddenly have a lot more security issues to deal with. And it is all down to flexible working.

Research for Adobe by London Research found that almost nine out of ten enterprise IT decision-makers (87%) say more of their employees are working remotely than before. And four out of five say that means their companies are more vulnerable to security issues (*Figure 1*).

FIGURE 1

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



The reason for this is straightforward, although the solutions are not. No matter how expert the IT department might be at maintaining the security and integrity of the company's technology infrastructure when everyone is working inside the firewall, it is infinitely harder when people start accessing company resources via unsecured networks, or on their personal laptops, tablets and mobile phones.

Paying the price for poor security
Some of the costs of a data security breach are obvious, such as:

- **Ransom payments**
- **Falling share price**
- **Lost revenues due to systems being down**
- **Damage to your brand.** Customers – and potential customers – may regard you as less trustworthy following a breach. A 2022 PwC[1] 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.
- **Fines from regulatory authorities.** If the breach results in the exposure of customers' personal data, you could be breaking legal obligations. Under the GDPR[2], national data protection authorities across Europe 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.

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

- **Loss of intellectual property**
- **Price hikes.** 60% of companies that suffer a data breach have to pass the cost onto their customers by raising prices, according to The Ponemon Institute[3].
- **Financing becoming more difficult and more expensive.** HBR also points out that cyber risks can result in a credit-rating downgrade.
- **Remediation**
- **Legal and audit fees.** Harvard Business Review[4] reports: "the audit fees for companies following data breaches can be about 13.5% higher than those for firms without breaches".
- **Increased insurance premiums**

1 https://www.pwc.com/gx/en/news-room/press-releases/2022/global-digital-trust-insights-survey.html
2 https://www.taylorwessing.com/-/media/taylor-wessing/files/germany/2019/10/german-data-protection-supervisory-authorities-model.pdf
3 https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/
4 https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

As a result, data security is the biggest area of concern for enterprise CTOs and CIOs in 2023 (*Figure 2*), with 86% saying it is a high priority. This is a higher percentage than for often more high profile areas such as digital transformation (77%), customer engagement and satisfaction (73%), and sustainability (56%). And three-quarters (75%) say it is more important than it was a year ago (*Figure 3*).

FIGURE 2

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

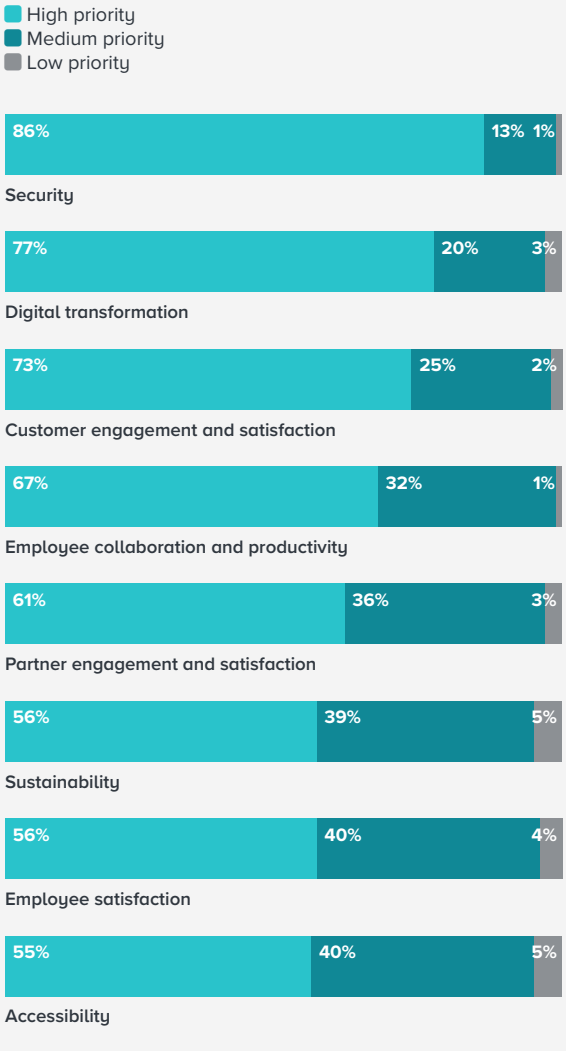
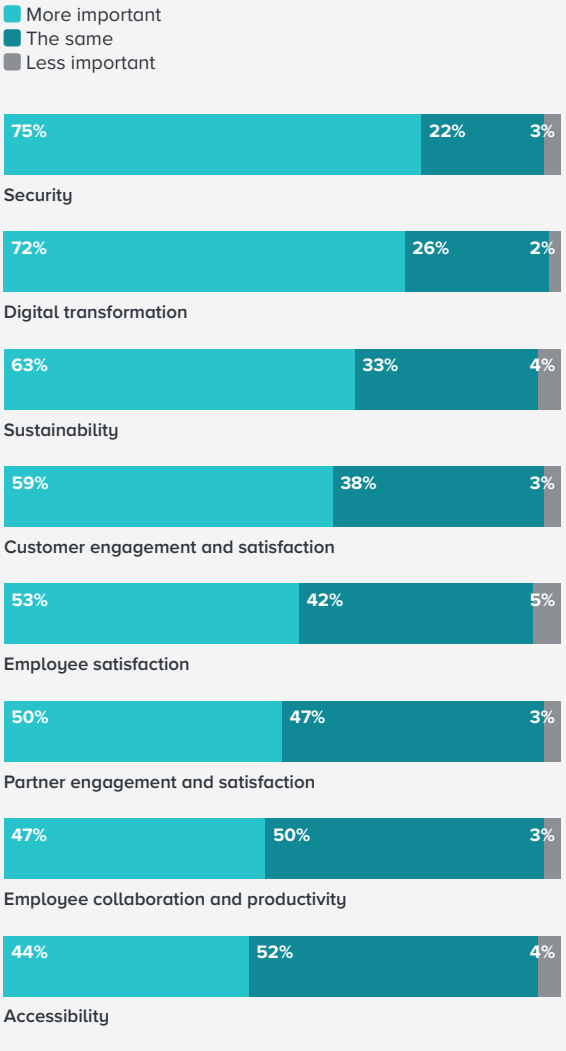


FIGURE 3

Are these themes more or less important to your CTO/CIO than they were a year ago?



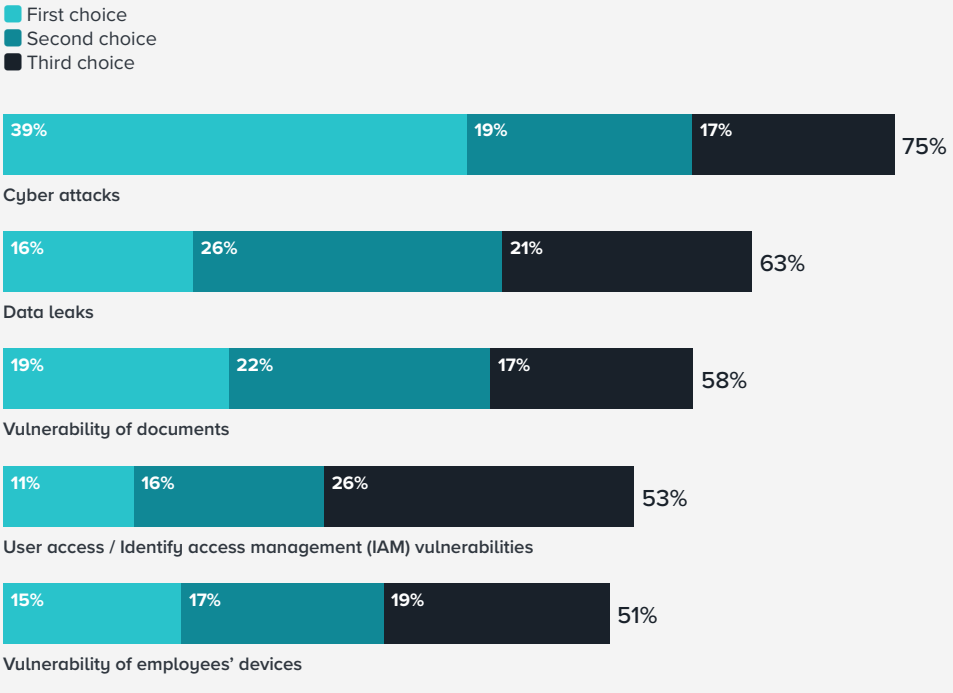
At the same time, enterprises want to capitalise on the benefits of offering flexible working. The CIPD reports that "direct business benefits include savings on office space" and that "flexible working also allows a better match between business resources and demand, for example serving customers on a 24/7 basis." Meanwhile, research from Cranfield University shows "flexible workers record higher levels of job satisfaction and organisational commitment than their non-flexible counterparts".

Document management in the age of flexible working

All this means document management needs to be one of the key areas of focus for security initiatives now that employees are increasingly working outside of the on-premise company firewall. When we asked IT leaders which security challenges and concerns were most likely to keep them awake at night, cyber attacks were by far the most worrying. Data leaks came in second, ahead of vulnerabilities relating to documents, user/identity access, and employee devices (*Figure 4*).

FIGURE 4

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



Alongside this, confidence is high that enterprises are going in the right direction. Some 87% of IT heads agreed that their document management technology helps support flexible and secure working. However, there are still lurking doubts. Less than half 'strongly agreed' they were confident in the security of their company's documents, even when created and shared outside its firewall (*Figure 1*).

The response to these concerns is further investment in more secure technology. More than nine out of ten IT leaders (92%) surveyed agreed they were investing in technology that helps them promote flexible and secure working (*Figure 1*). For IT teams at least, the benefits of this investment relate to both sides of the flexible-working coin; reduced security risks and increased employee productivity and satisfaction (*Figure 5*).

FIGURE 5

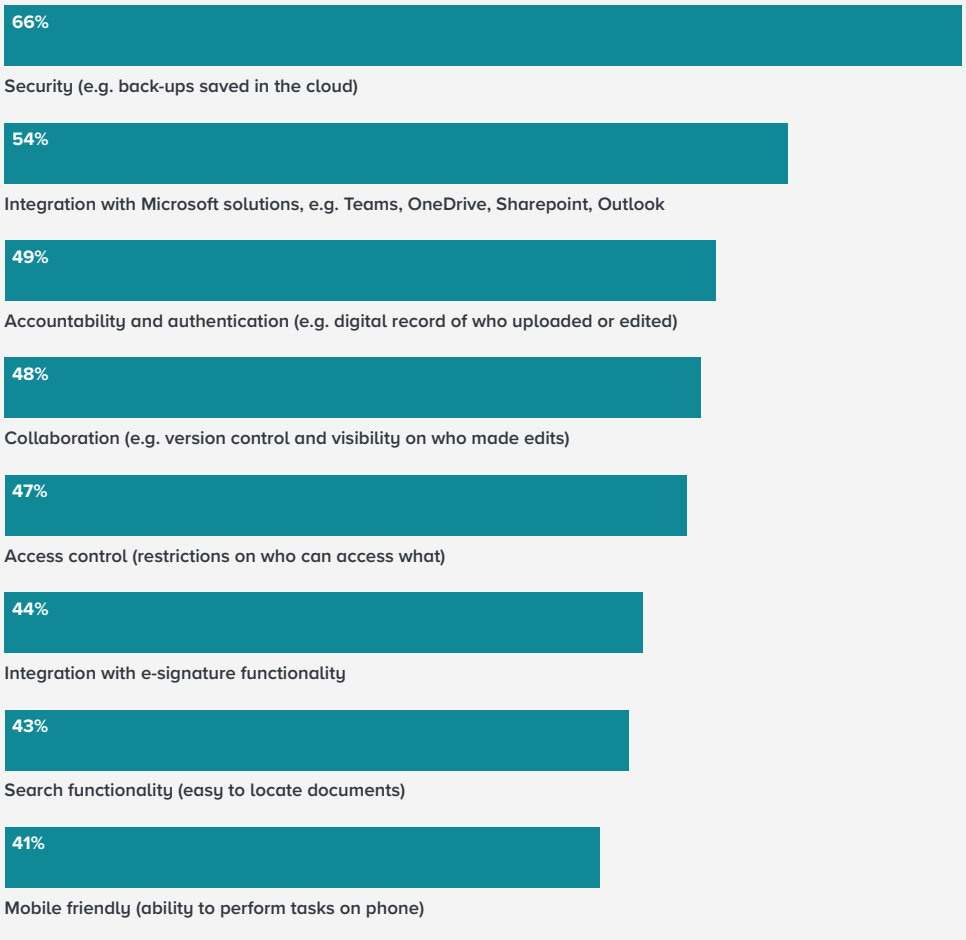
How does your organisation measure the impact of investment in document management software?

What users want

The end-users of these new document security systems have clear ideas of what they – rather than IT – need from the software (*Figure 6*). They are very much focused on security and accountability/authentication, but they also want integration with other solutions (e.g. Microsoft) and effective collaboration (e.g. visibility on edits, and version control). This shows how vital it is for IT departments to balance security with ease of use.

FIGURE 6

Proportion of organisations saying that the following document management features are 'very important' for their employees in their day-to-day role



These figures also suggest that, when end-users think about security, they are 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.

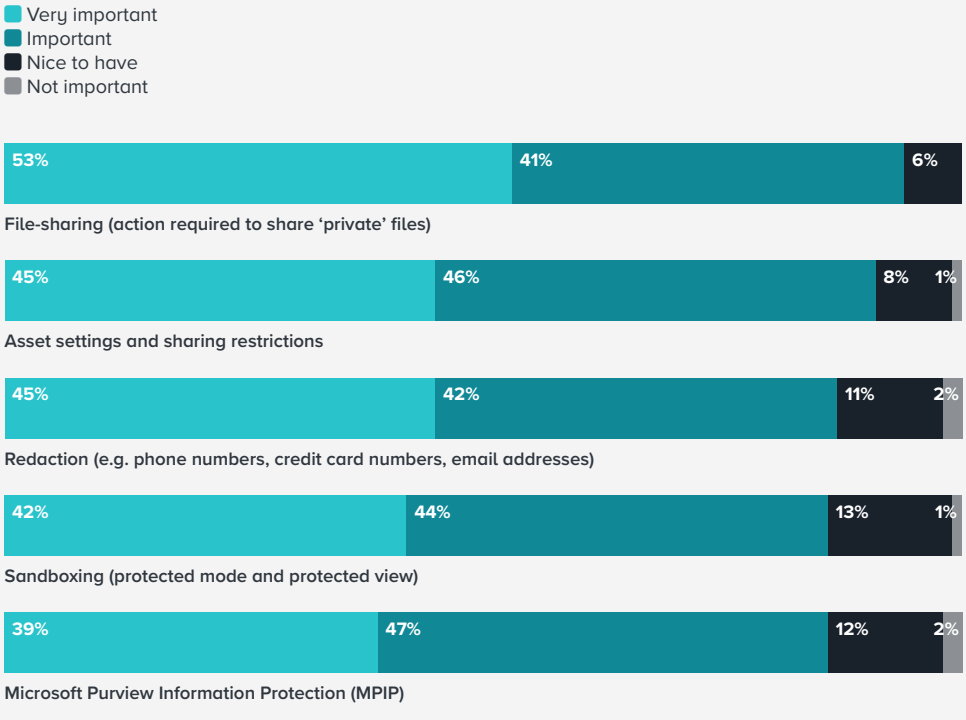
While users may recognise the importance of security at a theoretical level, that recognition can, in practice, go out of the window when faced with a deadline. Education plays an important role here, but even better is to have systems that are designed to be 'secure by default', that nudge users towards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

What IT needs

This move towards 'security by default' showed up when we asked our IT leaders what was on their shopping list of features for a document security system. The requirement of an action to share 'private' files is a perfect example of this kind of thinking, and came top of the list (*Figure 7*).

FIGURE 7

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



On top of this, enterprise organisations are increasingly seeking out document management solutions that enable them to secure other types of documents such as video files, not just PDFs. This too makes sense, since a system that is integrated by design will always be more secure than one bolted together from multiple solutions.

Recommendations for Enterprise IT leaders

Think flexible and secure working

It is 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 is no use making your security so tight that people struggle to use the authorised platforms. In fact, it is worse because if they can not use the official channels, they will find workarounds and then you will 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 will be, and the more productive you will be.

Think security-by-default

Do not rely on your staff to think about security when they have 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 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 enterprise businesses with responsibility for document management software working in the UK, France and Germany. The survey was fielded in February 2023. Enterprise companies are defined as organisations with annual revenues of more 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